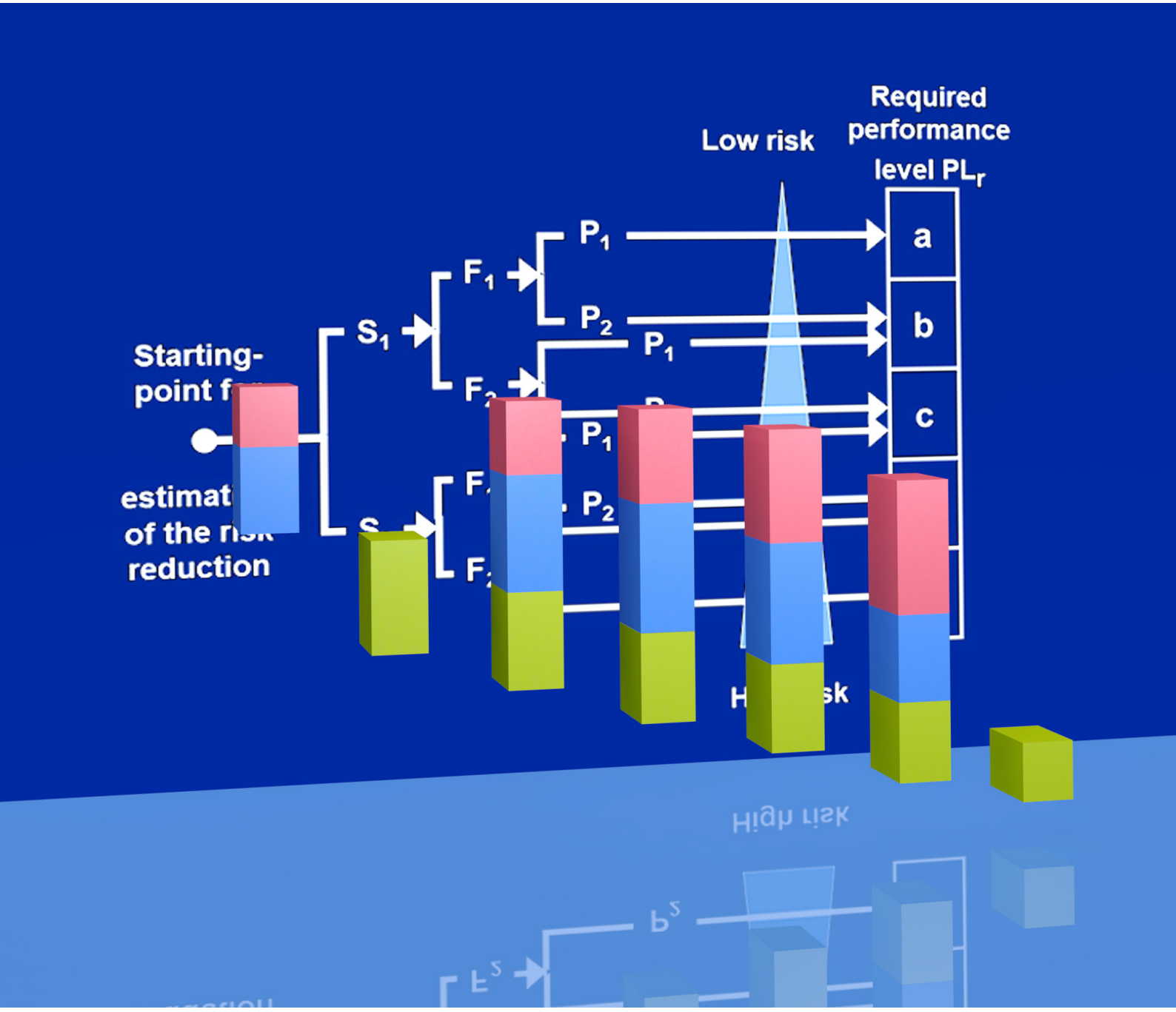
DGUV
Deutsche Gesetzliche
Unfallversicherung
Spitzenverband



IFA Report 2/2017e

Functional safety of machine controls

– Application of EN ISO 13849 –

Authors: Michael Hauke, Michael Schaefer, Ralf Apfeld, Christian Werner, Thomas Bömer, Michael Huelke, Andre Steimers, Torsten Borowski, Karl-Heinz Büllesbach, Michael Dorra, Hans-Georg Foermer-Schaefer, Jürgen Uppenkamp, Oliver Lohmaier, Klaus-Dieter Heimann, Burkhard Köhler, Helmut Zilligen, Stefan Otto, Paul Rempel, Günter Reuß
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin

Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Glinkastr. 40
10117 Berlin
Germany
Phone: + 49 (0)30 13001-0
Fax: +49 (0)30 13001-9876
Internet: www.dguv.de
E-mail: info@dguv.de

– July 2019 –

ISBN: 978-3-86423-232-9
ISSN: 2190-7994

Abstract

Functional safety of machine controls
– Application of EN ISO 13849 –

The EN ISO 13849-1 standard, "Safety of machinery – Safety-related parts of control systems", contains provisions governing the design of such parts. This report is an update of BGIA Report 2/2008e of the same name. It describes the essential subject-matter of the standard in its third, revised 2015 edition, and explains its application with reference to numerous examples from the fields of electromechanics, fluidics, electronics and programmable electronics, including control systems employing mixed technologies. The standard is placed in its context of the essential safety requirements of the Machinery Directive, and possible methods for risk assessment are presented. Based upon this information, the report can be used to select the required Performance Level PL_r for safety functions in control systems. The Performance Level PL which is actually attained is explained in detail. The requirements for attainment of the relevant Performance Level and its associated Categories, component reliability, levels of diagnostic coverage, software safety and measures for the prevention of systematic and common-cause failures are all discussed comprehensively. Background information is also provided on implementation of the requirements in real-case control systems. Numerous example circuits show, down to component level, how Performance Levels a to e can be engineered in the selected technologies with Categories B to 4. The examples provide information on the safety principles employed and on components with well-tried safety functionality. Numerous literature references permit closer study of the examples provided. The report shows how the requirements of EN ISO 13849-1 can be implemented in engineering practice, and thus makes a contribution to consistent application and interpretation of the standard at national and international level.

Kurzfassung

Funktionale Sicherheit von Maschinensteuerungen
– Anwendung der DIN EN ISO 13849 –

Die Norm DIN EN ISO 13849-1 „Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen" macht Vorgaben für die Gestaltung von sicherheitsbezogenen Teilen von Steuerungen. Dieser Report ist eine Aktualisierung des gleichnamigen BGIA-Reports 2/2008. Er stellt die wesentlichen Inhalte der Norm in ihrer dritten Ausgabe von 2016 vor und erläutert deren Anwendung an zahlreichen Beispielen aus den Bereichen Elektromechanik, Fluidtechnik, Elektronik und programmierbarer Elektronik, darunter auch Steuerungen gemischter Technologie. Der Zusammenhang der Norm mit den grundlegenden Sicherheitsanforderungen der Maschinenrichtlinie wird aufgezeigt und mögliche Verfahren zur Risikoabschätzung werden vorgestellt. Auf der Basis dieser Informationen erlaubt der Report die Auswahl des erforderlichen Performance Level PL_r für steuerungstechnische Sicherheitsfunktionen. Die Bestimmung des tatsächlich erreichten Performance Level PL wird detailliert erläutert. Auf die Anforderungen zum Erreichen des jeweiligen Performance Level und seine zugehörigen Kategorien, auf die Bauteilzuverlässigkeit, Diagnosedeckungsgrade, Softwaresicherheit und Maßnahmen gegen systematische Ausfälle sowie Fehler gemeinsamer Ursache wird im Detail eingegangen. Hintergrundinformationen zur Umsetzung der Anforderungen in die steuerungstechnische Praxis ergänzen das Angebot. Zahlreiche Schaltungsbeispiele zeigen bis auf die Ebene der Bauteile hinunter, wie die Performance Level a bis e mit den Kategorien B bis 4 in den jeweiligen Technologien technisch umgesetzt werden können. Sie geben dabei Hinweise auf die verwendeten Sicherheitsprinzipien und sicherheitstechnisch bewährte Bauteile. Zahlreiche Literaturhinweise dienen einem tieferen Verständnis der jeweiligen Beispiele. Der Report zeigt, wie die Anforderungen der DIN EN ISO 13849-1 in die technische Praxis umgesetzt werden können, und leistet damit einen Beitrag zur einheitlichen Anwendung und Interpretation der Norm auf nationaler und internationaler Ebene.

Résumé

La sécurité fonctionnelle des systèmes de commande de machines
– Application de la norme DIN EN ISO 13849 –

La norme DIN EN ISO 13849-1 « Sécurité des machines – Parties des systèmes de commande relatives à la sécurité » définit comment doivent être conçues les parties des systèmes de commande relatives à la sécurité. Le présent rapport est une version actualisée du rapport 2/2008 du même nom du BGIA. Il présente les principaux contenus de la norme dans sa troisième édition de 2015, et en explique l'application à partir de nombreux exemples pris dans les domaines de l'électromécanique, de la technique des fluides, de l'électronique et de l'électronique programmable, et notamment aussi des systèmes de commande de technologie mixte. Ce texte met en évidence le lien entre la norme et les exigences essentielles de sécurité de la directive Machines, et présente des procédures possibles permettant d'évaluer les risques. Sur la base de ces informations, le rapport permet de sélectionner le niveau de performance PL_r nécessaire pour les fonctions relatives à la sécurité des systèmes de commande. Il explique aussi en détail la manière de déterminer le niveau de performance PL effectivement atteint. Le rapport traite également en détail des exigences à satisfaire pour atteindre le niveau de performance donné et ses catégories correspondantes, de la fiabilité des composants, des taux de couverture de diagnostic, de la sécurité des logiciels et des mesures à prendre contre les défaillances systématiques, ainsi que contre les erreurs de cause commune. Cette offre est complétée par des informations générales concernant la mise en œuvre des exigences dans la pratique de la technique de commande. De nombreux exemples de circuits allant jusqu'au niveau des composants montrent comment les niveaux de performance 'a' à 'e' avec les catégories B à 4 peuvent être réalisés techniquement dans les technologies respectives. Ils fournissent des indications sur les principes de sécurité utilisés et sur les composants techniques qui ont fait leurs preuves en matière de sécurité. De nombreuses références bibliographiques permettent d'approfondir la compréhension des différents exemples. Montrant comment les exigences de la norme DIN EN ISO 13849-1 peuvent être mises en œuvre dans la pratique technique, le rapport contribue ainsi à ce que la norme soit utilisée et interprétée de manière identique, tant au niveau national qu'international.

Resumen

Seguridad funcional de los sistemas de mando de máquinas
– Aplicación de la norma DIN EN ISO 13849 –

La norma DIN EN ISO 13849-1 «Seguridad de las máquinas: partes de los sistemas de mando relativas a la seguridad» establece reglas para el diseño de partes de sistemas de mando relativas a la seguridad. El presente informe es una actualización del informe del mismo nombre del BGIA 2/2008. En él se presentan los contenidos esenciales de la norma en su tercera edición de 2015 y se explica su aplicación con numerosos ejemplos de los ámbitos de la electromecánica, la tecnología de fluidos, la electrónica y la electrónica programable, incluidos los sistemas de mando de tecnologías mixtas. Se muestra la relación de la norma con los requisitos básicos de seguridad de la directiva de maquinaria y se presentan los posibles procedimientos de estimación del riesgo. Sobre la base de estas informaciones, el informe permite seleccionar el nivel de prestaciones requerido (required performance level PL_r) para las funciones de seguridad de los sistemas de mando. Se explica detalladamente cómo de determinar el nivel de prestaciones PL que se ha alcanzado realmente. Se tratan en detalle los requisitos para lograr el nivel de prestaciones en cuestión y sus categorías correspondientes, la fiabilidad de los componentes, los grados de cobertura del diagnóstico, la seguridad del software y las medidas contra fallos sistemáticos así como los errores de causa común. La oferta se completa con informaciones de trasfondo para implementar los requisitos en la práctica de la ingeniería de control. Numerosos ejemplos de circuitos que abarcan hasta el nivel de sus componentes muestran cómo implementar técnicamente los niveles de prestaciones «a» hasta «e» con las categorías B a 4 en las tecnologías correspondientes. Además, se dan indicaciones sobre los principios de seguridad aplicados y los componentes que han demostrado su valía en materia de seguridad. Las numerosas referencias bibliográficas tienen por objeto permitir entender en mayor profundidad los distintos ejemplos citados. El informe muestra cómo se pueden implementar los requisitos de la norma DIN EN ISO 13849-1 en la práctica técnica, contribuyendo así a la homogeneidad de aplicación y de interpretación de la norma a nivel nacional e internacional.

Contents

1 Foreword

The thoroughly revised version of the EN ISO 13849-1 control standard was published nine years ago. BGIA-Report 2/2008e, "Functional safety of machine controls – Application of DIN EN ISO 13849", appeared shortly afterwards and like the preceding report published in June 1997 proved once again to be a best-seller. Since then, over 20,000 orders have been met for copies of the printed German version. The number of downloads from the website of the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) is even higher.

With this report and further tools for application of the standard – the widely used SISTEMA software application, the SISTEMA cookbooks and the disc calculator – the IFA has made an important contribution to successful introduction of the new strategies for assessing and designing the reliability of electronic and programmable control systems. This strategy, which gives consideration to the probabilities of failure of components, is enshrined in the IEC 61508 series of basic safety standards and is now established in almost all sectors of industry, including machine construction. Not least thanks to the close involvement of experienced experts at the IFA, the authors of EN ISO 13849-1 have succeeded in presenting its content and developing it further such that it remains practical in its application, despite the complexity of the subject-matter. The preceding EN 954 standard with its purely deterministic requirements has finally been replaced. The Performance Level is now firmly established in machine construction.

Over the past years, EN ISO 13849-1 has become established worldwide as the definitive standard for machine controls, and further practical experience with it has been gathered. The IFA's experts have commented in publications of their own upon the essential issues concerning application of this standard, and have discussed their opinions on standards committees. The result was the publication in 2015 of the third edition of EN ISO 13849-1.

Now is therefore an appropriate time for a revised IFA Report on safety-related machine control systems.
The team of authors has revised the entire report and all examples. The changes to the standard have also received particular intention and have been interpreted. The present document is the English version of the report.

This report, and the examples of controls that can be imported into SISTEMA, provide all stakeholders with straightforward access to the normative methods that have now become good practice. The report is intended as a tutorial and a reference work. It is not, of course, a substitute for the standard itself. However, it contains valuable advice, and in particular, experience and guidance that has already been developed in the field.

Professor Dr *Dietmar Reinert*
Director of the IFA

2 Introduction

Since 1 January 1995, all machines placed on the market within the European Economic Area have been required to satisfy the essential requirements of the Machinery Directive [1]. In accordance with Article 2 of this directive, a machine is the assembly of linked parts or components, at least one of which moves, with the appropriate actuators, control and power circuits, etc., joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material. In the amended 2006/42/EC [2] version of the Machinery Directive, safety components which are independently placed on the market by manufacturers in order to fulfil a safety function, the failure and/or malfunction of which endangers the safety of persons, and which are not necessary in order for the machinery to function or for which normal components may be substituted in order for the machinery to function, are also included under the term "machinery" in the sense of the directive. The formal definition of "machinery" is also satisfied by interchangeable equipment, certain lifting accessories, chains, ropes and webbing. Detailed explanations of the individual points can be found in the Guide to application of the Machinery Directive 2006/42/EC [2]. The directive now also applies to incomplete machines.

The essential requirements of the Machinery Directive for the design and construction of machines and safety components can be found in Annex I of the directive. In addition to general principles for the integration of safety, this annex contains dedicated subclauses governing controls for machines and the requirements placed upon protective devices. The essential safety requirements applicable to the design of machines and safety components oblige manufacturers to conduct a risk assessment in order to identify any hazards associated with the machine. Three principles are stated, in the following order, by which the accident risks associated with each hazard are to be reduced to an acceptable level:

- The elimination or reduction of risks by inherently safe design
- The taking of necessary measures for protection in relation to risks that cannot be eliminated
- The informing of users of the residual risks, particular training, instruction and personal protective equipment

Under Article 7, the observance of harmonized European standards the reference of which is listed in the Official Journal of the European Union (EU) gives rise to a presumption of conformity with the essential health and safety requirements of the Machinery Directive. Several hundred harmonized European standards detail/support the underlying philosophy set out in Annex I of the Machinery Directive for the attainment of occupational safety and health on machines. EN ISO 12100 [3], a Type A standard now comprising a single part only, governs basic concepts and general principles for design for the safety of machinery. Content of the former EN ISO 14121-1 standard – the full procedure for identifying hazards and for risk estimation and risk evaluation of each individual hazard – has also been incorporated into the new EN ISO 12100 [3] standard. In addition to the standards, the ISO/TR 14121-2:2013 [4] technical report serves as a practical guide to risk assessment, and contains methodical examples.

Based upon the (generic) EN ISO 12100 [3] standard, the updated EN ISO 13849-1:2015 [5] and EN ISO 13849-2:2012 [6] series of standards describes the risk reduction required during the design, structuring and integration of safety-related parts of control systems and protective devices, regardless of whether they are electrical, electronic, hydraulic, pneumatic or mechanical in nature. These standards present a generically applicable system of methods for machine controls and/or their protective devices. The Performance Levels described in the standards extend the concept of Categories familiar from EN 954-1. The safety architectures can now be employed with significantly more flexibility. An essential advantage of EN ISO 13849-1 is its treatment of safety-related parts of control systems independently of the technology employed, as has already been mentioned. The Performance Level enables different control structures employing different technologies to be combined easily. The standard offers everything needed from a single source comprising approximately 100 pages. The methods are formulated neutrally with regard to the specific application or the technology employed, and are therefore referenced by virtually all product standards for machine safety (generally Type C standards).

With entry into force of the revised 2006/42/EC Machinery Directive [2] in December 2009, the harmonized standard acquired greater importance. This can be attributed principally to the new provision that safety-related logic – also described as the safety-related parts of control systems – has been included in Annex IV of the directive. Annex IV products of this kind are subject to special treatment under the directive, unless they are manufactured in accordance with harmonized standards the reference of which is listed in the Official Journal.

On the one hand, Annex IV products are not in principle subject to compulsory EC type examination[1]; they can, for example, be placed on the market on the basis of an extended manufacturer's quality management system assessed by a notified body. However, the new directive resulted in control systems becoming more strongly the focus of the safety analysis [7; 8].

In its third, 2015 edition, EN ISO 13849-1 is the successor standard to EN 954-1:1996 [9], and is already listed in the Official Journal of the EU. The presumption of conformity to which the 2008 version gave rise expired on 30 June 2016. The three-year transitional period in which EN 954-1 remained valid in parallel has long expired; users may therefore use this standard, if at all, only by making dated reference to individual subclauses of it. Part 2 of EN ISO 13849-2 [6] was published in 2012 following revision.

The purpose of the present revised IFA Report is to describe the application of EN ISO 13849 and in particular its practical implementation with reference to numerous model solutions. Particular attention has been attached to the presentation and interpretation of the new or revised requirements set out in the third edition of EN ISO 13849-1. Neither the explanations nor the examples should be regarded as an official national or European comment upon (DIN) EN ISO 13849-1. Rather, the report is a compilation of thirty-five years' experience gained at the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) in the assessment of safety and control equipment employing various forms of technology, and the institute's many years of participation on relevant national and international standards committees.

Chapter 3 deals with the generic standards governing functional safety on machines and machinery installations. Chapter 4 presents an overview of the structure of this report with regard to application of EN ISO 13849.

The authors hope that this report will be of genuine assistance during design and operation activities and will provide OSH experts with firm support in implementing the requirements upon the safety-related parts of control systems. The present interpretation of the standard has been tested in practice in diverse applications, and the principles underpinning the examples have been implemented in technical form in numerous actual cases.

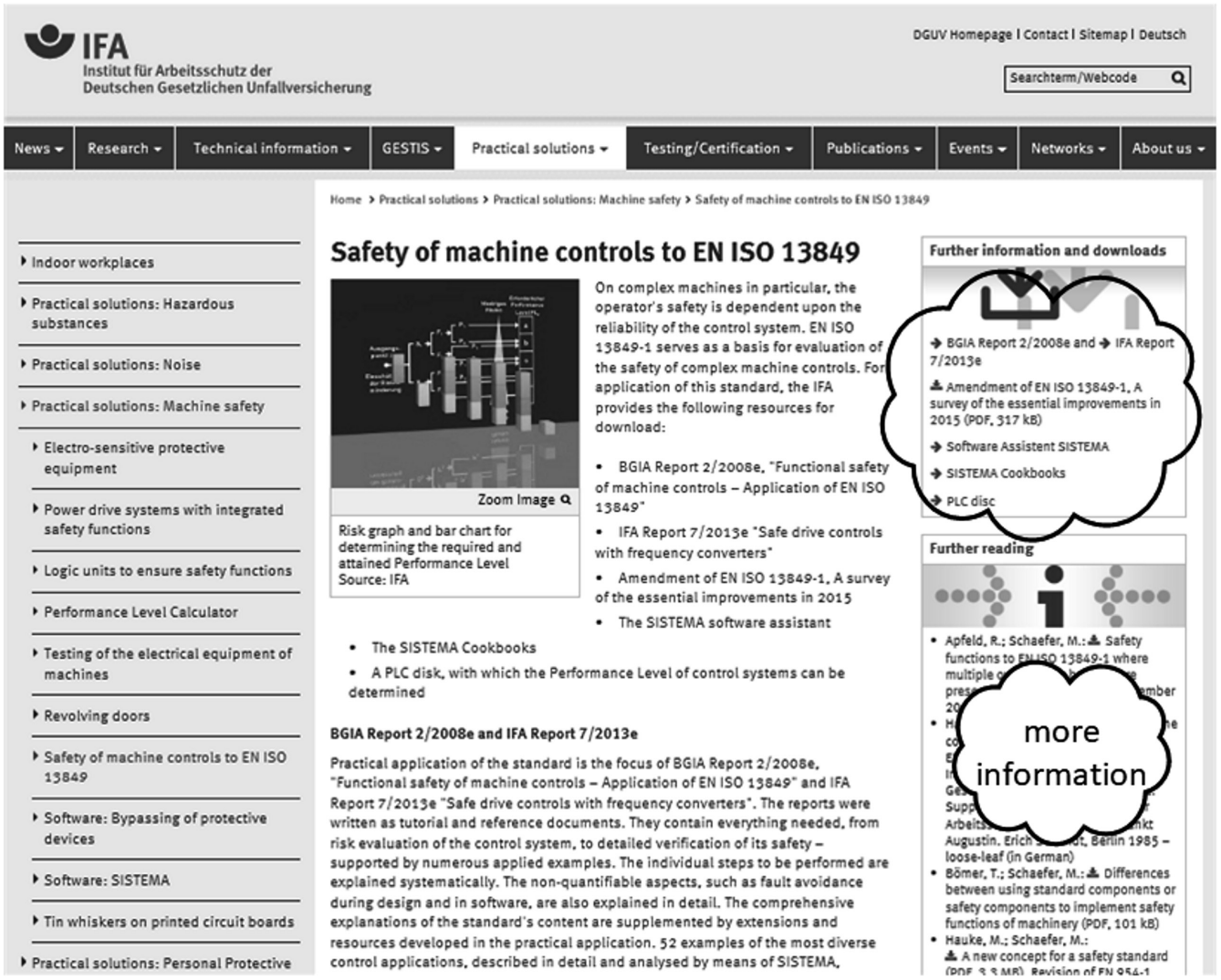
The IFA web page at www.dguv.de/ifa/13849e serves as a portal for the IFA's information on the functional safety of machine controls (Figure 2.1). The free SISTEMA software application (the German acronym "SISTEMA" stands for safety of controls on machinery) is available for download from this portal, as are the SISTEMA project files for the circuit examples shown in Chapter 8. Future extensions are planned to provide up-to-date assistance.

i

For readers already familiar with BGIA Report 2/2008e, a brief summary is provided at the beginning of each chapter of this report of the essential changes with respect to the BGIA Report 2/2008e.

1 As an alternative to EC type examination, the current Machinery Directive enables the manufacturer to perform his own conformity assessment procedure in conjunction with internal production monitoring, in areas in which harmonized standards exist.

Figure 2.1:
This website provides links to all practical tools concerning the safety of machine controls



3 Generic standards concerning the functional safety of machinery control systems

In addition to EN ISO 13849, which is discussed in this report, alternative generic standards of relevance exist in the area of functional safety[2]. As shown in Figure 3.1, these standards are those of the IEC 61508 series [10], and their sector standard IEC 62061 [11] for the machinery industry. Both of these are limited in their scope to electrical, electronic and programmable electronic systems.

A classification system involving "Safety Integrity Levels" (SILs) is set out in IEC 61508 and IEC 62061. The SILs serve as indicators of the level of safety-related reliability. The associated values are target failure measures, each comprising a decade[3]. IEC 61508 distinguishes two different applications of safety functions:

- Safety functions in low demand mode (max. frequency of demands once per year)
- Safety functions in high demand mode or continuous mode

In low demand mode, the dimension for the safety is the average probability of a dangerous failure of a safety function at the point in time of the demand: PFD_{avg}. In the high demand or continuous mode of operation, the average probability of a dangerous failure per hour PFH_D[4] is evaluated by IEC 62061 (for further information, refer also to [12]). With certain exceptions, only the second definition is relevant in the machinery sector and thus in IEC 62061. The new edition of EN ISO 13849-1 has also adopted this definition of the operating mode, and limits the scope of the standard accordingly. SIL 4 systems with higher risks are unknown in the area of machinery, and are not therefore considered in IEC 62061 (Figure 3.2, see Page 16).

The essential approach of the standards governing functional safety (IEC 61508 and IEC 62061) developed by the International Electrotechnical Commission (IEC), namely that of defining probabilities of failure as the characteristic parameter without the specific inclusion of architectures, initially appears more universal. The approach of EN ISO 13849-1, however, offers users the facility for developing and evaluating safety functions, ranging from a sensor to an actuator (e.g. a valve), under the umbrella of one standard, even though the functions may involve different technologies. Part 1 of EN ISO 13849 is accompanied by a Part 2 with the title of "Validation". The present edition, published in 2012, also considers the current

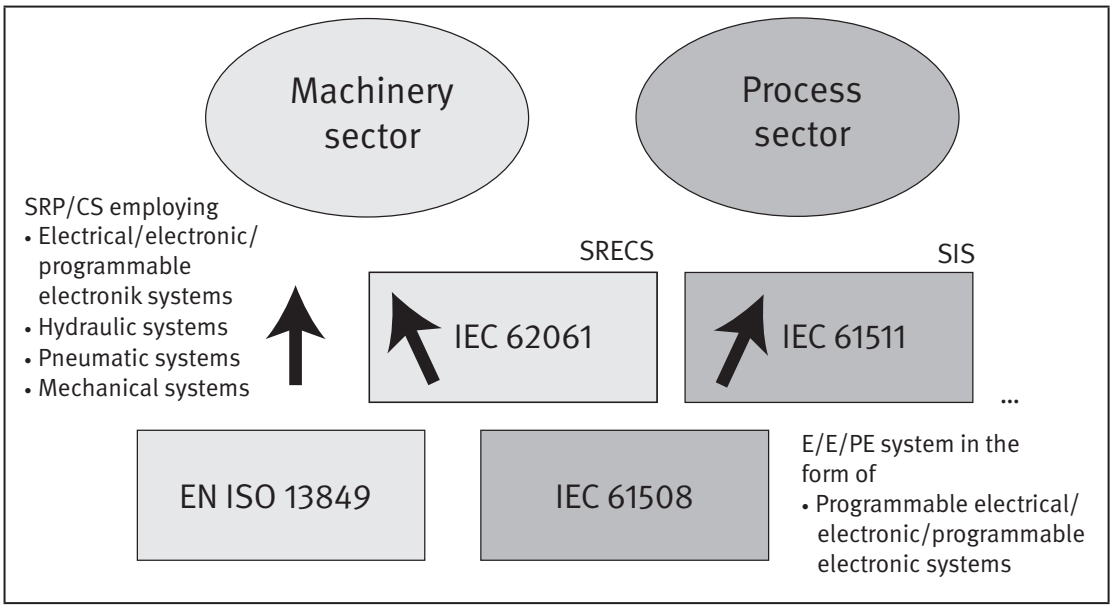


Figure 3.1:
Scope of generic standards governing functional safety; SRP/CS: safety-related part of a control system; SRECS: safety-related electrical control system; SIS: safety instrumented system; E/E/PE system: electrical/electronic/programmable electronic system

[2] In this context, functional safety means that potential hazards that arise as a consequence of failures of a control system, i.e. a malfunction, are dealt with.

[3] In addition, deterministic requirements are imposed that must be satisfied in the level concerned.

[4] In the second edition of IEC 61508:2010 – but not in its sector standard, IEC 62061 – the *PFH* was reformulated as the "average frequency of a dangerous failure of the safety function". The original abbreviation (*PFH*) was however retained (without the "D" suffix in IEC 61508).

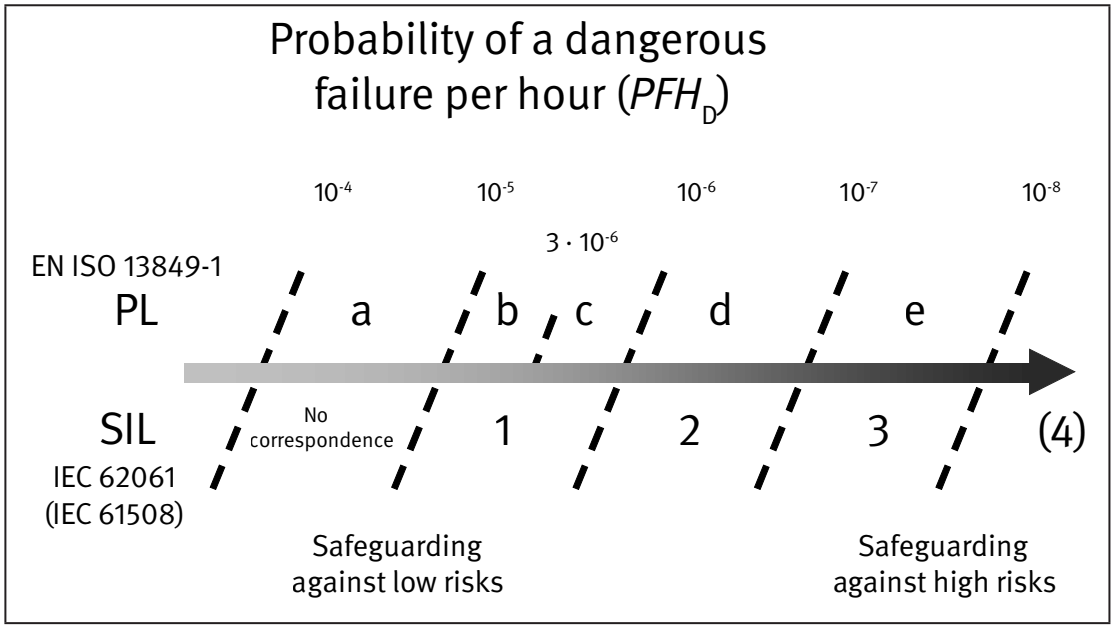


Figure 3.2: The Performance Level (PL) and Safety Integrity Level (SIL) representing the probability of a dangerous failure per hour

topics of Part 1. Annexes A to D of Part 2 contain comprehensive material on the subjects of "basic safety principles", "well-tried safety principles", "well-tried components" and "fault lists". Details can be found in Annex C of the present report.

The apparent overlap in regulatory scope of the two spheres of standardization initially appears unfavourable to manufacturers of control systems and other users of standards. Both EN ISO 13849-1 and IEC 62061 are harmonized standards under the Machinery Directive. Parts 1 to 4 of IEC 61508 have the status of basic safety standards from the IEC perspective (with the exception of simple systems); this series of standards cannot however be harmonized under the Machinery Directive, even as a European standard. This situation prompts for example the following questions:

- What standard(s) should be applied for compliance with the Machinery Directive?
- Where they overlap in their scope, do the standards yield equivalent results?
- Are the classification systems of the standards, such as Categories, Performance Level (PL) and Safety Integrity Level (SIL), compatible?
- Can devices which have been developed in observance of one of the two standards be employed during implementation of a safety function in accordance with a different standard?

For attainment of the greatest possible compatibility with IEC, and if possible to permit merging of the two spheres of standardization in the long term and also to enable the benefits of the probability approach to be exploited without abandonment of the proven Categories, EN ISO 13849-1, as the successor standard to EN 954-1, attempts the balancing-act of uniting both the deterministic approach of the Categories and the aspect of safety reliability with the definition of the Performance Level (PL) (see also [13]). Numerically, corresponding classes (see Figure 3.2) exist which permit rapid preliminary estimations for practical day-to-day use.

In the sense of the standard, the designated architectures are more an optional facility (simplified approach) than a requirement. They should however be regarded as a key element in simplification of the probabilistic approach implemented in EN ISO 13849, and their application is one of the tenets of this report. The scope of IEC 62061 indicates that it also covers complex, e.g. programmable electronics. Although this is correct, the development of "SRECSs" (see Figure 3.1) employing this technology must nonetheless satisfy the requirements of the standard in accordance with IEC 61508. The scope for the use of SRP/CS developed against the standards originating at IEC is emphasized by the new edition of EN ISO 13849-1. This means that such SRP/CS can be considered equally valid when used for the implementation of safety functions under EN ISO 13849-1.

Decisive arguments from the point of view of users in the field for selecting EN ISO 13849 as a basis for the implementation of functional safety in the area of machinery may be considered to be the cross-discipline approach with regard to technology, and the simplified approach to quantification with the use of the designated architectures. This includes the detailed consideration of non-electrical and electromechanical components. Large-volume producers of a safety component, such as a programmable logic controller (PLC) for safety applications, will of course in particular wish to serve other world markets in addition to that of machinery, and will therefore base

their development activity upon IEC 61508 in addition to EN ISO 13849.

The table previously found in identical form in the introductions of EN ISO 13849-1 and IEC 62061 for selection of the appropriate standard for the relevant application has now been deleted from both standards. A guidance document on application of EN ISO 13849-1 and IEC 62061 during the design of safety-related machine controls exists, although it has received little attention. As a sector standard of IEC 61508, IEC 62061 naturally describes the aspect of "management of functional safety" very explicitly. Development and verification of embedded software to EN ISO 13849-1 is based upon the essential requirements for safety-related software that are currently standard practice and are also described in IEC 61508. Broad agreement exists however that requirements from the two standards should not be mixed. The ISO/TR 23849 guidance document [14] was developed by members of both standards committees and was published in 2010 by ISO and IEC. Its core messages are:

- The methods described by the two standards differ, but can attain a comparable level of risk reduction.
- Activities merging the two standards require adequate experience with their application in practice.

The IEC proposed merging of the two standards to form an ISO/IEC standard as long ago as 2011, and began work in 2012. The result of an international survey conducted during work on ISO/IEC 17305 showed clearly that the 13849 standards predominated in application among machine manufacturers and end users. As shown in Figure 3.3, EN ISO 13849-1 was used by 90%, i.e. the great majority of the 715 persons surveyed. Development of the planned ISO/IEC 17305 standard was the subject of heated discussion among experts. The protracted discussions had resulted in the project being at least two years behind its original schedule. The working group was already aware of the essential need to consider backward compatibility to EN ISO 13849-1 and IEC 62061. Straightforward application of the new standard and retention of existing methods were explicit objectives. The question whether a new standard would have met these objectives and whether it would have been able to replace the existing standards cannot be answered. In October 2015, ISO/TC 199 took the decision to abandon the work on a joint standard and to suspend the working group's activities. No sooner had the work officially stopped however, than it became clear that the topic would not rest. Recommendations are therefore to be formulated for whether and if so how a future joint project concerning functional safety could be conducted jointly by the two standards organizations. Both standards will be revised in the near future in the course of "routine maintenance". The results of the work conducted to date on ISO/IEC 17305 will be taken up in both standards.

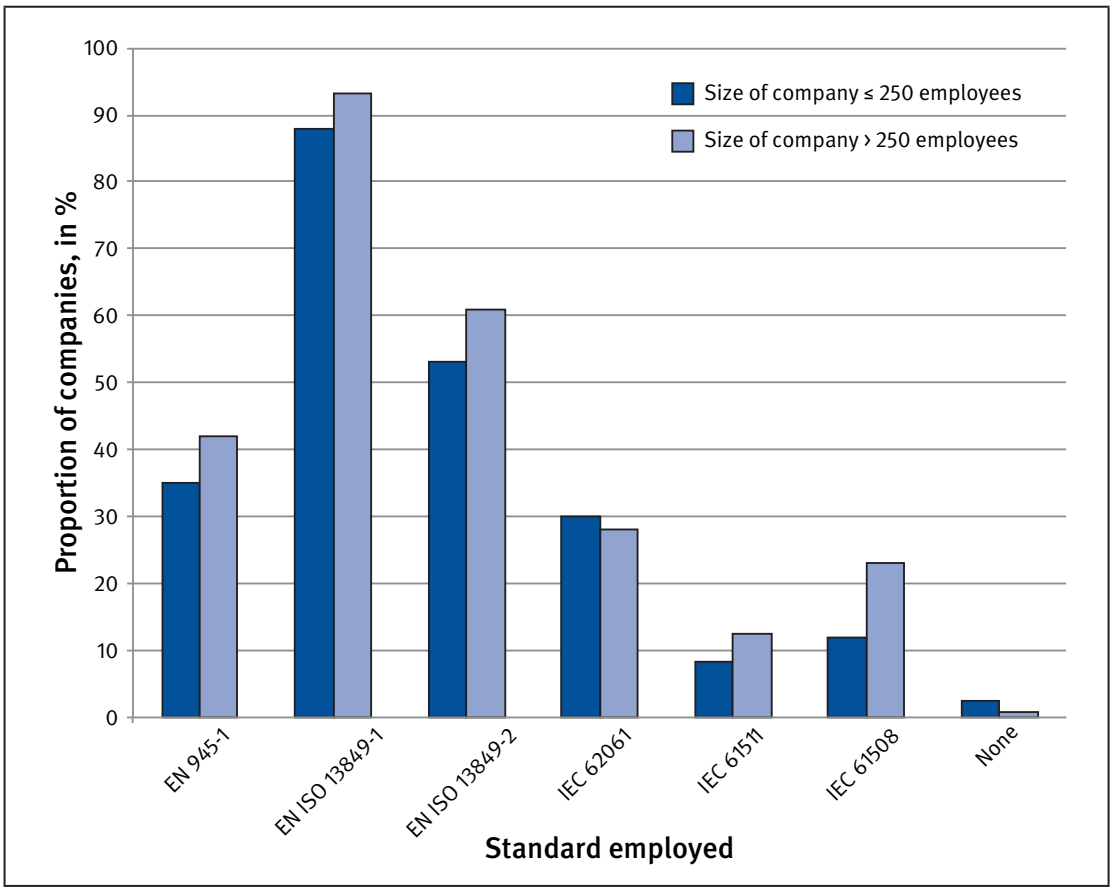


Figure 3.3: Standards used by machine manufacturers and end users as revealed by a survey conducted in 2012/2013 by ISO and IEC into the merging of EN ISO 13849-1 and IEC 62061

4 Report and standard: an overview

Changes with respect to the second edition (BGIA Report 2/2008e):

- References updated
- New subclause 4.4 concerning changes arising from the third edition of the standard, 2015
- Subclause 4.5 (formerly 4.4) concerning future development of the standard updated

This chapter cross-references the further chapters and annexes of this report to the standard. At the same time, it provides an overview of the iterative process for design of the safety-related parts of control systems, based upon Figure 4.1, which corresponds to Figure 3 of the standard. The changes between the second and third editions of the standard, and its future development, are discussed at the end of the chapter.

4.1 Identification of safety functions and their properties

The design and assessment process begins with a well-tried concept, that of the definition of one or more safety functions (SFs). The procedure is shown in Figure 4.1 by blocks 1 to 3, and is described in greater detail in Chapter 5. The question to be answered is: in what way do the safety-related parts of the control system contribute towards reducing the risk of a hazard on a machine?

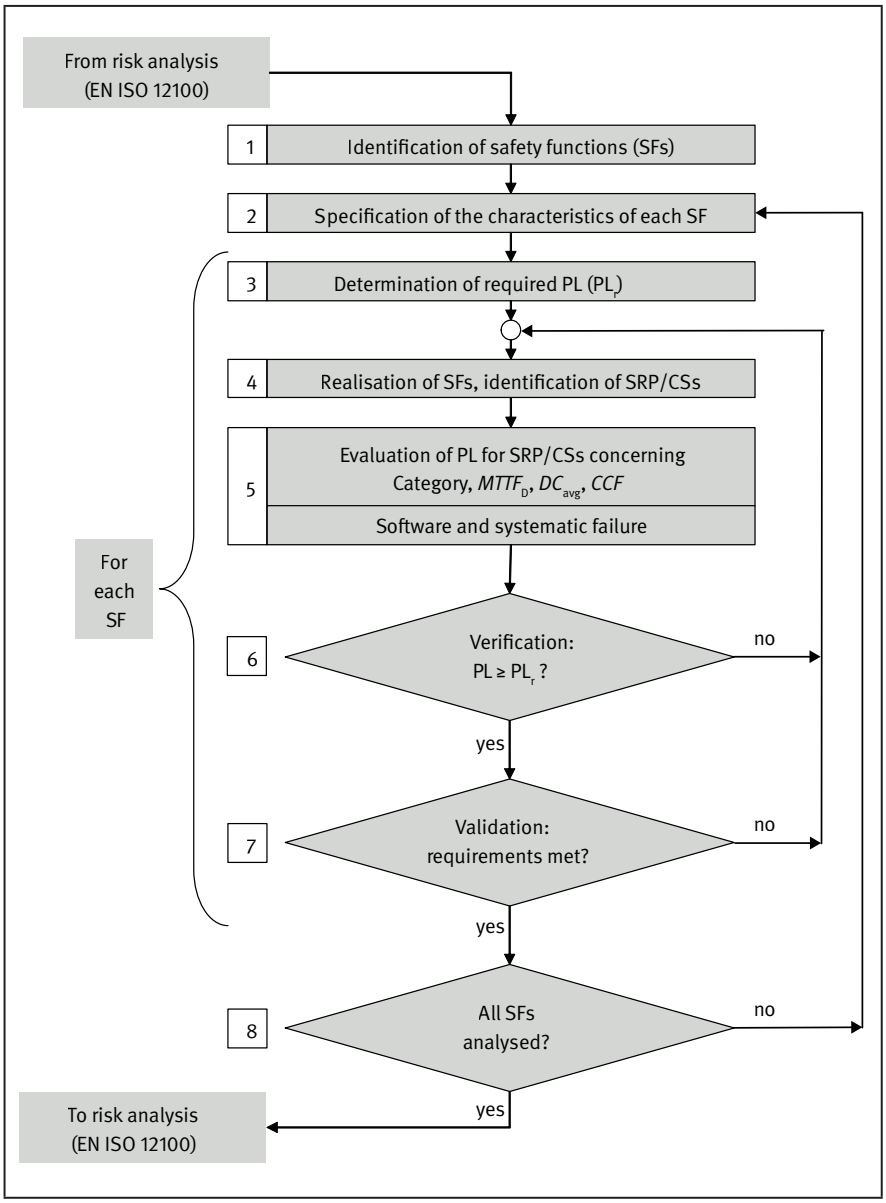


Figure 4.1:
Iterative process for the design of safety-related parts of control systems:
SF = safety function; PL = Performance Level; PL_r = required Performance Level; SRP/CS = safety-related part of a control system; $MTTF_D$ = mean time to dangerous failure; DC_{avg} = average diagnostic coverage; CCF = common cause failure

In the first instance, a machine should be constructed such that it is no longer able to present a hazard in use (inherent safety). The second step is then that of reducing the risk of any hazard that may still arise. This can be attained by protective measures, which often comprise a combination of protective equipment and safe control. In order for these protective measures to attain a defined quality in consideration of the risk, an essential step is that of risk assessment, as required by the Machinery Directive and described in EN ISO 12100 [3]. Protective devices are regarded in the sense of EN ISO 13849-1 (safeguards) together with the safe control as the safety-related part of a control system. Together, they execute a safety function; they may for example prevent unexpected start-up when an operator enters a hazard zone. Since a machine can easily have several safety functions (for example for automatic and setup modes), it is important for careful consideration to be given to each individual hazard and the associated safety function.

The safety function can be assumed by parts of the machine control system or by components required in addition to it. In both cases, these parts are safety-related parts of control systems. Although the same hardware may well be involved in the performance of different safety functions, the required quality of the risk reduction for each SF may differ. In the standard, the quality of the risk reduction is defined by the term "Performance Level" (PL). The result of the risk assessment determines the level of the PL value required for the safety function. This specification for the design of the control system is described as the "required Performance Level", PL_r. How is the PL_r obtained?

The risk of a hazard on a machine can be reduced not only by the control system, but also for example by a guard, such as a guard door, or by personal protective equipment, such as safety goggles. Once it has been established what part is to be played by the protective measures provided by the control system, the required Performance Level PL_r is determined quickly and directly with the aid of a simple decision tree, the "risk graph". Is the associated injury irreversible (e.g. death, loss of limbs), or reversible (e.g. crushing injuries, which can heal)? Is the operator present in the danger zone frequently and for long periods (e.g. more frequently than once every fifteen minutes), or infrequently and briefly? Is the operator still able to avoid an accident (e.g. owing to slow machine movements)? These three questions determine the PL_r. Details can be found in subclause 5.4, examples in Annex A.

4.2 Design and technical implementation of the safety functions

Once the requirements upon the safety-related parts of control systems have been defined, they are first designed, and then implemented. Finally, a verification is conducted to ascertain whether the required risk reduction, the target PL_r value (block 6 in Figure 4.1), can be attained by means of the planned implementation (blocks 4 and 5 in Figure 4.1) with the actual PL value. The steps of blocks 4 and 5 are described in detail in Chapter 6. Following the tradition of the previous control system reports, Chapter 8 of this report also contains a large number of formulated circuit examples for all control technologies and each Category. In addition, the general descriptions contained in Chapters 5, 6 and 7 are accompanied by a comprehensive description of a circuit example (paper cutting guillotine). This provides the developer with an illustrative explanation of the methods and parameters described below.

Safety-related parts of control systems are able to exert their risk-reducing effect only if the safety function was correctly defined from the outset. During the ensuing implementation, quality criteria are applied in the form of the quality of the components employed (lifetime), their interaction (dimensioning), the effectiveness of diagnostics (e.g. self-tests) and the fault tolerance of the structure. These parameters determine the average probability of a dangerous failure per hour (PFH_D) and thus the attained PL. EN ISO 13849-1 places the methods by which the PL is calculated at the user's discretion. Even the highly complex *Markov* modelling method may therefore be used, subject to the parameters stated above. The standard, however, describes a much simplified procedure, namely the use of designated architectures with application of a bar chart (see Page 61, Figure 6.10), in which the modelling of the PL is already taken up. Experts interested in the bar chart's derivation will find it in Annex G.

The Categories continue to be the basis upon which the PL is determined. Their definition remains essentially unchanged since the first edition of the standard; since the second edition however, additional requirements have been imposed upon the component quality and the effectiveness of diagnostics. Adequate measures against common cause failure are required in addition for the Categories 2, 3 and 4 (see Table 4.1).

Table 6.2 (Page 50) provides a summary of the Categories. An essential aspect when the proposed simplified calculation method is used is the presentation of the Categories as logical block diagrams, termed "designated architectures".

Since the Categories require analysis of the faults (avoidance and control of failures), additional aspects concern the reliability of the individual components, their failure modes, and fault detection by automatic diagnostic measures. Fault lists and safety principles serve here as a basis (see Annex C). In addition to the traditional FMEA (failure mode and effects analysis), EN ISO 13849-1 offers

Table 4.1:
Deterministic and probabilistic characteristics of the Categories; probabilistic additions since the second edition of the standard are highlighted in grey

Feature	Category				
	B	1	2	3	4
Design according to relevant standards; withstand the expected influence	X	X	X	X	X
Basic safety principles	X	X	X	X	X
Well-tried safety principles		X	X	X	X
Well-tried components		X			
Mean Time to Dangerous Failure – $MTTF_D$	Low to Medium	High	Low to High	Low to High	High
Fault detection (tests)			X	X	X
Single-fault tolerance				X	X
Consideration of fault accumulation					X
Average diagnostic coverage – DC_{avg}	None	None	Low to Medium	Low to Medium	High
Measures against CCF			X	X	X
Characterized primarily by	Selection of components		Structure		

simplified methods of calculation such as the parts count method. Further explanations of this subject can be found in Annex B.

One of the questions most frequently asked regarding the probability of failure concerns the sourcing of reliable failure data for the safety-related components, the $MTTF_D$ (mean time to dangerous failure) values. The manufacturer of the parts or components, i.e. his technical data sheet, should be given preference here over all other sources. Many component manufacturers already provide such data. Even where manufacturers' data are not available however, typical example values can be obtained from established databases (such as SN 29500 or IEC/TR 62380). The standard and Annex D of this report also list a number of realistic values obtained from the field, and provide information on modelling in the safety-related block diagram.

The effectiveness of diagnostics, in the form of the DC_{avg} value (average diagnostic coverage), can be determined according to the following simple principle: the test measures that monitor the block are compiled for each block. For each of these test measures, one of four typical *DC* values is determined from a table in the standard. An averaging formula, which appears complex but is essentially simple, can be used to calculate the DC_{avg} parameter from it. Further information can be found in subclause 6.2.14 and Annex E.

The final parameter, that of the CCF (common cause failure, subclause 6.2.15), is similarly easy to calculate: for this parameter, it is assumed that a cause, such as contamination, overtemperature or short circuit, can under certain circumstances give rise to several faults which may for example simultaneously disable both control channels. For control of this source of hazard, it must be demonstrated for Category 2, 3 and 4 systems that adequate measures have been taken against CCF. This is achieved by means of a points system for eight typical, for the most part technical counter-measures, with which at least 65 of a possible 100 points must be attained (for details, see Annex F).

The random hardware failures, which can be controlled by a good structure and by low probability of failure, are accompanied by the broad field of systematic faults – i.e. faults inherent to the system since its design, such as dimensioning faults, software faults, or logical faults – against which protection is to be provided by measures for fault avoidance and control. The software faults account for a large proportion of such faults. Since its second edition, the standard has included the requirements upon the safety-related software; individual aspects of them have however long been familiar from relevant standards. The actual measures are graded according to the required PL. Further information can be found in subclause 6.1.2 for systematic failures and in subclause 6.3 for software.

4.3 Verification and validation of the control system for each safety function

If the design has already reached an advanced stage by the time that the achieved PL is determined, the question arises as to whether this PL is sufficient for each safety

function executed by the control system. For this purpose, the PL is compared with the required PL_r (see Block 6, Figure 4.1). If the PL attained for a safety function is inferior to the required PL_r, design improvements on a greater or lesser scale are required (such as the use of alternative components with a superior $MTTF_D$), until an adequate PL is ultimately attained. Once this hurdle has been overcome, a series of validation steps are necessary. Part 2 of EN ISO 13849 comes into play at this point. This validation process systematically assures that all functional and performance requirements placed upon the safety-related parts of the control system have been attained (see Block 7, Figure 4.1). Further details can be found in Chapter 7.

4.4 Changes arising from the third edition of the standard published in 2015

With Amendment 1, the third edition of the standard was produced from the second. The amended passages primarily serve to improve comprehension and application. A detailed overview focusing upon the changes was published by the IFA in 2015 [15]. The essential changes include consideration, during specification of the required Performance Level (PL_r), of the probability of occurrence of a hazardous event; a new, simplified method for determining the PL for the output part of the safety-related part of the control system (SRP/CS); and a proposal for the handling of requirements for SRESW (safety-related embedded software) when standard components are used. Table 4.2 shows which main changes have been made in which subclauses of the standard and of the present report.

The example circuits in Chapter 8 of the report have been thoroughly updated from the 2008 versions based upon the above changes to the standard.

4.5 Future development of EN ISO 13849-1

The third edition of EN ISO 13849-1 replaces the previous edition without a specific transition period. Since the changes – as described in the preceding subclause – essentially concern additions, updating and improvements, however, the transition from the second to the third edition of the standard is not generally critical. As it has done for some time, the IFA is supporting this process with freely available guides to application. These guides take the form both of explanatory reference with examples, and of the "SISTEMA" free software program (the acronym stands for "Safety Integrity Software Tool for the Evaluation of Machine Applications"), which supports calculation and documentation of PL_r and PL (see Annex H). The series of SISTEMA cookbooks, which has been continually extended, is devoted to particular topics that are relevant during application of the standard. These concern not only SISTEMA itself (the SISTEMA libraries, use of network libraries, "Running several instances of SISTEMA in parallel"), but also the entire process of design against the standard ("Definition of safety functions", "From the schematic circuit diagram to the Performance Level", "When the designated architectures don't match"). Finally, the resources include the "Performance Level Calculator"[16] developed by the IFA. This presents the bar chart in the form of a rotating disc by means of which the PFH_D and PL can be determined easily and precisely at any time. All further resources and reference – such as information on the test standards and principles [17] of DGUV Test, the test and certification system of the German Social Accident Insurance – can be found on the IFA's website at: www.dguv.de/ifa/13849.

During work on the third edition of EN ISO 13849-1, several major work packages were identified that lay outside the scope of an amendment. These included, for example, thorough revision of the software requirements, in order to improve its suitability for application in practice, and also consistent precision of when "SRP/CS" refers to the entire control system executing a safety function, and when to a subsystem that executes only a part of the safety function. In order for these proposals to be implemented in the longer term, the committee responsible for the standard decided as early as 2016 , following publication of the third edition, to begin work on a revision of the standard. The IFA will support this activity as it has done effectively in the past, in order for the anticipated results (possibly in the form of a fourth edition of the standard) once again to be prepared for practical application as described above.

Table 4.2:
Essential changes in the third edition of the standard and the affected subclauses of the standard and of the present report

Section of the standard	Change	Section of the report
1 Introduction	Replacement of Table 1, "Recommended application of IEC 62061 and ISO 13849-1", by a reference to ISO/TR 23849	3 Generic standards concerning functional safety
2 Scope	The standard applies to SRP/CSs with high demand and continuous mode	3 Generic standards concerning functional safety
3 Terms, definitions, symbols and abbreviated terms	Abbreviation PFH_D for the average probability of a dangerous failure per hour	Throughout
	$MTTF_D$, B_{10D}, T_{10D} and λ_D with the "D" suffix in capitals	Throughout
4 Design considerations (and Annex K)	Updating of the references to ISO 12100:2010	5 Safety functions
	Combination with subsystems in accordance with other standards governing functional safety	6.4 Combination of SRP/CSs
	$MTTF_D$ capping for Category 4 increased to 2,500 years	6.2.13 FMEA versus the parts count method
	Test frequency and $MTTF_D$ of the test channel in Category 2	6.2.5 Category 2 and 6.2.14 Diagnostic coverage
	Alternative determining of the PFH_D for the output part of the SRP/CS in accordance with Section 4.5.5 of the standard	6.2.17 Determining of the PL for the output part of the SRP/CS
	Requirements for SRESW when standard components are used	6.3.10 Requirements for the software of standard components
5 Safety functions	Consideration of loss of power with possibly separate safety function	5 Safety functions
6.2 Categories	Warning of the hazard as an alternative to initiation of a safe state in Category 2 up to a PL_r of c	6.2.5 Category 2 and 6.2.14 Diagnostic coverage
6.3 Combination	Combination of SRP/CSs: Addition of PFH_D as the preferred method	6.4 Combination of SRP/CSs
Annex A, Determation of the PL_r	Emphasizing of the informative character	5 Safety functions, Annex A, examples
	Distinction between F1 and F2	5.4.1 Risk graph
	Probability of occurence of a hazardous event	5.4.1 Risk graph
	Overlapping hazards	5.3.2 Examples in which the definition of the safety function has an influence upon subsequent calculation of the PFH_D
Annex C, $MTTF_D$	Amendment of selected typical values in the good engineering practice method	Annex D, $MTTF_D$
Annex E, *DC*	Two *DC* measures deleted "Fault detection by the process" described in more detail	Annex E, *DC*
Annex I, Examples	Updating	Not relevant

5 Safety functions and their contribution to risk reduction

Changes with respect to the second edition (BGIA Report 2/2008e):

- References to standards updated
- "Overlapping hazards" included
- Information on the F1/F2 distinction updated
- Consideration for the "probability of a hazardous event occurring" inserted
- Subclause 5.4.2, "Transition from a required Category in accordance with EN 954-1 to a PL_r" deleted
- Example of a paper cutting guillotine revised

This Report deals with safety functions and their contribution to reducing risks in hazard zones on machinery. The design of such safety functions is part of a process for the design of safe machines. This chapter therefore begins by addressing the requirements of the Machinery Directive, before describing the definition of safety functions and their properties. Subclause 5.7 then demonstrates implementation with reference to the practical example of a paper cutting guillotine control.

5.1 Requirements of the EC Machinery Directive

The EC Machinery Directive [2] has been transposed into German law by the German Product Safety Act (ProdSG), and sets out essential health and safety requirements for machines. The general provisions of the Machinery Directive are supported by standards. Particularly significant in this respect is EN ISO 12100 [3], Safety of machinery –General principles for design. The machine designer is presented with a design method that is suitable for achieving machine safety. This method – a strategy for risk reduction – includes the design of safety-related parts of control systems[1].

Provided a harmonized product-specific standard (Type C standard) exists for the machine being designed and the reference of this standard has been published in the Official Journal of the EU [18], it may be assumed that the essential health and safety requirements are satisfied. In such cases, the standard is said to give rise to a "presumption of conformity", since its application justifies the assumption that the machine satisfies the requirements of the EC Machinery Directive. The strategy for risk reduction must however always be followed where a standard giving rise to the presumption of conformity does not exist, where a suitable standard exists but the design has deviated from it, or where additional aspects apply that are not covered by the product standard. In order for issues not covered by a product standard to be identified, the first two steps in the risk reduction strategy described below must always be performed, i.e. the limits of the machinery must be defined and the hazards identified.

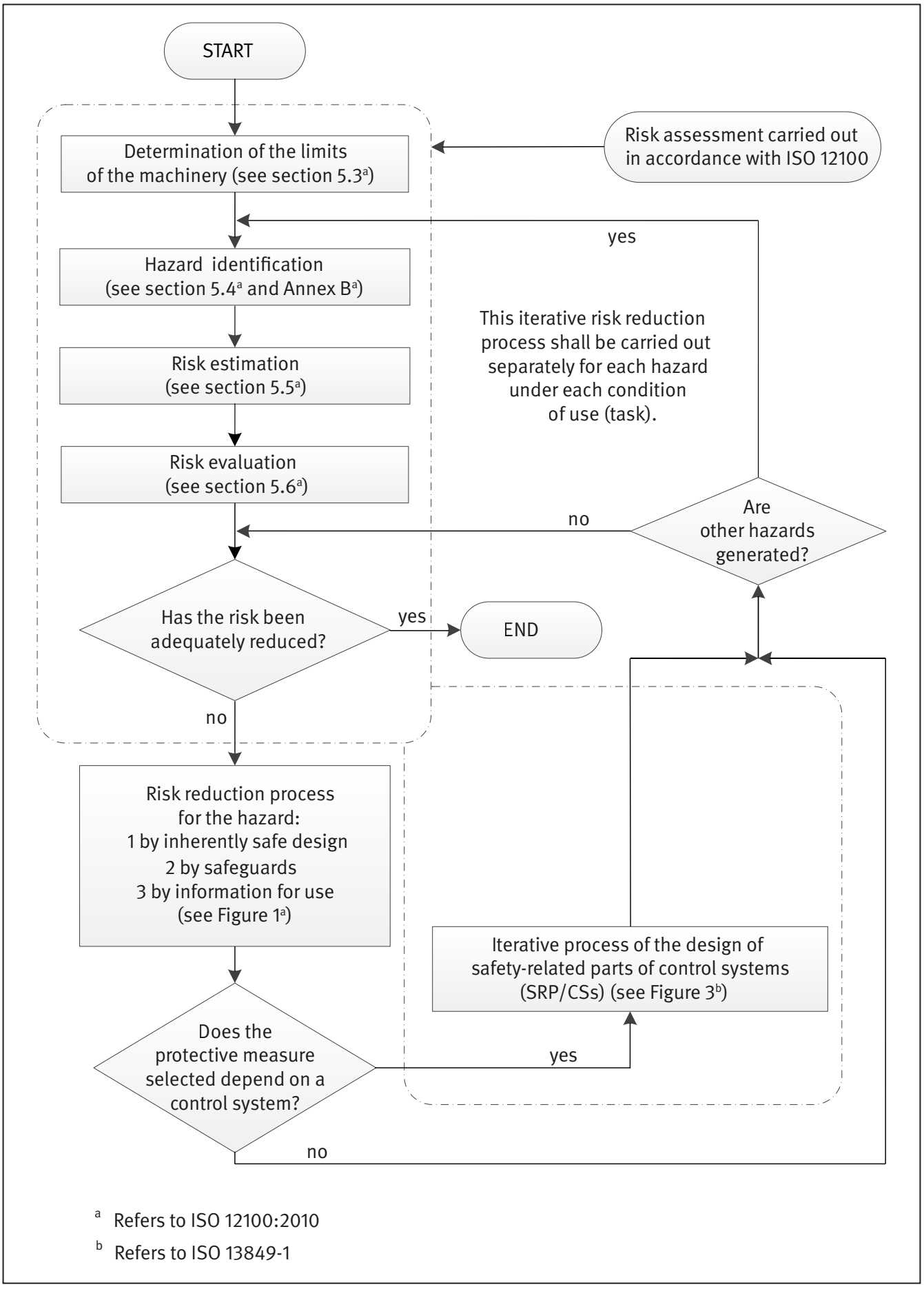
5.2 Risk reduction strategy

The risk reduction strategy presented in EN ISO 12100 [3] was adopted in Figure 1 of EN ISO 13849-1 and supplemented with the aspects detailed in the latter standard (see Figure 5.1). A risk assessment is first performed. An important point is the assumption during the following steps that no protective measures have as yet been taken on the machine. Ultimately, the entire risk reduction process serves to determine the type and also the "quality" of the protective measure/safeguard that is to be implemented.

The risk reduction process begins with definition of the limits of the machine. Besides the space limits and time limits of the machine, attention must be paid in particular to its use limits. Such limits include the intended use of the machine (e.g. materials which may permissibly be machined on it), including all operating modes and the various intervention procedures. Reasonably foreseeable misuse of the machine must also be considered; this includes consideration for the defeating of safeguards.

[1] Safety-related parts of control systems are one means by which a safety function is implemented. The starting-point for these systems is the reception of safety-related input signals, for example detection of the position of a guard door by means of a Type 2 position switch, the separate actuator of which is fitted to the door and itself constitutes a safety-related part. Once received, the signals are processed, leading to generation of an output signal.

Figure 5.1:
Iterative risk reduction process



[a] Refers to ISO 12100:2010

[b] Refers to ISO 13849-1

The hazards are then identified; all phases of the machine's lifetime must be considered in this process. In addition to automatic mode, particular attention is paid to operating modes requiring manual intervention, e.g. for:

- Setting
- Testing
- Teaching/programming
- Commissioning
- Material charging
- Retrieval of the product
- Troubleshooting and fault clearance
- Cleaning
- Maintenance

Further details of this process step can be found in EN ISO 12100 [3]. A range of methods exist for systematic identification of the hazards; examples can be found in ISO/DTR 14121-2 [4]. Possible hazards are also listed extensively in EN ISO 12100 [3]. Figure 5.2 shows an excerpt.

5.2.1 Risk estimation

Once all potential hazards which may be presented by the machine have been identified, the risk must be estimated for each hazard. The risk associated with a particular hazardous situation can be determined from the following risk elements:

a) Severity of harm

b) Probability of this harm occurring as a function of:
   – Exposure of a person/of persons to the hazard
   – A hazardous event occurring
   – The technical and human possibilities for avoidance or limitation of the harm

The objective of the further procedure is to reduce the risk to an acceptable level. For this purpose, Figure 5.3 shows the proportions of risk reduction with and without safety-related parts of a control system. Further information on the subject of risk can be found in the IFA Manual [19].

5.2.2 Risk evaluation

Following the risk estimation, a risk evaluation is performed in order to determine whether a risk reduction is necessary. The criteria for adequate risk reduction are specified in EN 12100 [3]:

- Have all operating conditions and all intervention procedures been considered?
- Have hazards been eliminated by suitable protective measures or the risks reduced to the lowest practicable level?
- Has it been ensured that the measures taken do not give rise to new hazards?
- Have the users been sufficiently informed and warned concerning the residual risks?
- Has it been ensured that the protective measures taken do not adversely affect the operators' working conditions or the usability of the machine?
- Are the protective measures taken compatible with one another?
- Has sufficient consideration been given to the consequences that can arise from the use in a non-professional/non-industrial context of a machine designed for professional/industrial use?

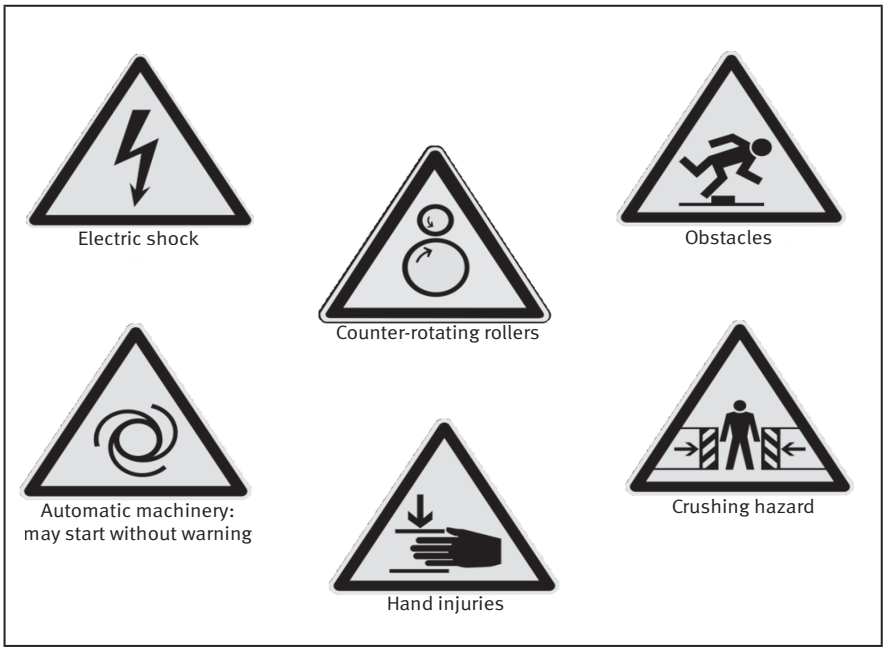


Figure 5.2:
Examples of hazards (source: German Social Accident Insurance Institution for the food stuffs and catering industry)

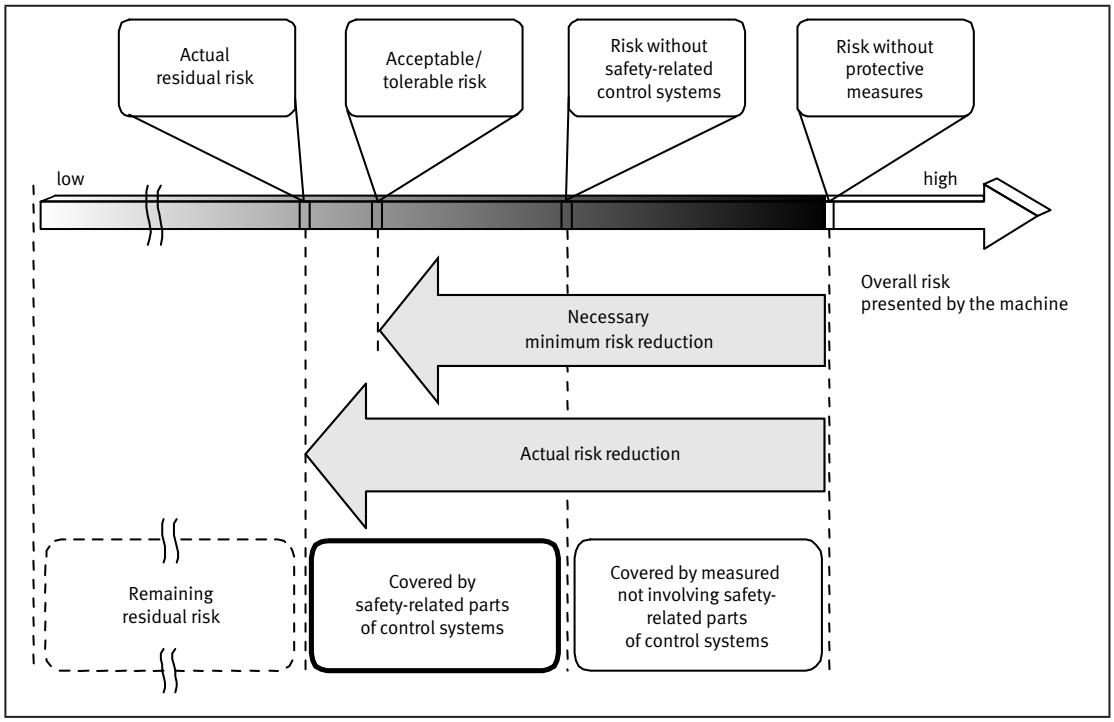


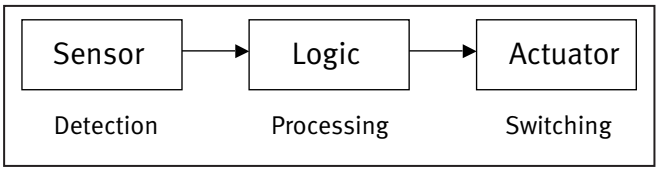
Figure 5.3:
Risk estimation and risk reduction

5.3 Identification of the required safety functions and their properties

Should the evaluation identify an (as-yet) unacceptable risk, appropriate safeguards must be provided. Priority is however to be given to efforts by which hazards are avoided (inherently safe design), or at least reduced to the greatest possible extent, by design modifications to the machine. In principle, information for use (including organizational measures) is also a possible means of risk reduction. Measures of this kind are acceptable however only in exceptional cases in which an economically reasonable risk reduction by means of technical protective measures is not possible; in the majority of cases, safeguards will however be required. In this context, safety functions are defined that are executed by the SRP/CS (safety-related parts of control systems) (see Figure 5.4).

An iterative process for design of the safety-related parts of control systems is set out in [5] (Figure 4.1). Figure 5.5 shows the part relevant to this subclause of the report.

Figure 5.4:
Safety functions are executed by SRP/CS



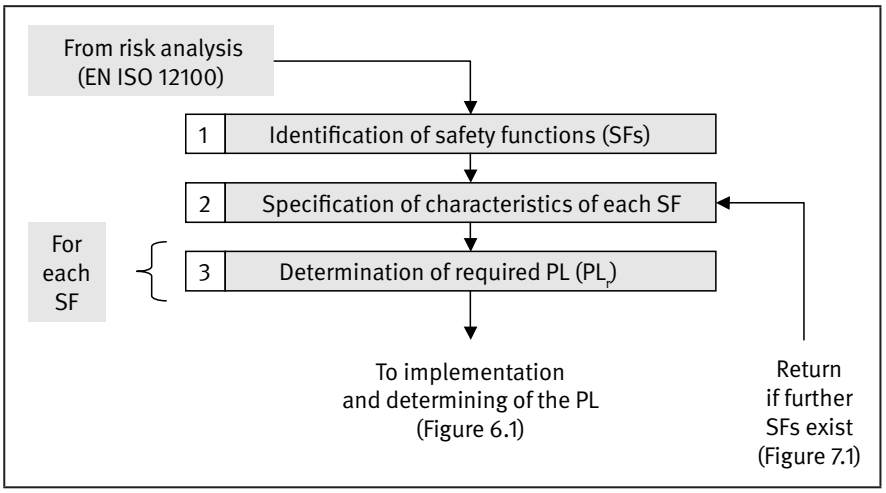


Figure 5.5:
Excerpt from the iterative process for the design of the dafety-related parts of control systems (SRP/CS)

5.3.1 Definition of safety functions

The necessary safety functions are defined in consideration of both the application and the hazard. For example, if flying debris must be anticipated, a light curtain will be an unsuitable solution, and an arrester (guard) will be required. A safety function is therefore a function by which measures (including measures in the control technology) reduce the risk presented by a particular hazard to an acceptable level. In the absence of relevant provisions in a Type C standard, the safety functions are defined by the designer of the machine, e.g.:

a) Controlled stopping of the movement and application of the holding brake in the rest position

b) Prevention of a crushing point being caused by descending machine parts

c) Reduction of the power of a cutting laser where the eye is directly exposed

d) Prevention of dropping of the shaft in setup mode

e) Evasion of the robot when a person enters its danger zone

f) Prevention of entrapment of persons

g) Stopping of the closing movement controlled by two-hand operation in the event of intervention in the danger zone by a second person (initiated by means of a light curtain)

Compound safety functions are frequently employed, as in the example in subclause 5.7. The movement is initially braked to a halt by the electronic drive, after which a mechanical holding brake is applied. The two tables below provide information on possible safety functions. Table 5.1 summarizes the safety functions according to subclause 5.1 of EN ISO 13849-1 and adds examples of possible applications. The “emergency stop function” is also included: though not part of a safeguard, it is used for implementation of a complementary protective measure (see subclause 5.5). Table 5.2 shows further safety functions for safe power drive systems to IEC 61800-5-2 (PDS/SR, power drive systems/safety related) [20]. The scope of this standard includes the safety functions frequently employed for prevention of unexpected start-up (safe torque off, STO), for safe stop SS1 and SS2 and for safely-limited speed (SLS).

Safety functions for pneumatic drive technology are described in VDMA Technical Rule 24584 [21].

Table 5.1:
Safety functions described in EN ISO 13849-1

Safety function	Example application
Safety-related stop function, initiated by a safeguard	Response to tripping of a protective device with STO, SS1 or SS2 (Table 5.2)
Manual reset function	Acknowledgement when areas behind the protective device are vacated
Start/restart function	Permissible only with interlocking guards with start function to EN ISO 12100
Local control function	Control of machine movements from a location within the hazard zone
Muting function	Temporary deactivation of safeguards, e.g. during material transport
Hold-to-run equipment (inching switch)	Machine movements controlled from a position within the hazard zone, e.g. during setup
Enabling function	Machine movements controlled from a position within the hazard zone, e.g. during setup
Prevention of unexpected start-up	Manual operator intervention in hazard zones
Escape and rescue of trapped persons	Separation of rollers
Isolation and energy dissipation function	Opening of a hydraulic valve for pressure release
Control modes and operating mode selection	Activation of safety functions by an operating mode selector switch
Function for stopping in an emergency	Response to actuation of an emergency-stop device with STO or SS1 (Table 5.2)

Table 5.2:
Safety functions described in IEC 61800-5-2 (2016 edition) [20]

Abbreviation	Description	Function
STO	Safe torque off	Motor not receiving energy capable of generating rotary movement; stop category 0 to EN 60204-1
SS1-r SS1-t	Safe stop 1	Motor decelerating; monitoring of deceleration ramp and STO following standstill (SS1-r), or STO following a timeout (SS1-t); stop category 1 to EN 60204-1
SS2-r SS2-t	Safe stop 2	Motor decelerating; monitoring of deceleration ramp and SOS following standstill (SS2-r), or SOS following a timeout (SS2-t); stop category 2 to EN 60204-1
SOS	Safe operating stop	Motor is stationary and resisting external forces
SLA	Safely-limited acceleration	Violation of an acceleration and/or deceleration limit value is prevented.
SLS	Safely-limited speed	Exceeding of the speed limit value is prevented.
SLT	Safely-limited torque	Violation of a torque/force limit value is prevented.
SLP	Safely-limited position	Exceeding of a position limit value is prevented.
SLI	Safely-limited increment	The motor is moved a specified incremental distance, after which it stops.
SDI	Safe direction	The motor is prevented from running in the undesired direction.
SMT	Safe motor temperature	Exceeding of a motor temperature limit value is prevented.
SBC	Safe brake control	Safe actuation of an external brake.
SCA	Safe cam	A safe output signal is generated as long as the motor position remains within a specified range.
SSM	Safe speed monitor	A safe output signal is generated as long as the motor speed remains below a specified value.
SAR	Safe acceleration range	The acceleration of the motor is kept within specified limit values.
SSR	Safe speed range	The speed of the motor is kept within specified limit values.
STR	Safe torque range	The torque of the motor (the force in the case of linear motors) is kept within specified limit values.

The manner in which a safety function is executed may take very different forms. For this reason, certain characteristics must be observed at selection, and specified on a case-by-case basis. These include:

- Use in different operating modes (e.g. automatic mode, setup mode, troubleshooting)
- Use of different safety functions according to whether the power supply is available or has failed (see also subclause 4.3 of [22])
- Response(s) to tripping of the safety function
- Response(s) to detection of a fault in the safety function
- Response time
- Frequency of actuation
- Priority, in cases where several safety functions may be active simultaneously
- Specification of safety-related parameters, such as the maximum permissible speed
- Required Performance Level PL_r

Detailed information on the definition of safety functions can be found in SISTEMA Cookbook 6, “Definition of safety functions: what is important?” [23].

5.3.2 Examples in which the definition of the safety function has an influence upon subsequent calculation of the PFH_D

Later chapters will show how the average probability of a dangerous failure per hour (PFH_D) can be calculated for a safety function. The foundation for this is however laid at this stage, with definition of the safety function. By its nature, the technical implementation of a safety function determines the type and scale of the components required for it. The definition of the safety function thus has a considerable influence upon determination of the

safety-related reliability. This will be explained in the following examples.

Example 1:
Safety function "Stopping when the guard door is opened"

When the guard door is opened, a machine operator has access to a danger zone in which five drives control the movements of machine parts. Opening the guard door causes all five drives to be brought to a halt as quickly as possible.

When the PFH_D of the safety function is calculated later, the PFH_D values of the following blocks[2] are therefore added:

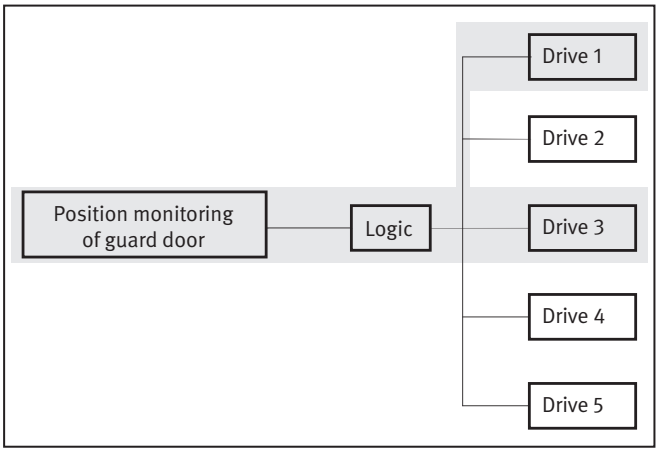
- Position monitoring of the guard door, including mechanical components
- Logic
- Drives 1 to 5

The calculation may yield a PFH_D that is no longer adequate for the application, even though it may be that only drives 1 and 3 initiate hazardous movements at the instantaneous location of the operator, and the remaining drives are halted purely "functionally". In this case, it is recommended that only the movements actually presenting a hazard be considered for the purposes of the safety function, and that the safety function be reformulated in consideration of the drives critical to the operator's safety. The associated functional diagram is shown in Figure 5.6.

If more than one drive is involved in the hazardous movements in the danger zone under consideration, the hazards are considered overlapping. If the number of drives to be considered is too high, the sum of the PFH_D values of the individual drives may once again be a total PFH_D that is too high for the required PL of the safety function. The revised standard makes provision for consideration of overlapping hazards. Accordingly, the hazards considered in the safety function in question can under certain circumstances be reduced to discrete hazards, i.e. the hazardous machine movements can be reduced to the movements of discrete parts of the machine. Whether this is possible in a given case must be determined during the risk assessment. Assistance in this context is provided by Annex J of the present report and by [24].

[2] Possible faults in the electrical system are assigned to the relevant blocks.

Figure 5.6:
Stopping of drives 1 and 3 when the guard door is opened



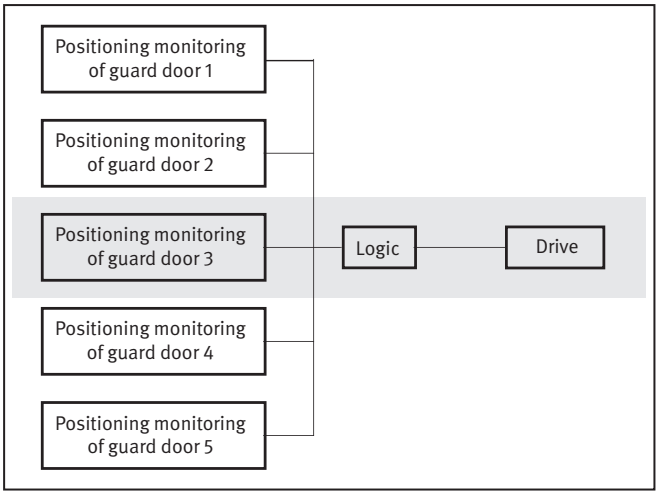
Example 2:
Safety function "Stopping of the drive when a guard door is opened"

A hazardous movement is safeguarded by a fence with five guard doors. Opening any of the doors halts the movement. Since a person will only ever open one of the guard doors at once, each door constitutes a safety function in its own right, SF1 to SF5, which is composed of the following blocks:

- Position monitoring of the guard door x (x = 1, 2, ... 5), including mechanical components
- Logic
- Drive

Figure 5.7 shows the functional diagram and blocks of the safety function SF3.

Figure 5.7:
Stopping of the drive when guard door 3 is opened



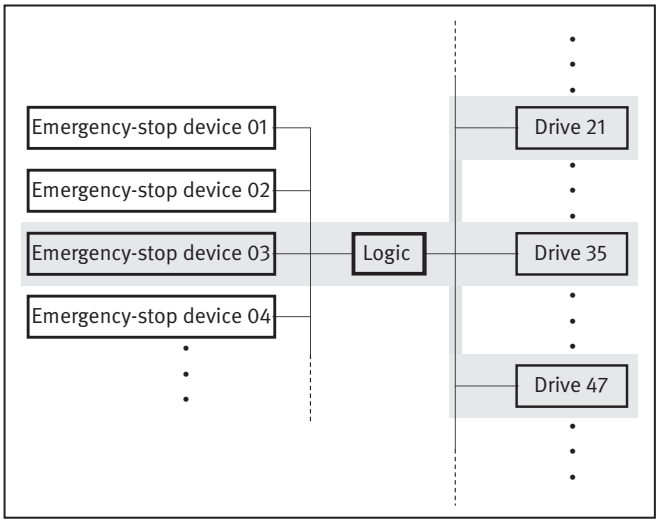
Example 3:
Safety function "Stopping of all drives when the emergency-stop device is actuated" (see subclause 5.5)

Twenty emergency-stop devices are installed on a larger machine; when actuated, they bring all 50 drives to a halt as rapidly as possible. What components must be considered in this case during implementation of the safety function? It cannot be predicted which of the emergency-stop devices will be actuated in order to initiate the safety function. Since the user only ever actuates one emergency stop device at any one time, safety functions SF1 to SF20 are defined. The location of a person exposed to a hazard at the time the emergency stop is initiated is not known. Regardless of where this person is located however, not all 50 drives present a hazard. The worst case should therefore be considered representative for all conceivable situations. The worst case is determined by the worst PFH_D, and is therefore partly dependent upon the number of drives in the safety chain that generate hazardous movements at the least favourable location, and upon the respective individual PFH_D values. The associated block diagram is shown in Figure 5.8.

The PFH_D values of the following blocks must therefore be taken into account during subsequent calculation of the PFH_D of the safety function:

- Emergency stop device 03
- Logic
- Drive 21
- Drive 35
- Drive 47

Figure 5.8:
Emergency stop of the entire machine, worst case



The examples show the advantage of a "local approach" for definition of a safety function, in which the following are considered:

- At what location are persons present at the point in time under analysis?
- What movements present hazards at the location of the person(s)?
- What safeguards initiate the safety function at the point in time under analysis?

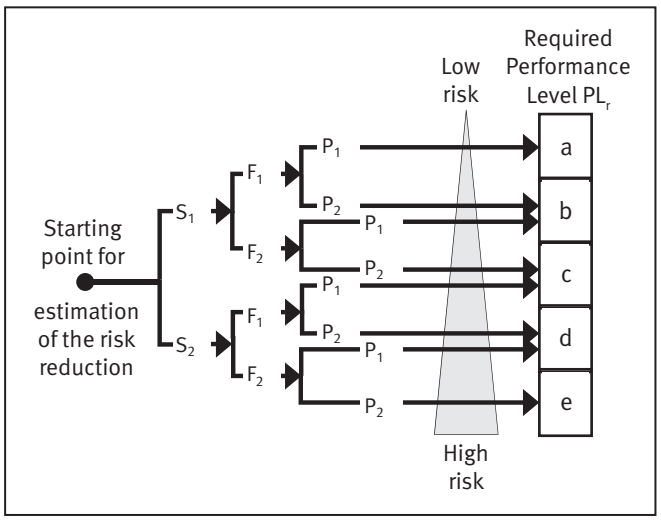
5.4 Determining of the required Performance Level PL_r

A required Performance Level PL_r – in technical terms, the desired value – must be specified for each implemented safety function[3]. The requirements are derived from the necessary risk reduction. During definition of the risk reduction, consideration must also be given to the likelihood and severity of accident, which may not be known. ISO/TR 14121-2 [4] describes methods for determining the required scale of the risk reduction. EN ISO 13849-1 employs one of these methods, that of the risk graph.

5.4.1 Risk graph

The diagram in Annex A of the standard leads directly to the required Performance Level PL_r and is explained below (see Figure 5.9). Further examples of determining of the PL_r can be found in Annex A.

Figure 5.9:
Risk graph for determining the PL_r for each safety function



[3] The r (required) suffix indicates that the Performance Level in this case is that required for the safety function (desired value). Validation at a later stage examines whether the PL attained by the actual control system (actual value) is greater than or equal to the PL. In this context, "greater than" means: PL = e › PL = d › PL = c › PL = b › PL = a

From the starting-point, the following risk parameters are evaluated[4]:

- S – severity of injury
- F – frequency of and/or duration of exposure to hazard
- P – possibility of avoiding the hazard or of limiting the harm

The risk graph thus leads to the necessary PL_r. This analysis must be performed for each safety function and without consideration of the risk reduction that is achieved as a result. Where other technical measures are in place that are implemented independently of the control system, such as a mechanical guard or further safety functions, they can be assumed to be effective for the purpose of determining the PL_r.

Severity of injury S1 and S2

Generally, the severity of injury (parameter S) in a hazard zone will be found to vary widely. For the requirements upon the control system however, only the following distinction is relevant:

- S1 – slight (normally reversible injury)
- S2 – serious (normally irreversible injury or death)

The usual consequences of accidents and the normal healing processes must be taken into account for determining between S1 and S2.

Frequency of and/or exposure to the hazard F1 and F2 (parameter F)

The frequency of and/or exposure to the hazard are evaluated as:

- F1 – seldom to less often, and/or exposure time is short
- F2 – frequent to continuous, and/or exposure time is long

Consideration is therefore given both to the number of interventions in the danger zone within a period and to the duration of presence within it. The standard assists decision-making by stating that where operator interventions occur more frequently than once every 15 minutes, F2 should be selected. In all other cases, F1 is the correct choice, provided the duration of hazard exposure does not exceed 1/20 of the total operation time of the machine. During evaluation, an average value should be considered for the duration of the hazard exposure in relation to the overall time for which a machine is in use.

For a manually charged metalworking press whose operator must reach cyclically between the dies of the press, F2 is clearly the appropriate choice. Conversely, for a machining centre that is set up once each year and then operates automatically, F1 will doubtless be selected. For evaluation of the frequency and duration of exposure to the hazard, cases in which the same person or different persons are exposed must be treated in the same way.

P – possibility of avoiding the hazard P1 and P2 (parameter P)

At this point, an evaluation must be made of whether recognition and avoidance of a hazardous situation is:

- P1 – possible under specific conditions
- P2 – scarcely possible

Aspects relevant to definition of this parameter include the physical characteristics of a machine, the qualifications of the operator, and their possible reaction. If, for example, the machine must be set up whilst running at limited speed, the parameter P1 will be the correct choice at the low acceleration values for setup: with the slow emergence of the hazards and given sufficient freedom of movement, the operator will be able to move out of the hazard zone. Conversely, P2 must be selected when higher speeds may rapidly be reached and the operator has no realistic chance of evading an accident. During this evaluation, consideration should be given only to hazard limitation by physically possible means, and not to limitation by control components, since the latter could fail in the event of a fault. For example, rollers moving in the direction of the operator‘s hand cannot entrap it under fault-free conditions. In the event of a control-system fault, however, the direction of rotation could be reversed, and under worst-case conditions, the hand would be drawn in.

A further factor influencing determining of the PL_r is the probability of the occurrence of a hazardous event ([3], 5.5.2.3.2). Human behaviour and technical failure may be factors in this context. Both are difficult to estimate numerically. The standard states the following example criteria however:

- Reliability data
- History of accidents on comparable machines

[4] The probability of a hazardous event occurring is analysed in conjunction with the risk parameter P.

Where factors exist that enable the probability of a hazardous event occurring to be deemed "low", the PL_r may be reduced by one level; it must however not drop below PL a.

What reasoning may now be given for a "low" ranking? Consideration of reliability data refers (among other aspects) to the process-related (i.e. not safety-related) control system. The machine manufacturer must therefore assess for this purpose whether high reliability of the components (high *MTTF*, in this case without "D") can also be assumed for his machine. How great is therefore the probability for example that a standard PLC for functional control of a machine will incorrectly initiate unexpected start-up of a drive? How should new components be evaluated that have good *MTTF* values but with which practical experience has not yet been gained? Are the conditions of use of PLCs and associated components (sensors, frequency inverters, power supplies, etc.) comparable with the usual applications? What are the characteristics of the supply network? Could there be elevated electromagnetic interference at the machine's planned location of use? What are the prevailing temperatures? Etc. Factors such as these may increase the probability of failure, even if the specified limits of the components used are not violated. The possibility further exists of errors in the software, which of course may also give rise to hazardous events.

Where the incidence and severity of accidents on comparable machines with identical risks, the same operating and safety concept and identical safeguards is known and is considered low, the probability of a hazardous event occurring can also be ranked as low.

The PL_r reduced as a result of these considerations must not under any circumstances be lower than that of the machines considered by way of comparison, since it does not follow from a low incidence and severity of accidents that the level of safety provided by the implemented safety functions is greater than that required. It cannot be predicted whether a reduction of the existing level would lead to an unacceptable increase in the incidence and severity of accidents.

Chapter 6 describes the subsequent design of the safety functions.

5.5 Complementary protective measures

The requirements for complementary protective measures are contained in EN ISO 12100 [3], subclause 6.3.5. With regard to the control technology issues addressed in this report, these complementary protective measures particularly include:

- Measures for stopping in an emergency
- Reversal of movements
- Isolation and energy dissipation

According to the definition, these do not constitute technical protective measures the implementation of which would require a certain Performance Level. These complementary protective measures should however take effect when technical protective measures (guards and/or protective devices) have failed or have been defeated. In these cases in particular, an emergency stop function for example is expected actually to be serviceable. The requirements placed by IEC 60204-1 [25] upon control circuits and the control functions of machines should therefore be observed. subclause 9.4, "Control functions in the event of failure", requires an appropriate level of safety performance, which must be defined by the risk evaluation of the machine. Ultimately, the requirements of EN ISO 13849 therefore also apply to these complementary protective measures. Under no circumstances may complementary protective measures influence the function and standard of safeguards.

5.6 Treatment of legacy machinery

Legacy machinery in this context refers to machines that were placed on the market before the Machinery Directive came into force. The requirements of the directive were not applied to these machines. However, its application may become necessary should legacy machines be extended, modified, modernized, etc. In such cases, it must be assessed whether an essential change has occurred. Should this be the case, the requirements of the EC Machinery Directive apply to "old", i.e. legacy machines in the same way as to new machinery. These requirements include the application of EN ISO 13849. An interpretation paper produced by the German Federal Ministry of Labour and Social Affairs (BMAS) assists in determining whether an essential change has occurred [21].

5.7 Risk reduction with reference to the example of a paper-cutting guillotine with diverse redundancy in the logic control (Category 4 – PL e)

The example in this subclause illustrates the application of EN ISO 13849-1 on a paper-cutting guillotine. Only certain aspects will be considered in detail, and not the entire process.

Paper-cutting guillotines (see Figure 5.10) are used to cut stacks of paper sheets or similar materials by means of a knife. The product to be cut is generally placed under the knife by hand. Immediately before the cutting action is performed, a clamping bar is lowered at high force onto

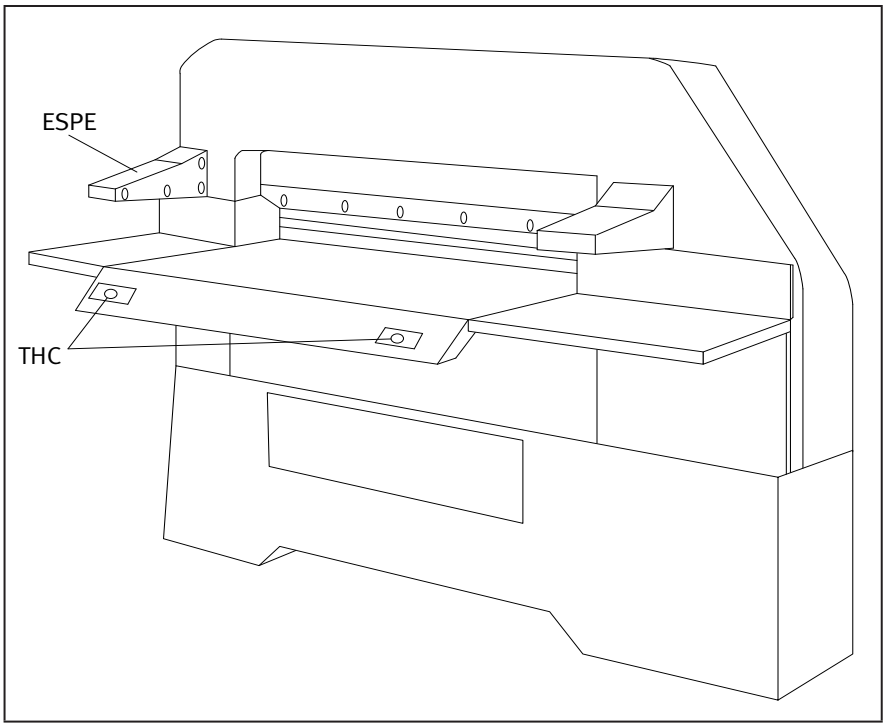


Figure 5.10:
Paper cutting guillotine with two-hand control (THC) and electro-sensitive protective equipment (ESPE)

the stack in order to hold it in place during cutting. The knife and the clamping bar are driven hydraulically.

5.7.1 Definition of the limits of the machine

Space limits

Since paper-cutting guillotines are charged manually, sufficient space is required for the handling of product for cutting, onward transport and storage of the cut paper stack, and disposal of paper waste, as well as sufficient space for the operator to move.

Time limits

Depending upon the application, the machine may be used for a period of approximately 20 years. Component wear may lengthen the time required for a movement to stop. The resulting violation of the overrun must therefore be detected and must result in the machine being stopped.

Use limits

The intended use of the machine is that of cutting stacked sheets of paper or similar materials. The machine is charged manually by a single person. Depending upon the site of installation and the width of the machine, however, the presence of other persons in the vicinity cannot be excluded.

The following operating modes are implemented:

1. Pressing
2. Manual cutting (single cut)
3. Automatic sequence of cuts (automatic process following the first, manual cut)
4. Knife change

In the first three operating modes, movement of the clamping bar alone is possible, in order for the line of cut to be indicated. For this purpose, the operator operates a pedal, and is able at the same time to alter the position of the paper stack with his or her hands within the danger zone.

5.7.2 Identification of the hazards

The following mechanical hazards are significant for a paper-cutting guillotine:

- G1 – crushing by the clamping bar
- G2 – cutting by the knife during the cutting process
- G3 – cutting by the knife in the rest position

Risk estimation

The dynamic press force of the clamping bar (hazard G1) is sufficiently great to cause not only reversible crushing injuries, but also broken bones. For hazard G2, amputation of limbs must be assumed. During manual positioning of the paper stack, hazard G3 may lead to injury to the hands or forearms on the stationary knife. These injuries are however generally reversible.

The operators‘ exposure to hazard is very high, since they regularly (cyclically) intervene manually in the danger zone in the course of routine work.

The drop speeds of the clamping bar and knife (hazards G1 and G2) are very high, with the result that the operator has virtually no means of avoiding the hazard. When the knife is stationary (hazard G3), the operator is able to avoid or limit harm.

The probability of a hazardous event occurring as a result of technical failure is not known. The incidence and severity on comparable machines is however low; the safeguards implemented here are therefore evidently adequate. Should the risk analysis for a safety function yield a higher PL_r than that actually implemented on the comparable machines, the PL_r can in principle be reduced by one level. However, since the safety functions on comparable paper-cutting guillotines are achieved with the highest PL, a reduction of the PL_r will not be possible in this case (see subclause 5.7.4).

Risk evaluation

In consideration of all operating conditions and all possibilities for operator intervention, a risk reduction is found to be required.

Inherently safe design

It is not possible for the dynamic press force of the clamping bar and the energy of the knife to be reduced, as this would impair the functionality of the machine. An arrangement and design of the machine that would prevent the operator from reaching into the danger zone is also not possible, since this is precisely where the operator must line up the stack of paper.

The following measures can however be taken:

1. Shrouding of all points of access to the danger zone except on the operator side.

2. Avoidance of sharp edges and corners.

3. Assurance of a suitable working position and accessibility of the controls.

4. Ergonomic design of the machine.

5. Avoidance of electrical hazards.

6. Avoidance of hazards presented by the hydraulic equipment.

7. The mechanical components for guiding the knife and the clamping bar are linked such that in its top rest position, the knife is shrouded by the clamping bar.

5.7.3 Required safety functions

In consideration of all operating modes and all manual interventions, the following safety functions are required:

- SF1 – STO (safe torque off), for avoidance of unexpected start-up

- SF2 – Controlled location of the operator‘s hands outside the danger zone during a hazardous movement

- SF3 – Detection of intervention by further persons in the danger zone by means of ESPE (electro-sensitive protective equipment), e.g. a light curtain, and immediate interruption of the cutting operation

- SF4 – Automatic stopping of all movements following each individual cut or following completion of the automatic cutting sequence

- SF5 – Reduction of the dynamic press force for the clamping bar during the “indicate cut” function

- SF6 – Automatic return of the clamping bar and knife to their initial positions following interruption of a cutting operation

Note: The principle of overlapping hazards could be applied to the machine parts of knife and clamping bar (see subclause 5.3.2). In this case, SF1, SF3, SF4 and SF6 would be divided up such that dedicated safety functions would be defined separately for the knife and the clamping bar. In the present case however, this division is not made, since owing to the low number of components in SF1 to SF6, the required PFH_D can still be attained when these safety functions are grouped.

Characteristics of the safety functions

The cut must be interrupted immediately should the light curtain be penetrated. The safety function SF3 therefore takes priority over SF2. For SF5, the maximum permissible force for the clamping bar during the “indicate cut” function must be specified (see [27]).

5.7.4 Determining of the required Performance Level PL_r

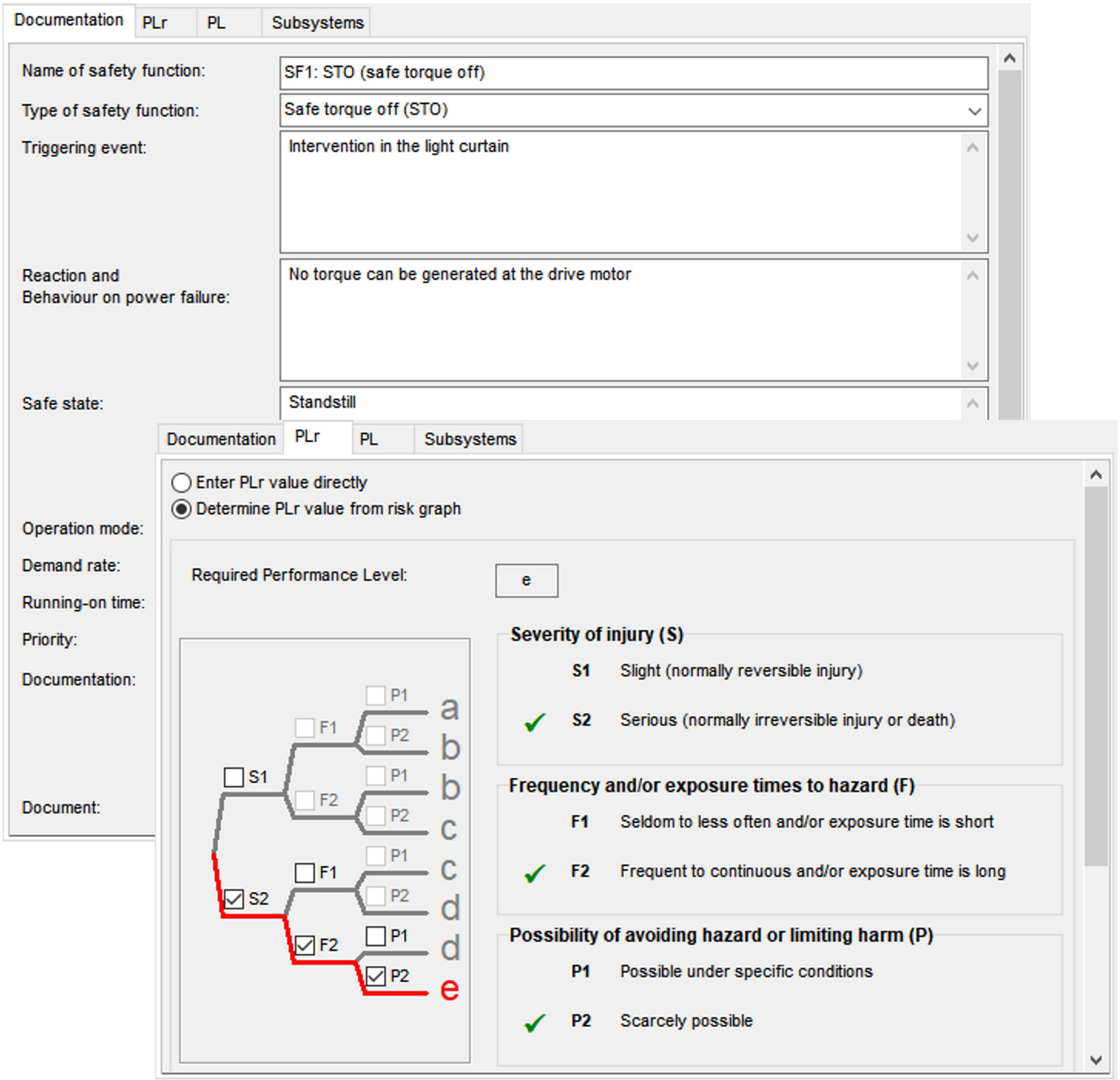
The PL_r must be determined for each safety function. If the situations in which the individual safety functions are used are analysed, evaluation of the risk parameters S, F and P is seen to be similar for the safety functions SF1 to SF6:

- S2 – serious, generally irreversible injury
- F2 – continuous presence in the danger zone; the frequency is therefore greater than once every 15 minutes
- P2 – evasion of a hazardous situation is virtually impossible

In accordance with the risk graph in Figure 5.9, this evaluation yields a required Performance Level PL_r of e. The incidence and severity of accidents on comparable machines is low. The safety functions considered here of these machines have already been implemented with PL e, as specified in [28]. The result of the risk analysis is therefore confirmed by the situation in practice; a possible reduction in the PL_r is not indicated. Figure 5.11 shows the documentation and risk graph in the SISTEMA software application for the SF1 safety function.

An adequate risk reduction has been achieved for the hazard G3, “Cutting by the knife in the rest state”, by mechanical coupling of the knife and the clamping bar. A safety function is not required.

Figure 5.11:
Documentation and risk graph for SF1



5.7.5 Complementary protective measures

The following measures are required:

1. Emergency stop

   Suitable safety functions with a PL of e are already available in the machine control system and are used for the emergency stop. Provided the emergency-stop device features a two-channel circuit, stopping in an emergency therefore also satisfies a PL of e.

2. Freeing of a trapped person requires a reverse movement of the knife and clamping bar; this is achieved by spring force.

6 Design of safe control systems

Changes with respect to the second edition (BGIA Report 2/2008e):

- Further information added in subclause 6.1.2 (Systematic failures) on application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), programmable logic modules and complex standard modules. subclause 6.1.3 (Ergonomics) brought into line with the new 2006/42/EC Machinery Directive.
- Recommendations added to subclause 6.2.5 (Category 2) for interpretation of the requirements for a Category 2.
- Clarification added in subclauses 6.2.5 (Category 2) and 6.2.14 (*DC*) that up to a PL_r of c, providing a warning is a permissible alternative under certain circumstances to initiation of a safe state. In addition, testing immediately upon demand of the safety function added as an alternative to testing being at least 100 times as frequent as the demand of the safety function. If the safety function is tested only 25 times as frequently as a demand is made upon it, this can be estimated on the safe side by multiplication of the PFH_D with the factor of 1.1. In addition, the requirement for the quality of the test equipment in Category 2 now refers to the $MTTF_D$ of the test channel (instead of only of the "TE" block) in relation to the $MTTF_D$ of the functional channel (instead of only of the "L" block).
- "Encapsulated subsystem" introduced in subclauses 6.2.9 and 6.4.
- Raising of the $MTTF_D$ capping in Category 4 to 2,500 years added in subclause 6.2.13 (FMEA vs. parts count method).
- Explanations of the test rate revised and information on components with $DC < 60\%$ down to $DC = 0\%$ added in subclause 6.2.14 (diagnostic coverage).
- New subclause 6.2.17 added on alternative determining of the PFH_D for the output part of the SRP/CS in accordance with subclause 4.5.5 of the standard.
- The previous subclause 6.2.17 (Bus systems as "interconnecting means") becomes subclause 6.2.18 as a result.
- Subclause 6.3.10 concerning requirements for SRESW for standard components brought into line with the new subclause 4.6.2 of the standard. Reference to IFA Report 2/2016 concerning safety-related application software for machinery also added.
- Summation of PFH_D values stated as the new standard procedure in subclause 6.4 (Combination of SRP/CSs as subsystems); tabular method for downgrading of the PL according to the number of subsystems degraded to the status of an alternative solution for the event that PFH_D values are not available for subsystems.
- Example of the paper-cutting guillotine in subclause 6.5 updated.
- References to SISTEMA Cookbooks 1, 4 and 6 as sources of further information added.

6.1 Introduction

Once the precise safety function and its required risk reduction in the form of the PL_r have been defined, design proper begins of the safety-related parts of the control system (SRP/CS) that are to carry out the safety function(s). The corresponding subclause from the iterative design process of EN ISO 13849-1 is shown in Figure 6.1 (see Page 40).

The safety-related quality of the SRP/CS is indicated by one of five Performance Levels (PLs). Each of these PLs corresponds to a range of the probability of a dangerous failure per hour (Table 6.1, Page 40). In addition to the average probability of a dangerous failure per hour (PFH_D), further measures, for example to enhance software robustness or to counter systematic failures, are required in order for the corresponding PL to be attained.

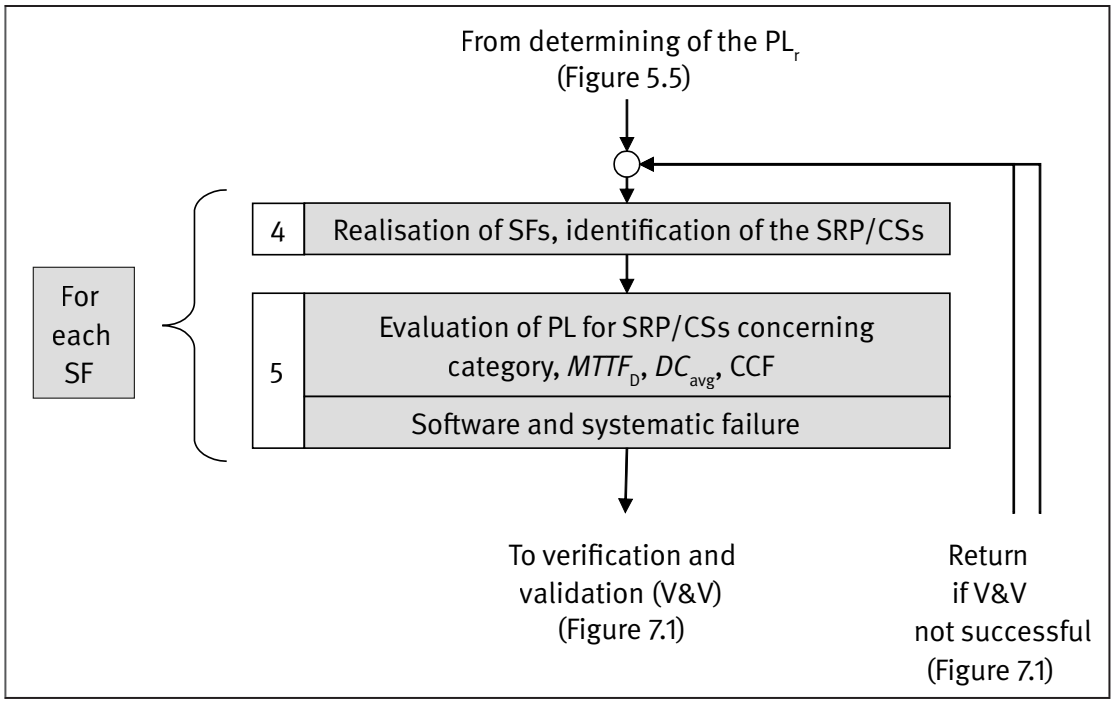


Figure 6.1: Determining of the attained PL in the implementation phase of the SRP/CS: excerpt from the iterative design process, see Figure 4.1

Table 6.1:
Correspondence between the probability of failure and the Performance Level

Performance Level (PL)	Average probability of a dangerous failure per hour (PFH_D) in h^{-1}
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \cdot 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \cdot 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

In principle, any method (e.g. *Markov* calculations, Petri nets) may be used to prove the probability of failure. The following criteria must however always be observed:

- Quantifiable aspects (structure, component reliability, diagnostics in the form of tests, common cause failure)
- Non-quantifiable, qualitative aspects that influence the behaviour of the SRP/CS (behaviour of the safety function under fault conditions, safety-related software, systematic failures and environmental conditions)

For both groups of criteria, EN ISO 13849-1 proposes practical methods that produce a good and scientifically sound estimate of the attained PL. For each specific sub-aspect, proof can be made coarser or finer as required, permitting both a fast approximation and a more detailed determination.

The development procedure is first described (see subclause 6.1.1). This includes requirements upon the specification and upon the documentation within the life cycle of the SRP/CS. It is followed by measures necessary for the control of systematic failures (subclause 6.1.2) and ergonomic design aspects (subclause 6.1.3). Subclause 6.2 describes the Categories and the simplified method based upon them for evaluation of the quantifiable aspects. Subclause 6.3 then presents requirements upon the software. Finally, subclause 6.4 shows which quantifiable aspects must be considered when SRP/CSs are used in combination. Figure 6.2 explains the need for this additional subclause. The machine control system (CS) as a whole is divided into safety-related parts (SRP/CS) and the non-safety-related parts; the latter are generally substantially more comprehensive and serve only to perform normal operating functions. The combination of safety-related parts of a control system begins at the point at which safety-related signals are generated (these include, for example, the actuating cam and roller of a position switch), and ends at the outputs of the power control elements (for example including the main contacts of a contactor). Where hazards do not arise in the de-energized state (closed-circuit current principle, de-energization principle), power components such as motors or cylinders are not regarded as an SRP/CS. Should external forces take effect, however (for instance on vertical axes), the power elements must be reenforced for functional safety (e.g. non-return valve on cylinders; supplementary mechanical brakes). Finally, subclause 6.5 takes up the content of subclause 5.7 by describing actual implementation with reference to the practical example of the control system of a paper-cutting guillotine.

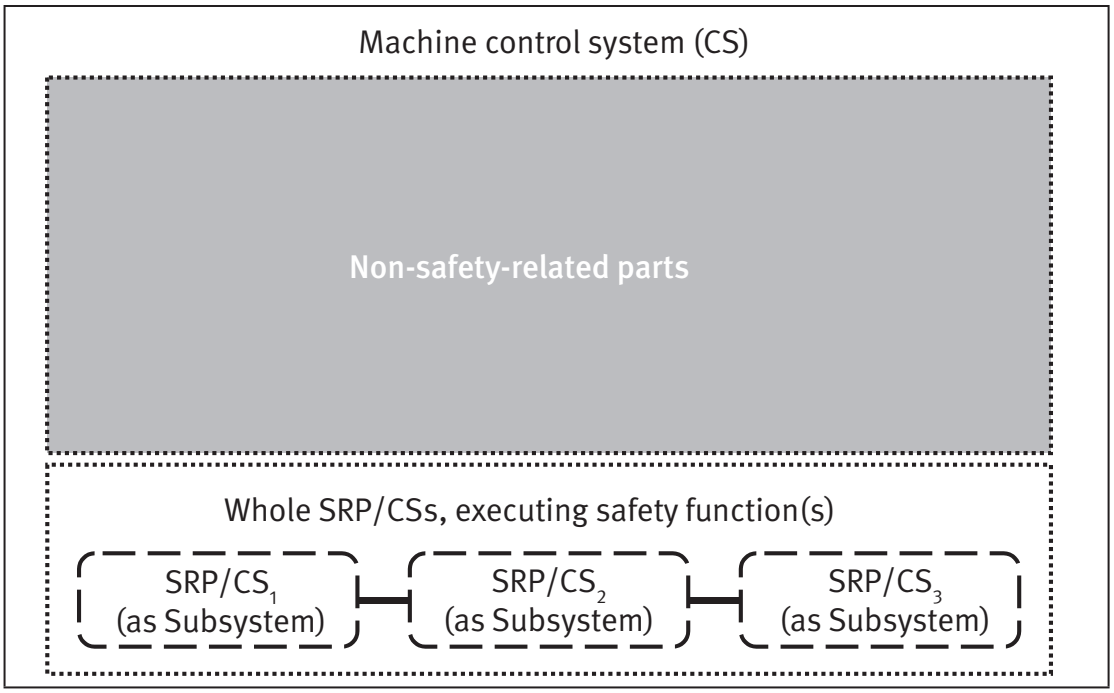


Figure 6.2: SRP/CS and subsystems within the machine control system

6.1.1 Design and development process

The objective of each activity during the design and integration of the safety-related parts of control systems (scope of the standard) is the development and use as intended of products that are as free of faults as possible and that satisfy the requirements. The objective is after all the health of human beings and the avoidance of accidents. The motto for the design and development process must therefore be: "Structured and well documented".

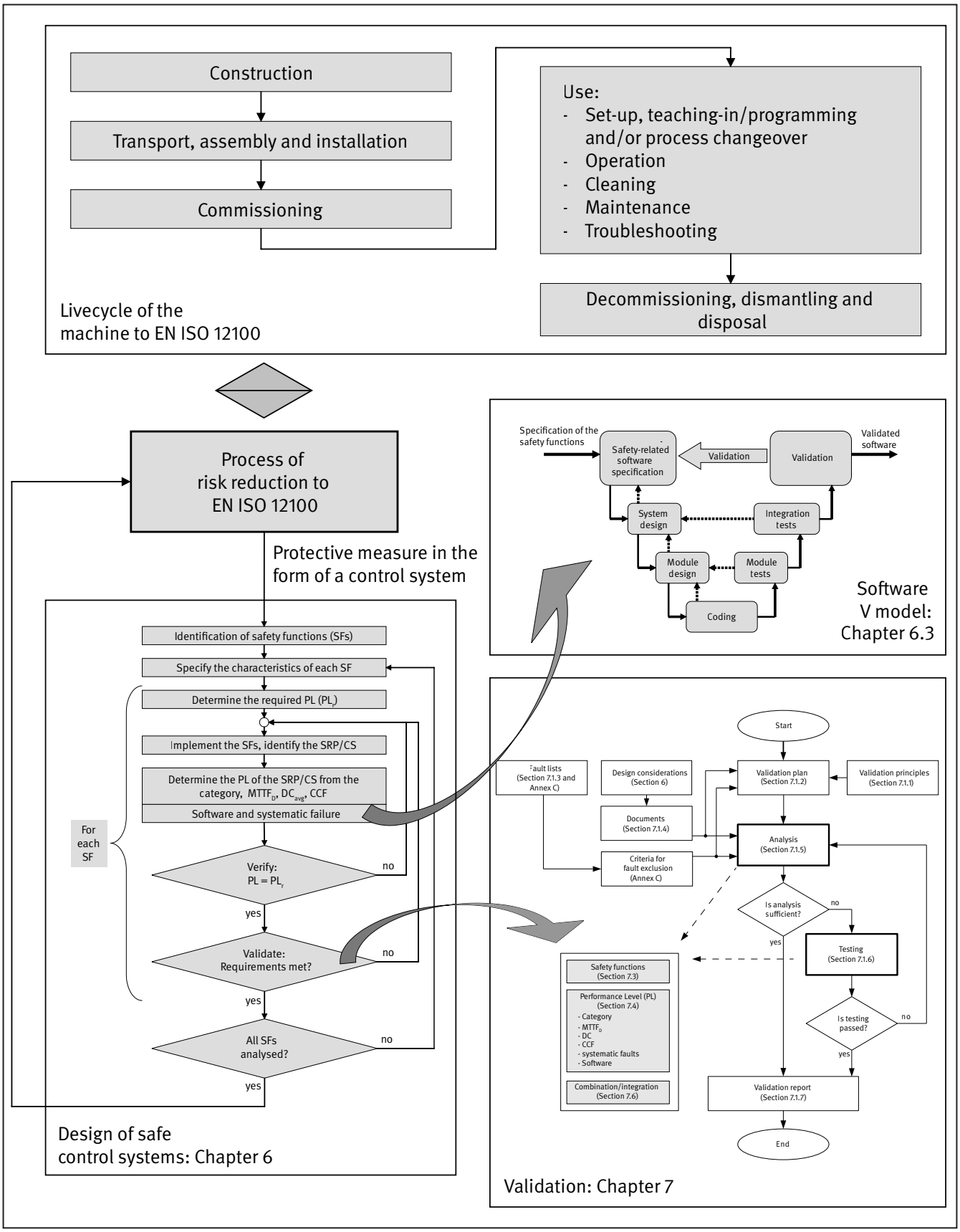
The process of risk reduction in accordance with EN ISO 12100 [3] must be geared to the entire life cycle of a machine, as shown in Figure 6.3. Although EN ISO 13849-1 contains no explicit provision to this effect, the concept of the life cycle must also be taken up during design and integration of one or more SRP/CSs, in order for the activities to be structured appropriately. The description of the standard in Chapter 4 also shows clearly that the iterative process described in the standard for the design of the safety-related parts of control systems is a process subdivided into individual phases. As can be seen in Figure 6.3, the validation phase is characterized by structured procedures of its own. These will be discussed in greater detail in Chapter 7. Structuring into life-cycle phases is characterized very comprehensively by the V model employed during development of safety-related software; this is explained in subclause 6.3. For example, although the maintenance phase is not explicitly addressed by the design process for the SRP/CS, it is taken into account by the required content of the information for use.

Since an SRP/CS constitutes parts of a machine, requirements in virtually any phase of the machine's life cycle may also have an influence upon an SRP/CS. All phases in the machine's life cycle must therefore be considered during identification of the safety functions and definition of their characteristics. In order for this process to be organized as comprehensibly and verifiably as possible, safety functions are first specified. SISTEMA Cookbook 6 [23] addresses this topic in detail: "Definition of the safety functions: what is important?". An SRP/CS that is not developed for a specific machine control system – examples include light curtains or safety PLCs – therefore requires a particularly precise description of their characteristic data and their interfaces in order for proper use to be assured.

The life cycle of the SRP/CS begins with specification of the safety functions. Besides particular aspects of various safety functions, EN ISO 13849-1 also lists general aspects that are a minimum requirement in such a specification.

A specification of this kind sets out, at the beginning of the design process, the framework for all parties involved. It constitutes a set of requirements specifications; in no way is it a product specification produced post-development. A safety function is implemented by the SRP/CS that is part of the machine control system and that possesses interfaces to further SRP/CSs and to the functional control system. A specification must therefore be drawn up. Box 6.1 (Page 43) shows a general arrangement template for a specification of the safety requirements. The arrangement also includes the specification of the safety functions. This arrangement template refers to the SRP/CS that executes the entire safety function. Where the SRP/CS takes the form of subsystems, the specification must be suitably adapted.

Figure 6.3:
Life cycles of machines and SRP/CS



Box 6.1: General arrangement template for a safety requirements specification

1 General product and project information

1.1 Product identification
1.2 Author, version, date, document name, file name
1.3 Contents
1.4 Terminology, definitions, glossary
1.5 Version history and changes
1.6 Directives, standards and technical rules relevant to development

2 Functional information on the machine, where relevant to safety

2.1 Intended use and reasonably foreseeable misuse
2.2 Process description (operating functions)
2.3 Operating modes (e.g. setup mode, automatic mode, operation of localized relevance or of parts of the machine)
2.4 Characteristic data, e.g. cycle times, response times, overrun distances
2.5 Other characteristics of the machine
2.6 Safe state of the machine
2.7 Interaction between processes (see also 2.2) and manual actions (repair, setting, cleaning, troubleshooting, etc.)
2.8 Action to be taken in an emergency
2.9 Behaviour of the machine in the event of energy loss

3 Required Performance Level(s) (PL_r)

3.1 Reference to existing documentation concerning identified hazards and risk assessment for the machine
3.2 Results of the risk assessment for each identified hazard or hazardous situation and determination of the safety function(s) required in each case for risk reduction

4 Safety functions (information applies to each safety function; see also Table 4 in [23])

– Description of the function ("input – logic – output") including all functional characteristics (refer also to Tables 5.1 and 5.2)
– Activation/deactivation conditions or events (e.g. operating modes of the machine)
– Behaviour of the machine when the safety function is triggered
– Conditions to be observed for re-starting
– Performance criteria/performance data
– Process (timing behaviour) of the safety function, including response time
– Frequency of actuation (i.e. demand rate), recovery time following demand
– Other data
– Adjustable parameters (where implemented)
– Classification and assignment of priorities in the event of simultaneous demand upon and processing of multiple safety functions
– Behaviour in the event of a power failure
– Functional concept for separation or independence/freedom of reciprocal action from non-safety functions and further safety functions

5 Required information for the SRP/CS design

5.1 Allocation of the SRP/CS and the form of technology by which the safety function is to be implemented; intended equipment
5.2 Selection of the Category, designated architecture (structure) in the form of a safety-related block diagram and description
5.3 Description of the interfaces (process interfaces, internal interfaces, user interfaces, control and display elements, etc.)
5.4 Behaviour at switch-on, implementation of the required starting and restarting behaviour
5.5 Performance data: cycle times, response times, etc.

5.6 Behaviour of the SRP/CS in the event of component failures and faults (achieving and maintenance of the safe state), including timing behaviour
5.7 Failure modes of components, modules or blocks that are to be considered; where applicable, reasoning for fault exclusions
5.8 Concept for implementation of the detection and control of random and systematic failures (self-tests, test circuits, monitoring arrangements, comparisons, plausibility tests, fault detection by the process, etc.)
5.9 Quantitative aspects
5.9.1 Target values for $MTTF_D$ and DC_{avg}
5.9.2 Switching frequency of components subject to wear
5.9.3 Frequency of measures for fault detection
5.9.4 Mission time, where different from the assumption upon which the designated architecture is based (20 years)
5.10 Operating and limit data (operating and storage temperature range, humidity class, IP degree of protection, values for resistance to shock/vibration, EMC values, supply data with tolerances, etc.) (IP = ingress protection; EMC = electromagnetic compatibility)
5.11 Generic standards to be applied for design (for the equipment, for protection against electric shock/ hazardous shock currents, for resistance to environmental conditions, etc.)
5.12 Technical and organizational measures for protected access to safety-related parameters and to SRP/CS characteristics (protection against tampering, access protection, program/data protection) and for protection against unauthorized operation (key switch, code, etc.), for example in non-standard operating modes
5.13 General technical requirements and organizational framework for commissioning, testing and acceptance, and for maintenance and repair

In order to be valid, such a specification must be verified prior to the next design step. Verification primarily concerns completeness, correctness, intelligibility and freedom from contradictions. It is clearly advantageous for verification to be performed, for example by way of an inspection, by a party not involved in the project. If safety-related software is employed, this safety requirements specification must form the basis for a dedicated software specification (see subclause 6.3.2).

The specification is the first document to be created in the procedure for the design of the SRP/CS. The documentation is of great importance in the interests of verifiable development. It must be considered that the task of updating a product may lie with a party other than the original designer. Details concerning the necessary documentation in the context of the iterative design process of the SRP/CS can be found in subclause 6.3.8 concerning software, and in subclauses 7.1.4 ff. The reader is reminded at this point that the documents must be unambiguously identifiable; version management is therefore essential. The contents of the information for use are ultimately of major importance for the proper implementation of safety functions. EN ISO 13849-1, Clause 11 lists the minimum items of information that must be included in the information for use. The content of the manufacturer's internal technical documentation for the SRP/CS is listed in clause 10 of the standard. Requirements concerning the documentation are also set out in legislation. Box 6.2 shows the content of the technical documentation for machines required in accordance with the European Machinery Directive 2006/42/EC [2].

6.1.2 Systematic failures

In contrast to random component failures, systematic failures have causes that can be eliminated only by modification for example of the design, the manufacturing process, the operating methods or the documentation. They arise at some point in the life cycle of a product, for example as a result of errors in the specification or the design, or during modification of the SRP/CS. The implementation of multi-channel structures and analysis of the probability of component failures are important elements in the design of safety technology. Should fundamental aspects not be considered, even the most favourable figures for the probability of failure are of no benefit. If, for example, a product is not used correctly or is used in the wrong environment, a risk of systematic failure may exist. This fact is addressed by EN ISO 13849-1 in conjunction with Part 2, when it requires that possible systematic failures also be considered for attainment of a PL. Essentially, it can be said that many of the basic and well-tried safety principles are already effective in preventing systematic failures (see Annex C). These principles, which supplement Annex G of the standard, should be considered in accordance with EN ISO 13849-2.

The informative Annex G of the standard contains a list of measures, and therefore indirectly also of influences that are to be considered. The measures are divided into those

Box 6.2: Technical documentation for machines: excerpt from the Machinery Directive (2006/42/EC), Annex VII, A

1. The technical file shall comprise the following:
   a) a construction file including:
      — a general description of the machinery,
      — the general drawing of the machinery and drawings of the control circuits, as well as the pertinent descriptions and explanations necessary for understanding the operation of the machinery,
      — full detailed drawings, accompanied by any calculation notes, test results, certificates, etc., required to check the conformity of the machinery with the essential health and safety requirements,
      — the documentation on risk assessment demonstrating the procedure followed, including:
        i) a list of the essential health and safety requirements which apply to the machinery,
        ii) the description of the protective measures implemented to eliminate identified hazards or to reduce risks and, when appropriate, the indication of the residual risks associated with the machinery,
      — the standards and other technical specifications used, indicating the essential health and safety requirements covered by these standards,
      — any technical report giving the results of the tests carried out either by the manufacturer or by a body chosen by the manufacturer or his authorised representative,
      — a copy of the instructions for the machinery,
      — where appropriate, the declaration of incorporation for included partly completed machinery and the relevant assembly instructions for such machinery,
      — where appropriate, copies of the EC declaration of conformity of machinery or other products incorporated into the machinery,
      — a copy of the EC declaration of conformity.
   b) for series manufacture, the internal measures that will be implemented to ensure that the machinery remains in conformity with the provisions of this Directive.

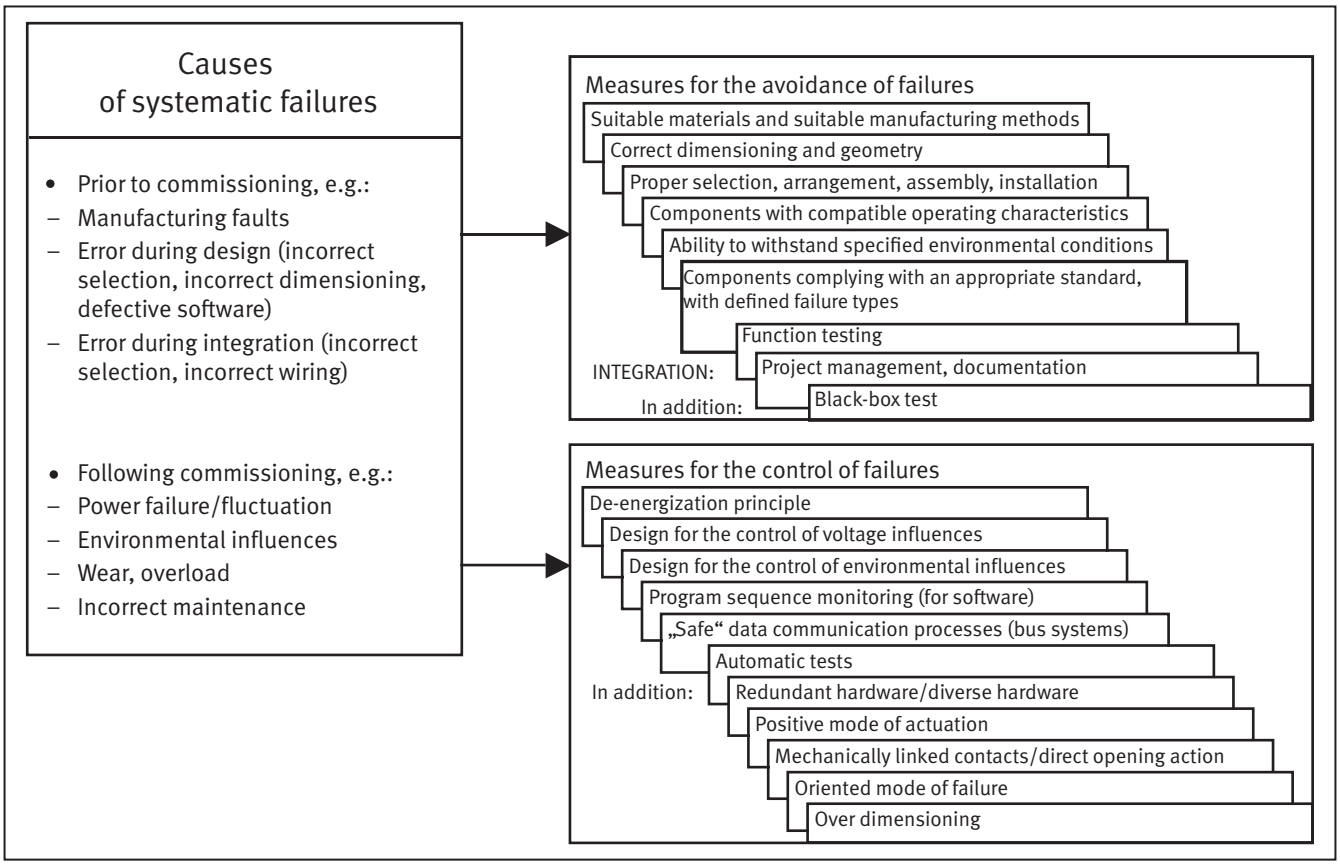
for the avoidance of failures (G.3 and G.4) and those for their control (G.2). Figure 6.4 provides an overview. The measures for the avoidance of failures must be effective throughout all phases of a product's lifetime, and are addressed accordingly to some degree in Chapter 7 of this report, under the aspect of validation. Although not stated explicitly, appropriate care must be taken not least during modifications, troubleshooting and maintenance. It is during these phases in particular that the details of development are not (or are no longer) evident. Conversely, measures for the control of failures must be implemented within a product, and take full effect during operation. Besides basic requirements, the standard also lists measures for selection, one or more of which are to be applied in consideration of the complexity of the SRP/CS and of the PL (marked “in addition” in Figure 6.4).

Most of the measures are explained briefly in the standard. Attention is drawn to the fact that in the day-to-day activities of the IFA, diversity is assumed to be of major benefit in general, and not only as shown for hardware in Figure 6.4 (see Page 46). Refer in this context also to the information in subclause 6.3.10 concerning the requirements upon software.

Should application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), programmable logic modules or similar be used, attention is drawn to Annex F of IEC 61508-2:2010, which lists design and development techniques and measures for the avoidance of systematic failures.

Particular care must be taken where complex standard components are used. Should software be involved, the standard provides relevant information; refer in this context to subclause 6.3.10 of the present report. Manufacturers of standard components take only limited measures for fault avoidance in a safety context. The user must therefore concentrate on the measures for the control of systematic failures. Should for example two standard PLCs be used in two-channel structures, an overvoltage in the power supply could give rise to a systematic failure despite redundancy (including diverse redundancy). Systematic failure can be prevented in such cases only by additional measures.The astute reader of this report may wonder in what way these measures differ from those against common cause failure (CCF, see subclause 6.2.15). Common cause failures are of course also to be regarded as systematic failures. The analysis of CCF however addresses only structures that are multi-channel in form or that at least possess test equipment (Categories 2, 3 and 4). A further difference is the “attempt” to consider CCF aspects numerically (quantitatively); by contrast, the analysis described in Annex G of the standard is purely qualitative. Given adequate measures against systematic failures in accordance with Annex G of the standard and observance of basic and well-tried safety principles, it

Figure 6.4:
Measures against systematic failures in accordance with Annex G of the standard



would not appear particularly difficult to satisfy the requirements for measures against common cause failure (CCF).

Three examples will show that actual requirements may indeed vary according to application and technology, and that the general requirements may therefore also require interpretation on occasion.

Example 1:
Measures for control of the effects of a power failure

The design of safety-related parts of control systems must also give consideration to faults in the power supply (electric power, air pressure in pneumatic systems, hydraulic fluid pressure) (see subclause 5.2.8 and Annex G of the standard). Voltage breakdown, voltage fluctuations and overvoltage or undervoltage may for example endanger the safe state of a machine. This particularly applies to the holding of loads in a raised position by means of electrical and hydraulic drives (vertical axes). Such disturbances may be caused by component faults within the SRP/CS. In this case, their effects upon the Performance Level are considered during verification. Should however the cause lie in the mains supply, or should the mains disconnecting device (main switch) of the machine have been actuated, these cases lie beyond the scope of quantitative analysis. They can be considered only as systematic failures – and in some cases even as operating states – that must be controlled by the SRP/CS such that the safe state is achieved and/or maintained. Since its third edition, the standard proposes that different safety functions be provided for these scenarios:

a) Where power is available
b) Where power is not available

If it is assumed that power is normally available, assessment of the risk parameters for the two safety functions to EN ISO 13849-1 may yield different results. In individual caes, this may – depending upon the actual risk parameters – enable safety functions to be implemented with a lower PL_r in cases where power is not available.

Example 2:
Failure of pneumatic or hydraulic valves

Among the requirements of EN ISO 13849-2, Tables B.1 “Basic safety principles” and B.2 “Well-tried safety principles” for pneumatic systems are that attention must be paid to the “use of suitable materials and adequate manufacturing” and the “proper avoidance of contamination of the fluid” during the design and manufacture of pneumatic components. These requirements apply above all to the selection of materials and the processes of manufacture and treatment in consideration of factors

such as stresses, durability, abrasion, wear, corrosion and temperature, and the consideration of highly effective filtration of the compressed air and the removal of solids and water. The requirements upon hydraulic components are specified in a similar manner in Tables C.1 and C.2. Here too, attention must be paid to "sufficient avoidance of contamination of the fluid" and "correct dimensioning and shaping".

Greater resistance to operating movement may nevertheless arise in fluid power components that are operated infrequently, owing to their design features (gap between the valving element and the enclosure):

- On pneumatic valves with soft seals that remain in the same switching position for a longer period, the seals may swell owing to chemical influences caused by the lubricant (oil with additives in the compressed air, introduced by the compressor, lubricator, or lubrication for life), or the lubricating film may collapse under the pressure of the seal edge, resulting in increased resistance to operation.

- On hydraulic valves, silting may occur when the valve remains in the same switching position for a longer period. In this case, fine dirt particles are deposited in the sealing gap between switching cycles, causing the valving element to stick.

For these reasons, a high force surplus (e.g. spring force) must generally be engineered for return of the valving element to the "safety-oriented switching position". On non-mechanical springs, retention of the reset function must be assured by suitable measures. In addition, the effects described above must be prevented by cyclical switching, to which the standard now refers. Failures caused by the absence of switching are to be prevented by suitable switching cycles/test cycles at intervals for example of less than eight hours.

Example 3:
Separation of safety-related and non-safety-related functions

Standards governing functional safety generally address the separation of safety-related functions from other (non-safety-related) functions. EN ISO 13849-2 is one such example, regarding this separation for example as a well-tried safety principle for electrical systems under the heading "Minimise possibility of faults". This requirement applies to both hardware and software. At the same time, there may be reasons why complete separation is disadvantageous. In such cases, clearly defined functional and technical interfaces must at least be implemented that enable influences upon the safety-related part to be avoided and/or controlled.

This requirement is illustrated well by the example of the development of application software. The most far-reaching form of separation between standard application software and safety-related application software (SRASW, see subclause 6.3) is of course for them to be written with separate programming systems (engineering suites) and run on separate PLCs. For economic reasons in particular, however, it is desirable for the entire application software to be written by means of a single programming system, possibly in the same engineering process. Numerous aspects must however be considered when this approach is followed. These include the requirement that safety-related variables, results or outputs must not be overwritten by non-safety-related parts of software (program, function block, function/instruction, etc.). Links between the two environments are permissible, but only with the observance of specified conventions. One such convention is that safety-related signals and functions must always retain priority: linking by means of an OR operation, for example, is not permitted under any circumstances. Modern software development tools support such approaches, and specified functions and rules with automatic checking have been implemented in their editors and compilers. Errors in logic operations, which may have an effect only in unpredictable operational situations and which may not be detectable with reasonable effort during acceptance/commissioning, can thus be prevented in a user-friendly manner.

This does not mean that the designer is spared a complete analysis of the influence exerted by functional standard components of a control system upon its safety-related parts (including the influence of the safety-related functions upon each other); the analysis of where (technically) and how (functionally) such influences may arise is however considerably simplified and accelerated by the use of the development tools referred to above. The even more pertinent question, namely how to eliminate (avoid or control) influences that are detected, may not even arise.

6.1.3 Ergonomics

Annex I, subclause 1.1.6 of the European 2006/42/EC Machinery Directive requires requires manufacturers of machines to reduce, at the design stage of the machine, the discomfort, fatigue and psychological stress faced by the operator to the greatest possible extent, taking into account ergonomic principles. This therefore also applies to the interfaces between operators of a machine/installation and the SRP/CS. These interfaces include both the safeguards themselves, such as a guard door with position switch, and the operation of a safety function, for example by means of pushbuttons or even by a software display interface suitable for this purpose. A machine-determined work rate and monitoring that requires lengthy concentration are also to be avoided.

The importance of ergonomic principles for the SRP/CS, and the fact that the design of a machine does not always take account of all cases of intended use or foreseeable misuse of the SRP/CS, is demonstrated by the HVBG report on the defeating of protective devices on machinery [29]. Resources and further information on the subject of defeating can be found on the www.stop-defeating.org website.

EN ISO 13849-1 therefore requires that ergonomic principles be applied, and lists a number of useful standards for this purpose in subclause 4.8. In order for designers of machines to be able to check the design of the human-machine interface of the SRP/CS, the IFA has drawn up a checklist for ergonomic machine design. In February 2018, this checklist was updated together with further documents in the form of DGUV Informative publication 209-068/069 (formerly BGI/GUV-I 5048-1/2) [30]. Among the subjects addressed more specifically are: manually operated actuators; keyboards, (keypad) keys and input devices; displays; visual danger signals; and the software ergonomics of user interfaces. VDI/VDE guideline 3850 [31] for example serves as an aid to the user-friendly design of user interfaces for machines.

6.2 Quantification of the probability of failure

The numerical quantification of the probability of failure required by the standard for determining of the PL, often referred to (including in other standards) simply as "quantification", can strictly speaking never be attained exactly, but only by approximation with the aid of statistical methods or other estimations. The main influencing variables that must be considered during this process of determination are stated; the method by which the probability of failure is actually determined from them is however at the user's discretion. Any validated and recognized method can be used for this purpose. Such methods include reliability block diagrams, fault tree analysis, *Markov* modelling or Petri nets. Depending upon who determines the probability of failure, i.e. the manufacturer of the control system, the user of the machine, or a test body, preferences for and experience with different methods may differ. For this reason, any suitable method is explicitly permitted in this context.

At the same time, parties lacking prior experience in quantification of the probability of failure require some degree of support in the use of EN ISO 13849-1. This need was addressed by the development of a simplified approach which, whilst being based upon sound scientific principles (*Markov* modelling), describes a simple method for quantification in successive steps. At certain points, the description makes estimates erring on the safe side which could result in a higher figure for the probability of failure being estimated than that yielded by more precise methods; the method is, however, suitable for practical application even by non-mathematicians, and the procedure is largely transparent and therefore verifiable. This simplified method is presented below in detail, both in general terms and with reference to a calculated practical example (see subclause 6.5). Further details on selected specific subjects can be found in the annexes.

6.2.1 Designated architectures...

The structure or architecture of a safety-related control system determines its tolerance of faults, and constitutes the framework upon which all other quantifiable aspects are based, by which the PL of the safety-related parts of control systems is ultimately formed. The experience gained by the IFA in conjunction with industry since 1985 confirms that the greater part of all implemented controls can be assigned to a very small number of basic types of safety-related control systems (or to combinations of these basic types, see below). These types are: at one end of the spectrum, the single-channel untested system with components of differing reliability; in the middle of the spectrum, the same type, but enhanced by testing; and at the other end, the two-channel systems featuring high-quality testing. Systems with more than two channels and other "exotic" structures are extremely rare in machine construction, and the simplified method is of only limited use for their assessment. Even where more than two channels are present, however, it is generally sufficient for the two most reliable channels to be considered in order for the PL to be estimated with sufficient precision by means of the simplified method involving designated architectures. Systems employing more than two channels are not therefore considered in EN ISO 13849-1. SISTEMA Cookbook 4 [32] provides support in some of these cases: "When the designated architectures don't match". In addition to the "horizontal" division into different functional or test channels, a "vertical" division into a sensor level (input devices, "I"), a processing level (logic, "L") and an actuator level (output devices, "O") is generally also advantageous.

Continuity is assured, fully intentionally, to the Categories set out in EN 954-1, which are established in the machine construction industry and in the associated standards. In accordance with this system, EN 954-1 defines five structures as Categories. EN ISO 13849-1 supplements the former Category definition slightly with quantitative requirements for the component reliability ($MTTF_D$), the diagnostic coverage of tests (DC_{avg}) and the resistance to common cause failures (CCF). In addition, it maps the Categories to five basic structural types, termed "designated architectures". The same Categories may still take different structural forms; the generalization which their mapping to the associated designated architecture represents is still permissible as an approximation within the

simplified approach, however. The number of "vertical" blocks (input, logic, output) in a channel is for example generally of little relevance to determination of the PL from a mathematical and safety technology perspective.

Where more complex safety functions are involved, it may no longer be possible to map the entire safety chain to any single one of the five basic types. In this case, the solution is generally for the safety chain to be broken down into several subclauses ("subsystems"), each of which can be mapped to a particular designated architecture. The method by which these subsystems are then recomposed and an overall value determined from the individual Performance Levels is explained in greater detail in subclause 6.4. The following information relates to control systems (SRP/CS) that can be assigned to a Category without being broken down into subsystems. It can however be applied by analogy to subsystems that perform only a part of a safety function.

6.2.2 ... and Categories

The Categories classify safety-related parts of a control system (SRP/CS) with respect to their resistance to faults and their subsequent behaviour in the fault condition, based upon the reliability of the parts and/or their structural arrangement (see Table 6.2, see Page 50). A higher resistance to faults translates into a greater possible risk reduction. For definition of the probability of failure and of the PL, the Categories therefore form the backbone, complemented by the component reliability ($MTTF_D$), the tests (DC_{avg}), and the resistance to common cause failures (CCF).

Category B is the basic Category, the requirements of which must also be met in all other Categories. In Categories B and 1, the resistance to faults is attained primarily by the selection and use of suitable components. The safety function may be rendered ineffective by the occurrence of a fault. Category 1 has a greater resistance to faults than Category B owing to the use of special components and principles that are well-tried for safety applications.

In Categories 2, 3 and 4, superior performance in terms of the specified safety function is attained primarily by structural measures. In Category 2, performance of the safety function is generally checked automatically at regular intervals by self-tests performed by technical test equipment (TE). The safety function may fail however should a fault arise between the test phases. By appropriate selection of the test intervals, a suitable risk reduction can be attained with application of Category 2. In Categories 3 and 4, the occurrence of a single fault does not result in loss of the safety function. In Category 4, and where reasonably practicable also in Category 3, such faults are detected automatically. In addition, the resistance to an accumulation of undetected faults is also assured in Category 4.

Consideration of the faults must include an assessment of what component faults may be assumed, and what faults may (with reasoning) be excluded. Information on the faults to be considered is provided in Annex C.

In Categories 3 and 4, common cause failures capable of causing simultaneous failure of more than one channel must also be adequately controlled. The same applies to Category 2, since the test equipment and its dedicated shut-off path also constitute a second channel. Essentially, it can be said that many of the basic and well-tried safety principles are effective not only against random hardware failures, but also against systematic faults that may creep into the product at some point in the product life cycle, e.g. faults arising during product design or modification.

6.2.3 Category B

The SRP/CS must be designed, constructed, selected, assembled and combined for the intended application in accordance with the relevant standards with application of the basic safety principles in such a way that they can resist:

- The expected operating stresses (e.g. reliability with respect to breaking capacity and frequency)
- The influence of the processed material (e.g. aggressive chemical substances, dusts, chips)
- Other relevant external influences (e.g. mechanical vibration, electromagnetic interference, interruptions or disturbances in the power supply)

With regard to electromagnetic compatibility (EMC), the standard refers to particular requirements stated in the relevant product standards, such as IEC 61800-3 for power drive systems. It emphasizes the importance of the requirements for immunity to interference in particular for the functional safety of the SRP/CS. Where no product standard exists, the requirements of IEC 61000-6-2 concerning immunity to interference should at least be observed. Annex K contains a detailed description of EMC and functional safety of machinery.

Table 6.2:
Summary of the requirements for Categories; the three right-hand columns show the essential changes from the Category definition in the first edition of the standard (EN 954-1)

Category	Summary of the requirements	System behaviour	Principle for attainment of safety	$MTTF_D$ of each channel	DC_{avg}	CCF
B	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components	Low to Medium	None	Not relevant
1	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for Category B.	Mainly characterized by selection of components	High	None	Not relevant
2	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system (see Section 6.2.14).	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of the safety function is detected by the check.	Mainly characterized by structure	Low to High	At least Low	Measures required, see Annex F
3	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed so that: • a single fault in any of these parts does not lead to the loss of the safety function, and • whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure	Low to High	At least Low	Measures required, see Annex F
4	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed so that: • a single fault in any of these parts does not lead to the loss of the safety function, and • a single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs, the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC_{avg}). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	High	High including accumulation of faults	Measures required, see Annex F

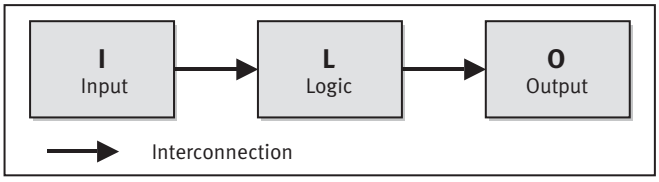
These general principles can be presented, both in general terms and with regard to specific technologies, in the basic safety principles listed in Annex C. The general basic safety principles apply in full here to all technologies, whereas the technology-specific principles are required in addition for the technology concerned. Since Category B is the basic Category underlying all other Categories (see Table 6.2), the basic safety principles must be applied generically during the design of safety-related parts of control systems and/or safeguards.

For components that satisfy Category B, no further special safety measures are required. The $MTTF_D$ of each channel may therefore be low or medium (see below for the definition of "low" and "medium"). Should a component failure occur, it may lead to loss of the safety function. No monitoring measures, including DC_{avg}, are required. Common cause failures are also not relevant on single-channel control systems; no requirements therefore exist with regard to CCF.

Owing to this very rudimentary resistance to failure, the maximum attainable PL of Category B systems is limited to PL b.

The designated architecture for Category B in Figure 6.5 corresponds to a single-channel system with input (I), logic (L) and output (O) levels.

Figure 6.5:
Designated architecture for Category B and Category 1



6.2.4 Category 1

In addition to satisfying the requirements for Category B, for example the application of basic safety principles, Category 1 SRP/CS must be designed and constructed using well-tried components and well-tried safety principles.

A well-tried component for a safety-related application is a component that has been either

- widely used in the past with successful results in similar applications, or
- made and verified using principles that demonstrate its suitability and reliability for safety-related applications.

Annex C provides an overview of known components employing a range of technologies that are well-tried for safety applications.

Newly developed components and safety principles may be considered as equivalent to "well-tried" when they fulfil the second condition stated above. The decision to accept a particular component as well-tried depends on the application. Complex electronic components, such as programmable logic controllers (PLCs), microprocessors or application-specific integrated circuits (ASICs) cannot generally be considered as equivalent to "well-tried".

The well-tried property of a component is dependent upon its application, and indicates only that a dangerous failure is improbable. It follows that the anticipated dangerous failure rate is greater than zero, and is considered in the form of the $MTTF_D$ during calculation of the PL. Conversely, the assumption of a fault exclusion (see subclause 6.2.10) gives rise to assumption of an "infinitely high" $MTTF_D$ that is not considered in the calculation.

Owing to the expected higher component reliability, the $MTTF_D$ of the single channel in Category 1 must be high; as in Category B, however, no requirements are placed upon the DC_{avg} and CCF. The occurrence of a fault can lead to the loss of the safety function. The $MTTF_D$ of the channel in Category 1 is however greater than that in Category B. In consequence, loss of the safety function is less probable, and the maximum PL that can be attained with Category 1 is PL c.

The designated architecture for Category 1 is the same as for Category B (see Figure 6.5), since the differences lie in the component reliability and not in the structure.

6.2.5 Category 2

In addition to the requirements for Category B (e.g. the application of basic safety principles), Category 2 SRP/CS must employ well-tried safety principles and be designed such that their safety functions are tested at reasonable intervals, for example by the machine control system. The safety function(s) must be tested:

- at start-up of the machine, and
- prior to initiation of any hazardous situation, e.g. the start of a new cycle, start of other movements, as soon as the safety function is required, and/or periodically during operation, where the risk assessment and the form of operation indicate that this is necessary.

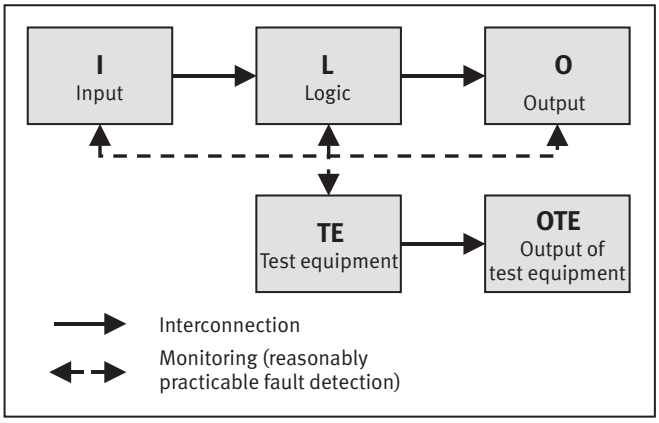
These tests can be initiated automatically. Each test of the safety function(s) must either:

- permit operation, if no faults have been detected, or
- should a fault have been detected, generate an output for the initiation of appropriate control action (OTE).

As a general rule, and always where PL_r = d, the output (OTE) must initiate a safe state that is maintained until the fault has been eliminated. Up to PL_r = c, when initiation of a safe state is not practicable (for example owing to welding of the contacts of the final switching device), a sufficient alternative may be for the output of the test equipment (OTE) to provide only a warning.

For the designated architecture of Category 2 (Figure 6.6), calculation of the $MTTF_D$ and DC_{avg} considers only the blocks of the functional channel (i.e. I, L and O). When the simplified method in the standard is used, the $MTTF_D$ of the blocks of the test channel (i.e. TE and OTE) is considered indirectly, since this method requires the $MTTF_D$ of the test channel to be at least half the $MTTF_D$ of the functional channel. Values from "low" to "high" are permitted for the $MTTF_D$ of the functional channel. The DC_{avg} must be at least "low". Adequate measures against CCF must also be applied (see subclause 6.2.15 and Annex F).

Figure 6.6:
Designated architecture for Category 2; dashed lines indicate reasonably practicable fault detection



The test must not itself give rise to a hazardous situation (e.g. owing to lengthening of the response time). The test equipment may be integral with or separate from the functional channel (see below for further information). Category 2 cannot be applied in some cases, since testing of the safety functions is not possible on all components. Since the safety function can fail unnoticed between tests, the interval between tests is a critical parameter. In addition, the test equipment could itself fail undetected before the functional channel fails. Simplified quantification of the PL by means of the designated architecture and the bar chart (Figure 6.10, Page 61) is therefore subject to the following requirements:

- The $MTTF_D$ value of the test channel is not lower than half the $MTTF_D$ value of the functional channel, and
- The test rate is at least 100 times the mean demand rate upon the safety function (as an exception, at least 25 times as high; see subclause 6.2.14) or testing is performed immediately when a demand is made upon the safety function, and the overall time for detection of the fault and for bringing the machine into a non-hazardous state (the machine is generally stopped) is shorter than the time to reach the hazard (see also EN ISO 13855).

Owing to these restrictions and to the fact that with the designated architecture, a DC_{avg} of over 90% is difficult to attain in practice with external test equipment, undetected first faults may result in loss of the safety function. For these reasons, the maximum PL that can be attained with Category 2 is limited to PL d.

Interpretation of the requirements for a Category 2 presents certain difficulties that can sometimes only be decided on a case-by-case basis. The following recommendations can be made in this respect:

- The standard requires testing of the safety function. Should this not be possible for all components, Category 2 cannot be applied (Note 1 in EN ISO 13849-1:2015, subclause 6.2.5). It thus follows that all components of the functional channel must be tested. The functional channel encompasses all components that can cause failure of the safety function by at least one failure mode. The standard specifies at least a low DC_{avg} for the functional channel.
- "Testing of the safety function" cannot always be performed by testing of the functional channel from input to output. Ideally, it should be performed actively by the test equipment itself, or the test equipment should use components of its own to monitor execution of the safety function passively. In the passive solution, an adequate test rate must be ensured by the application. Alternatively, the blocks (I, L, O) or components in the functional channel can be monitored individually; diagnostics should always be as close as possible to the "actual execution of the safety function".
- The statement that the test equipment may be integral with or separate from the functional channel means that whilst it is permissible for elements of the test equipment performing the test to be located within the functional channel, for example in an SRP/CS consisting of electronics, the part of the test equipment evaluating the diagnostic results must however normally be engineered external to the functional channel, for example in the form of a separate watchdog. Only in this way can the requirements concerning mutual independence of the functional and test channels be satisfied. The diagnostic information for the test equipment should provide adequate information on the safety-related serviceability of the monitored parts of the functional channel. It must therefore exhibit a certain minimum complexity in order to enable the test equipment to reach a sound decision regarding the serviceability. Complete merging of TE with the functional channel is not acceptable, as for example in the case of an on-chip watchdog without the separation described in IEC 61508-2, Annex E (Special architecture requirements for integrated circuits with on-chip redundancy) or test equipment that is engineered only in the form of software and accesses OTE directly by means of a de-energizing signal generated by software.

- Subclause 6.2.14 and Annex E provide further information, in particular on the required test rate, reliability of the test equipment, initiation of the test (automatically, manually, in response to a demand of the safety function) and diagnostics measures.

6.2.6 Category 3

In addition to the requirements for Category B (e.g. the application of basic safety principles), Category 3 SRP/CS must embody well-tried safety principles and be designed such that a single fault does not result in loss of the safety function. Whenever reasonably practicable, a single fault must be detected at or prior to the next demand of the safety function.

Values ranging from low to high may be selected for the $MTTF_D$ of each channel. Since not all faults need be detected or the accumulation of undetected dangerous faults may lead to a hazardous situation, a low DC_{avg} is the minimum requirement. Refer to subclause 6.2.14 for issues relating to the test rate. Adequate measures must be taken against common cause failure (CCF).

The requirement of single-fault tolerance does not necessarily mean that a two-channel system must be implemented, since single-channel components with no potential for dangerous failure (fail-safe design), for example, may also be tolerant of single faults. The same applies to systems with a high standard of monitoring that respond to a fault sufficiently quickly by means of a dedicated shut-off path for a dangerous state to be avoided. Nevertheless, the majority of Category 3 systems are implemented in two-channel form. A corresponding designated architecture was selected for this reason (Figure 6.7). A purely "logical two-channel arrangement", for example employing redundant software on single-channel hardware, will however not generally offer single-fault tolerance of hardware failures.

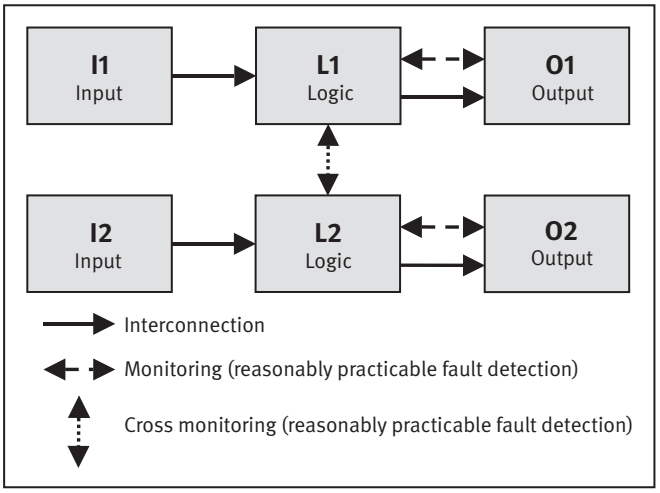
6.2.7 Category 4

Over and beyond the requirements for Category B (e.g. the application of basic safety principles), Category 4 SRP/CS must apply well-tried safety principles and be designed such that:

- a single fault does not result in loss of the safety function, and

- the single fault is detected at or prior to the next demand of the safety function, for example immediately when the machine is switched on or at the end of a machine operating cycle. Should such detection not be possible, the accumulation of undetected faults must not result in loss of the safety function. (In practice, consideration of a fault combination for two faults may be sufficient.)

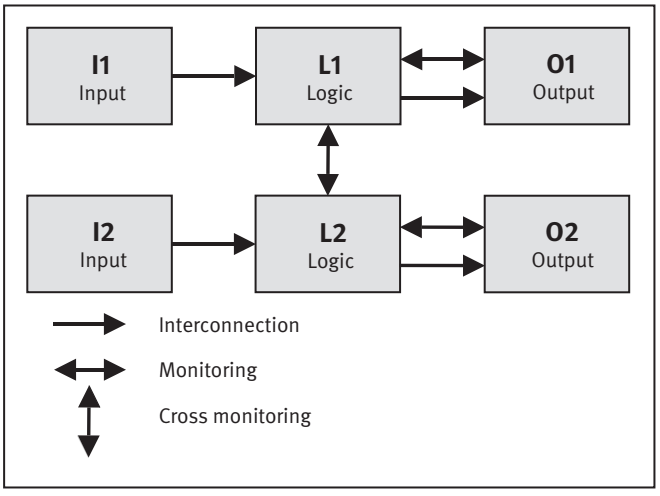
Figure 6.7:
Designated architecture for Category 3: dashed lines indicate reasonably practicable fault detection



Since this is the Category with the greatest resistance to faults (the greatest contribution to risk reduction), both the $MTTF_D$ of each channel and the DC_{avg} must be high (see subclause 6.2.14 for the issue of the test rate), and adequate measures must be taken against CCF.

Since the differences between this Category and Category 3 lie primarily in the $MTTF_D$ and the DC_{avg}, the designated architecture for Category 4 (Figure 6.8) is similar to that for Category 3. The unbroken lines for monitoring symbolize the higher DC_{avg}, however.

Figure 6.8:
Designated architecture for Category 4



6.2.8 Blocks and channels

For simplified quantification of the probability of failure, presentation of the safety-related control in the form of abstracted blocks and channels is helpful. The term

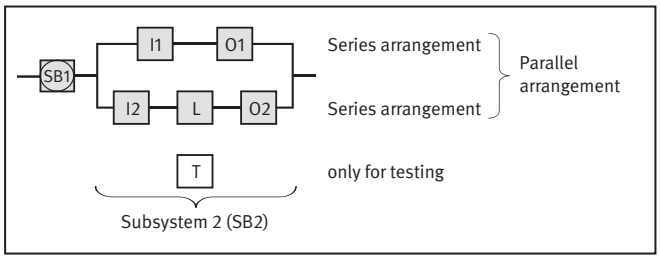
"blocks" has a defined meaning of its own in this context. It refers to function blocks only in the sense that the safety function is executed in smaller units arranged in series and in parallel. The following rules can be stated for mapping of the hardware structure to a safety-related block diagram:

- The blocks should map, in abstract form, all control components that relate to performance of the safety function.
- If the safety function is performed in multiple redundant channels, they should be presented in separate blocks. This reflects the fact that should one block fail, performance of the safety function by the blocks of the other channel is not impaired.
- Division of the blocks within a channel is somewhat arbitrary; although EN ISO 13849-1 proposes three blocks per channel (input level I, logic level L and output level O), this is primarily in the interests of clarity. Neither the precise boundary between I, L and O, nor the number of blocks in a channel significantly affects the probability of failure calculated in the form of the PL.
- The block assignment of each hardware unit relevant to safety must be clearly specified, e.g. in the form of a parts list. This permits calculation of the mean time to dangerous failure ($MTTF_D$) of the block, based upon the $MTTF_D$ of the hardware units belonging to the block concerned (e.g. by failure mode and effects analysis (FMEA) or the parts count method, see subclause 6.2.13).
- Hardware units employed purely for test purposes, failure of which cannot directly impair performance of the safety function in the various channels, may be grouped as a separate block. For Categories 3 and 4, the standard does not set out direct requirements for the reliability of this block; with reference to Category 2, however, a general guideline is that its $MTTF_D$ should be at least half that of the individual (symmetrized, see below) channel, and consideration should also be given to systematic failures and CCF.

6.2.9 Safety-related block diagram

The safety-related block diagram is based upon the more familiar reliability block diagram [33]. Common to both diagrams is the principle that the (safety) function may continue to be performed provided a chain of blocks that have not failed dangerously remains intact from left to right along the functional connecting lines. However, the safety-related block diagram presents additional test mechanisms, such as the cross monitoring of redundant channels, or tests performed by separate test units. A general example of a safety-related block diagram is shown in Figure 6.9.

Figure 6.9:
General example of a safety-related block diagram; I1 and O1 constitute the first channel (series arrangement), whilst I2, L and O2 constitute the second (series arrangement); the safety function is performed redundantly with both channels (parallel arrangement); T is used only for testing



In accordance with this definition, the following rules can be formulated for presentation of a safety-related control system in the form of a safety-related block diagram:

- The arrangement of blocks in series in the form of a "channel" (e.g. blocks I, L and O) expresses the fact that failure of one block may lead to failure of the entire chain. Should for example a hardware unit in a channel fail dangerously, the entire channel becomes unable to execute the safety function.
- A parallel arrangement of blocks or channels symbolizes the multiply redundant performance of the safety function, or of relevant parts of it. For example, a safety function performed by multiple channels is maintained provided at least one channel has not suffered failure.
- Blocks employed for test purposes only, which do not impair performance of the safety function in the different channels should they fail, can be presented as a separate test channel. Although failure of test measures causes the reliability of the system as a whole to be reduced, the effect is initially only minor provided performance of the safety function proper in the individual channels remains assured.

Definition of the blocks and channels goes hand-in-hand with determining of the Category, and is the first step in quantification of the PL. Further values are required for this purpose: the evaluation of the component reliability ($MTTF_D$), of the tests (DC_{avg}), and of the relevance of common cause failures (CCF). Further information on the journey "from the conceptual schematic diagram to the Performance Level", specifically, on deriving the safety-related block diagram, can be found in SISTEMA Cookbook 1 [34]. This cookbook also introduces the term "encapsulated subsystem". This refers to a subsystem for which the manufacturer already states the PL, PFH_D and Category, and the precise internal structure and parameters of which are not transparent. These stated parameters require observance of the conditions for use specified by the manufacturer, which for example may

include the implementation of external diagnostics. It is presented in the safety-related block diagram at subsystem level in single-channel form as a circle within a block (see subsystem "SB1" in Figure 6.9). It contributes to quantification of the PL only through its parameters PFH_D and PL; statement of the Category is merely informative.

6.2.10 Fault considerations and fault exclusion

In a real-case control system, there is no limit whatsoever to the number of theoretically possible faults. Evaluation must therefore be limited to the faults that are relevant. Certain faults can be excluded if the following points are considered:

- The technical improbability of their occurrence (a probability that is several orders of magnitude lower than that of other possible faults and the risk reduction that is to be attained)
- Generally accepted technical experience, irrespective of the application under consideration
- The technical requirements relating to the application and to the specific hazard

The component faults that may occur and those that can be excluded are described in EN ISO 13849-2. The following points must be observed:

- The fault lists constitute a selection only. Where necessary, new fault models must therefore be created (for example for new components), or further fault types considered, depending upon the application. This can be determined for example by means of an FMEA.
- Secondary faults are evaluated as a single fault together with the initial fault giving rise to them, as are multiple faults with a common cause (CCF, common cause failures).
- The simultaneous incidence of two or more faults differing in their cause is considered extremely unlikely, and need not therefore be taken into account.

Further information on fault exclusion can be found in Annex C and in Part 2 of EN ISO 13849. Should faults be excluded without the reason for exclusion being immediately apparent (such as the peeling-off of tracks on a properly dimensioned circuit-board layout), precise reasoning must be stated in the technical documentation.

Provided the relevant conditions are met, fault exclusions are also possible for components, for example for the electrical break contacts and the mechanical actuation of electromechanical position switches or emergency stop devices. The validity of fault exclusions may be limited here to low PLs; refer for example to Table D.8 of EN ISO 13849-2 and Annex D of the present report. If fault exclusion applies, failure rates ($MTTF_D$) and monitoring measures (DC) need not be considered for such components.

6.2.11 Mean time to dangerous failure – $MTTF_D$

The reliability of the individual components from which the control system is constructed makes a decisive contribution to its overall reliability. The $MTTF_D$ (mean time to dangerous failure) is thus also considered in the PL as a reliability value. It is clear that "failure" in this context refers to component defects that result in the implemented function not or no longer being performed. The other parts of the term require explanation, however:

- "Mean" indicates that the value is a statistical mean: it does not refer to a specific component, but is defined as an anticipated value for the mean lifetime of the typical component. In this context, the anticipated value for an individual component can be considered equal to the mean value of a large number of components of the same type. The value is not therefore a guaranteed minimum lifetime in the sense of failure-free period. This approach employing a mean value is also reflected in the fact that the lifetime values are not normally adapted to the conditions of use (e.g. load, temperature, climate), provided the components are employed within the conditions of use specified for them. It is generally assumed here that the higher load in one application of a device is averaged out by a lower load in another application. Should higher loads be anticipated in all applications (e.g. owing to extreme temperatures), however, these conditions must be considered when the $MTTF_D$ is determined.
- "Time" indicates that the reliability is expressed in terms of a time in the sense of a lifetime. The $MTTF_D$ is generally indicated in years (abbreviated "a"). Other forms of notation that may be converted to an $MTTF_D$ include failure rates or (switching) cycles. Failure rates are generally indicated by the small Greek letter λ (lambda) and expressed in the unit "FIT" ($= 10^{-9}$/h, i.e. failures per billion component hours). The relationship between λ_D and $MTTF_D$ is expressed, at a constant failure rate λ_D over the lifetime, as $MTTF_D = 1/\lambda_D$. The conversion from hours to years must of course be considered. For components that wear primarily as a result of their mechanical operation, the reliability is usually expressed in switching cycles, for example as a B_{10D} value, i.e. the mean number of cycles until 10% of the components fail dangerously. The $MTTF_D$ can be calculated in this case by consideration of the mean number of operations per year n_{op} that are anticipated in the application concerned. For more details, refer to Annex D.

- "Dangerous" indicates that only failures that impair performance of the safety function are ultimately considered for the PL (unsafe failure). By contrast, safe failures may well cause the safe state to be assumed (operating inhibition) or reduce the availability or productivity of a machine, but the safety function is nevertheless executed properly, or the safe state initiated/maintained. In redundant structures, however, the "dangerous" attribute refers to each individual channel. Should a failure in one channel result in the safety function being rendered inoperative, the failure concerned is considered dangerous, even where a further channel is still able to perform the safety function successfully.

An $MTTF_D$ may be stated both for an individual component, such as a transistor, valve or contactor, and for a block, a channel, or the control system as a whole. This overall $MTTF_D$ represents the value for a channel, possibly symmetrized over several channels, and is based upon the $MTTF_D$ of all components involved in the SRP/CS. In accordance with the bottom-up principle, the unit under consideration is successively enlarged. In the interests of minimizing effort, it is often advantageous only for safety-related components to be considered in the analysis, i.e. components the failure of which could have an indirect or direct negative influence upon performance of the safety function. For simplification purposes, fault exclusions are possible in addition; these take account of the fact that certain failures are extremely improbable and their contribution to the overall reliability negligibly small. The assumption of fault exclusions is however subject to certain conditions; these are set out in detail in EN ISO 13849-2 and described more comprehensively in subclause 6.2.10. Conductor short circuits or certain mechanical failures can for example be excluded on the basis of the design, provided certain conditions are met.

6.2.12 Data sources for individual components

One of the questions most frequently posed in this context concerns the sourcing of reliable failure data for the safety-related components. The manufacturer, and for example his technical data sheet, should be given preference here over all other sources. Many manufacturers, for example of electromechanical or pneumatic components, now make such information available. Where data are not available from the manufacturer, typical example values can still be obtained from established databases (see Annex D). Such sources do not generally distinguish between dangerous and safe failures; it can however be assumed as a general approximation that on average, only half of all failures are dangerous. With consideration for the problem of obtaining reliability values, EN ISO 13849-1 lists a number of typical values. These are however very conservative estimates, and their use is therefore recommended only if the data sources indicated above are not available. In addition to $MTTF_D$ values for mechanical, hydraulic and electronic components, the standard also contains B_{10D} values for pneumatic and electromechanical components. Details are described in Annex D.

A convenient source of reliability data for components intended for use in safety-oriented control systems are the large number of available SISTEMA libraries (see Annex H). These contain $MTTF_D$ or B_{10D} values for elements and components, and PL and PFH_D values for entire subsystems.

6.2.13 FMEA versus the parts count method

Once the $MTTF_D$ values of all safety-related components have been obtained, certain simple rules can be used to calculate the $MTTF_D$ value of the control system from them. A number of methods can be used for this purpose: complex, with the use of a precise failure mode and effects analysis (FMEA), or fast and simple by means of the parts count method, involving minor estimations erring on the safe side. This begins with the small difference between *MTTF* and $MTTF_D$: what proportion of failures of a certain component are dangerous? All conceivable failure modes can be listed in a complex FMEA, evaluated as either "safe" or "dangerous", and the fraction of their occurrence estimated. Since the effects of a component failure upon the block determine whether the failure mode is safe or dangerous, detailed analyses of the effect caused by a failure may be necessary. A greater number of failure modes may then prove to be "safe" than is the case with a simplified assessment, as proposed by EN ISO 13849-1: if the parts count method is used, its conservative approach assumes that overall, the safe and dangerous failures are similar in number. In the absence of more detailed information, the $MTTF_D$ is therefore always assumed with this method to be double the *MTTF*.

Once again, the principle is that of the statistical mean, i.e. an excessively favourable evaluation of one component is cancelled out by an overly pessimistic evaluation of another. It is quite possible for the parts count method and an FMEA to be combined. Where the values produced by a parts count alone yield a sufficiently low *PFH*, an FMEA need not be performed. Should this not be the case, however, a study of the failure modes is advantageous, for example by means of a partial FMEA, particularly on the components exhibiting poorer $MTTF_D$ values. Further explanations of this subject can be found in Annex B.

As with other methods of quantification, evaluation to EN ISO 13849-1 assumes a constant failure rate throughout the mission time of the component for all $MTTF_D$ values. Even if this does not directly reflect the failure behaviour, as for example in the case of components subject to heavy wear, an approximate $MTTF_D$ value that remains valid throughout the component's mission time

is nevertheless determined in this way by an estimation erring on the safe side. Early failures are generally disregarded, since components exhibiting pronounced early failure patterns do not satisfy the availability requirements for a machine control system and are therefore not generally significant on the market. The advantage of this procedure is that the $MTTF_D$ is always equal to the reciprocal of the associated dangerous failure rate λ_D. Since the dangerous failure rates λ_D of the components in a block can simply be added together, the $MTTF_D$ values of the components involved (N components with running index i) give rise to the $MTTF_D$ of the block as follows:

$$\lambda_D = \sum_{i=1}^{N} \lambda_{Di} \text{ bzw.} \frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}} \quad (1)$$

The same relationship applies to calculation of the $MTTF_D$ of each channel from the $MTTF_D$ values of the associated blocks. Once the $MTTF_D$ for each channel is known, a further simplification is made in the form of a classification. The calculated values are assigned to three typical classes (Table 6.3).

Table 6.3:
Classification of the $MTTF_D$ of each channel

$MTTF_D$ for each channel	
Description	**Range**
Not suitable	0 years ≤ $MTTF_D$ < 3 years
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years
Permissible only in Category 4	100 years < $MTTF_D$ ≤ 2,500 years

A mean (important: not guaranteed) lifetime of less than three years is deemed not reasonable for safety engineering components. Other than for Category 4, values exceeding 100 years may not be substituted; this prevents the component reliability being overstated in comparison with the other main influencing variables such as the structure or tests. Should a figure of less than three years actually be produced for a channel, the components should be replaced with more reliable alternatives, since even PL a cannot otherwise be attained. Values over 100 years for the mean lifetime are not unusual, but owing to "capping", do not have any bearing upon the PL above this value, since the maximum value of 100 years (the maximum value in Category 4 is 2,500 years) is substituted in this case for the component reliability.

If several channels are involved in a control system, it is not initially clear which value should be employed as representative for the entire system. A cautious approach would of course be to take the lower value; results that are better whilst still being safe are however produced by the following averaging formula (C1 and C2 refer here to the two channels, which are symmetrized):

$$MTTF_D = \frac{2}{3}\left(MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right) \quad (2)$$

Where the channels concerned are balanced, the $MTTF_D$ value calculated in this way corresponds to the $MTTF_D$ value of one channel. Where they are imbalanced, the result is an average $MTTF_D$ than can be no less than two-thirds of the better value. In this scenario, the effect may arise in addition that the better value was previously capped to an $MTTF_D$ of 100 years (2,500 years in the case of Category 4), and as a result the symmetrized value is less than 100 years (2,500 years for Category 4). It is therefore generally more effective to implement channels of balanced reliability wherever possible. Irrespective of the number and form of the channels, this method always produces an $MTTF_D$ value for a single control channel which, averaged over the control system, indicates the level of component reliability.

6.2.14 Diagnostic coverage of test and monitoring measures – *DC*

A further variable with a major influence upon the PL are the (self-)test and monitoring measures in SRP/CS. Effective tests for example permit some compensation to be made for poor reliability of the components. The quality of the tests is measured in EN ISO 13849-1 by the diagnostic coverage (*DC*). The *DC* is defined as the proportion of detected dangerous failures among all conceivable dangerous failures. The reference quantity may be a component, a block, or the entire SRP/CS. In the last of these cases, the *DC* is the average diagnostic coverage DC_{avg}, which has an important function in the simplified quantification of the PL by means of the bar-chart method.

As at many other points in the standard, two methods exist for calculation of the DC_{avg}: one more precise but more complex; the other simpler, involving a series of estimations erring on the safe side. The precise, complex method involves a failure mode and effects analysis (FMEA) and is based upon the *DC* definition. In this case, the dangerous detectable (DD) and dangerous undetectable (DU) failure modes for each component are determined, together with their proportions of the total failure rate of the component. Finally, summation and formation of the ratio produces the *DC* value for the unit under consideration:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} = \frac{\sum \lambda_{DD}}{\sum \lambda_{D}} \quad (3)$$

The method favoured by EN ISO 13849-1 is based upon a reasoned conservative estimate of the *DC* directly on the component or block level, followed by calculation of the DC_{avg} from the individual *DC* values by means of an averaging formula. Many tests can be classified as typical standard measures for which estimated *DC* values are listed in Annex E of the standard. These measures are assigned a coarse system comprising four key values (0%, 60%, 90% and 99%). A comprehensive list of the typical test measures stated in the standard can be found in Annex E. Application is explained with reference to the example of the control system of a paper-cutting guillotine (see subclause 6.5).

A number of boundary conditions must be observed for calculation of the *DC* of a component or block:

- Detection of a dangerous failure is only the beginning. In order for the test to be passed, a safe state that presents no further hazard must be initiated in time. This includes an effective shut-off path, which for example in the case of single-channel tested systems (Category 2) entails a requirement for a second shut-off element. This is required in order to initiate and maintain the safe state when the test has detected failure of the normal shut-off element (block "O" on the safety-related block diagram). Only where the risk is low (up to PL_r = c) and when initiation of a safe state is not possible (for example owing to welding of the contacts of the final switching device) may it be sufficient in Category 2 for the output of the test equipment (OTE) only to provide a warning.

- The initiation of a test, its performance, and the necessary shut-off process should ideally be performed automatically by SRP/CS. Only in exceptional cases is it acceptable to rely here upon manual intervention, for example by the machine operator, since experience in practice shows that the necessary measures are often not adequately implemented, whether out of idleness, or owing to pressure of work or poor information or organization. Effective implementation of manual tests involves greater involvement in the work process, or greater organizational effort and discipline. Calculation of the *DC* nonetheless takes account of fault detection when a demand is made upon the safety function, i.e. consideration is not limited to tests initiated automatically by programmable electronics; electromechanical components such as relays or contactors constitute classic cases in which the fault of a "failure to drop out" can typically be detected only when a demand is made upon the safety function. Where faults are to be detected in the event of a demand, the frequency must be considered with which a demand is made upon the safety function, in order to ensure an adequate test rate, as described in the next point.

- A further aspect is the question of the necessary test rate. A test that is not executed sufficiently frequently may under certain circumstances be overtaken by the incidence of a hazardous event, and may therefore create a false sense of safety. As a rule of thumb, the test rate is always in competition with other frequencies; for this reason, a generic adequate frequency cannot be stated. Furthermore, tests have the function of revealing not only random but also systematic failures.

  On Category 2 single-channel tested systems, the test must be passed before a demand is next made upon the safety function, i.e. before a potential hazard arises. In this scenario, the test rate is therefore in competition with the frequency of the demand of the safety function. In this case, a factor of 100 is considered sufficient, i.e. a test rate that is at least 100 times the mean demand rate upon the safety function. By contrast, down to a factor of 25, the maximum increase in the probability of failure is approximately 10% (refer also to subclause 4 in [32]). Below this level, the synchronization of demand and testing essentially determines whether testing even takes effect. Should, in single-channel tested systems, the test be executed simultaneously with the demand of the safety function and so quickly that the safe state is attained before a hazard arises, no conditions are imposed upon the frequency of testing. (This applies – with reference to the recommendations stated below for the test rate in two-channel systems – provided at least one demand per year can be assumed.) A special example of this is continuous testing (e.g. analogue overvoltage/undervoltage monitoring), for which the requirements for the test rate are always met when the safe state is attained sufficiently swiftly.

  In two-channel Category 3 and 4 systems, the test rate is in competition with the frequency of incidence of a second dangerous failure, since only if the second channel fails before a test has detected the failure of the first channel does a danger exist of the safety function not being executed. As per the definition, Category 4 systems even tolerate the accumulation of undetected faults. In practice, a range of recommendations exist for the minimum necessary test rate in Categories 3 and 4.

  IEC 61800-5-2 [20] governing the safety of electrical power drive systems considers the following minimum diagnostic test frequencies acceptable for the case in which testing cannot be performed without interruption of the machine's working cycle and in which no reasonable technical solution can be implemented: one test per year for PL d with Category 3, one test every three

months for PL e with Category 3, and one test per day for PL e in Category 4.

In EN ISO 14119 [35] and a "Recommendation for Use" by the notified test bodies in the machinery sector [36], an automatic or manual test is required at the following intervals for electromechanical outputs (relays or contactors): at least once per month for PL e with Category 3 or 4 and at least once every twelve months for PL d with Category 3. The test should preferably be performed automatically; alternatively, the test interval may be monitored automatically. Only in exceptional cases should it be assured by organizational measures.

At the test rates stated here, these are minimum requirements that apply when more frequent tests are not possible, for example because the test can be performed only when a demand is made upon the safety function (for which a signal change is required, as for example with electromechanical or fluid power technology), or because an interruption in the machine's work cycle is required, as for example when the machine is started at the beginning of the shift. Automatic tests that are not subject to these constraints, such as processor or memory tests in electronic systems, can often be implemented at substantially higher frequency without major overhead. In these cases, testing at least once per shift for Category 3 has proved suitable in practice; in Category 4, a minimum test rate of once per hour was already selected when EN 954-1, the predecessor standard, was in force.

- A further point is the reliability of the test equipment itself. For this, the standard sets out only the basic requirements of Category B, applicable to all Categories, i.e. compliance with the relevant standards in order for the anticipated influences to be withstood, and the application of basic safety principles. Well-tried safety principles should also be applied to the extent possible. Where dangerous failures of the test equipment are detected by its cyclical incorporation into the process, deviation from these basic requirements is permissible. An additional general requirement is that the test equipment should not fail prior to the components that it monitors. At the same time, it is inefficient for much greater investment to be made in the reliability of the test equipment than in the safety equipment performing the safety function proper. EN ISO 13849-1 therefore imposes only limited requirements upon the reliability of the test equipment. For Categories 3 and 4, reliance is upon single-fault tolerance, since including failure of the test equipment, a total of three dangerous failures must occur before the safety function ceases to be performed. The occurrence of such a case unobserved is considered extremely unlikely and not therefore critical. For Category 2, a secondary condition exists – at least with the simplified procedure for determining of the PL by means of the bar chart – that was set out during calculation of the "Category 2 bars": in this case, the dangerous failure rate of the test channel should be no more than twice the dangerous failure rate of the functional channel that it monitors.

- The effectiveness of a given test measure, for example fault detection by the process, may depend heavily upon the application, and can vary anywhere between 0 and 99%. Particular care must be taken here during selection of one of the *DC* key values. Further explanations can be found in Annex E.

- Position switches connected in series, where present, must be considered during determining of the DC_{avg} value for electromechanical contacts. Masking of faults may occur in such cases, requiring reduction of the DC_{avg} value and the attainable PL. Details can be found in Annex E.

- A situation is possible in which components or blocks are monitored by several tests, or in which different tests act upon different components, with the result that an overall *DC* must be determined for the component or the block. Annex E provides assistance in these issues.

- The DC_{avg} formula (4) provides a means of calculation in which blocks with different *DC* values are grouped in such a way that the minimum DC_{avg} requirements for the attained Category are met even though individual blocks have a *DC* below 60%, or even no diagnostics at all (*DC* = 0%). In such cases, it must be determined on a case-by-case basis whether this form of implementation is consistent with the requirements of the Category. Category 3 requires for example that wherever reasonably possible, a single fault must be detected at or prior to the next demand of the safety function. For Category 2, a "check of the safety function" is a generic requirement. Category 4 also requires detection of the discrete fault, and only "if this detection is not possible" that the safety function also be performed in the event of an accumulation of undetected faults.

- With regard to programmable electronic systems in particular, a large number of complex faults is conceivable; corresponding requirements must therefore also be placed upon the complexity of the tests. In this case, should a *DC* of over 60% be required for the (programmable or complex) logic, EN ISO 13849-1 calls for at least one measure for variable memory, invariablememory and the processing unit – where present – with a *DC* of at least 60% in each case.

Once the *DC* values of all blocks are known, the DC_{avg} value for the system is calculated by means of the approximation formula (4). This formula weights the individual *DC* values with the associated $MTTF_D$ values, since very reliable parts (with a high $MTTF_D$) are less reliant upon effective tests than less reliable parts (the sums in numerators and denominators are formed across N blocks of the entire system):

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}} \qquad (4)$$

Once obtained, the DC_{avg} constitutes a value describing the quality of the test and monitoring measures averaged over the entire SRP/CS. Before this value can be substituted in the simplified quantification of the PL together with the Category (five classes) and the $MTTF_D$ of each channel (three classes), it must be assigned to one of the four classes in Table 6.4.

Table 6.4:
The four classes of diagnostic coverage in accordance with the simplified approach of EN ISO 13849-1

Diagnostic coverage (*DC*)	
Description	**Range**
None	$DC < 60\%$
Low	$60\% \le DC < 90\%$
Medium	$90\% \le DC < 99\%$
High	$99\% \le DC$

When the DC_{avg} is subsequently used in the simplified quantification involving the bar chart (see subclause 6.2.16), only the respective lower key value of a DC_{avg} class (0, 60, 90 or 99) is used. A further simplification thus takes effect here, based upon an estimation erring on the safe side.

In specific cases, this coarsely simplified system may however give rise to paradoxes, if for example an unreliable component with an above-average *DC* for the SRP/CS is replaced by a more reliable component (for a more detailed explanation, refer to the end of Annex G).

6.2.15 Measures against common cause failure (CCF)

The final parameter relevant to the simplified quantification of the probability of failure concerns common cause failures (CCF). Such failures are related dangerous failures, for example in both channels of a redundant SRP/CS, that are attributable to a common cause. Examples include unfavourable environmental conditions or overloads that were not adequately addressed during design of the control system. Should the channels not be adequately separated, dangerous secondary faults may occur that render the intended single-fault tolerance ineffective. The quantitative relevance of these effects in a specific system is difficult to estimate (refer also to Annex F). In Annex D of IEC 61508-6 [37], the "beta-factor" model is used for this purpose. In this model, the rate of common cause failure is placed, as $\beta \cdot \lambda_D$, in relation to the dangerous failure rate of a channel λ_D. Without a precise FMEA, β can at best only be estimated for real-case SRP/CS, however. For this purpose, EN ISO 13849-1 contains a checklist of eight important counter-measures, for which between 5 and 25 points are awarded:

- Physical separation between the signal paths of different channels (15 points)
- Diversity in the technology, the design or the physical principles of the channels (20 points)
- Protection against possible overloading (15 points)
- Use of well-tried components (5 points)
- Failure mode and effects analysis during development, for the identification of potential common cause failures (5 points)
- Training of designers/maintainers in CCF and its avoidance (5 points)
- Protection against common cause failures triggered by contamination (mechanical and fluid power systems) and electromagnetic interference (electrical systems) (25 points)
- Protection against common cause failures triggered by unfavourable environmental conditions (10 points)

The points stated for a given counter-measure are to be awarded either in full, or not at all; no points are awarded for a "partial" implementation of the counter-measures. Different packages of measures may however be effective against CCF at subsystem level. Should all eight counter-measures be satisfied, a maximum total of 100 points is awarded. However, EN ISO 13849-1 requires only a minimum total of 65 points and even then, only for SRP/CS in Categories 2, 3 and 4. In Category 2 systems, the objective is the avoidance of dangerous common cause failures in test and functional channels that could give rise to an undetected occurrence of a dangerous fault. During creation of the bar chart for simplified quantification, the 65 points were equated to a beta factor of 2%. The coarse approximation with respect to the five Categories and the three $MTTF_D$ and four DC_{avg} classes was carried further and reduced to a simple yes/no decision. Whereas the bene-

fits of a redundant structure are wiped out almost completely even at a beta factor of 10% or higher, a beta factor of no more than 2% reduces the relevance of common cause failures to a justifiable level.

6.2.16 Simplified determining of the PL by means of the bar chart

Even when the four essential quantitative parameters for calculation of the probability of failure have been resolved, determining the PL attained for the SRP/CS from them is still a difficult task. Although in principle, any suitable method is permitted, EN ISO 13849-1 proposes a simple graphical method that is based upon more complex calculations and estimations erring on the safe side: the bar-chart method (see Figure 6.10).

This diagram was generated by *Markov* modelling based upon the designated architectures for the Categories; further details can be found in Annex G. When the bar chart is used, the relevant bar is first determined on the horizontal axis from the attained Category in combination with the attained DC_{avg} class. Adequate measures against CCF must be provided for Categories 2, 3 and 4 in this case. The level of the $MTTF_D$ attained by the SRP/CS on the selected bar determines the PL, which can be read off on the vertical axis. This method permits rapid qualitative estimation of the attained PL even in the absence of precise quantitative data. Should more precise values be required, for example not only the PL, but also a value for the average probability of a dangerous failure per hour PFH_D, the tables in Annex K of the standard provide assistance. Similar assistance is also provided by the IFA's SISTEMA software (see Annex H), which analyses the bar chart quantitatively, and by the IFA's user-friendly PLC disc [16].

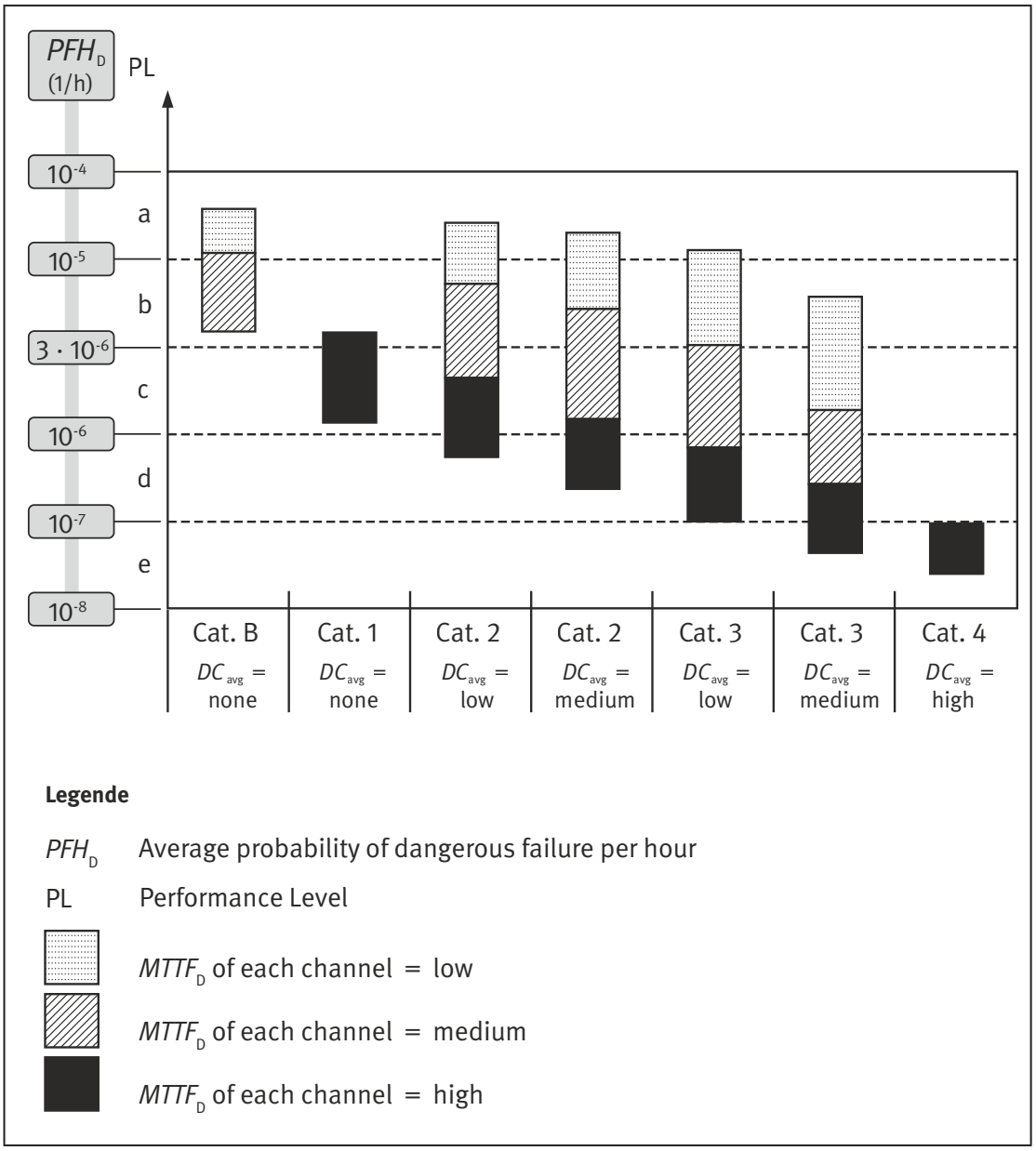


Figure 6.10: Bar chart for simplified determining of the PL from the Category (including measures against CCF), the DC_{avg} and the $MTTF_D$

During creation of the bar chart, consideration was not only given to designated architectures; certain conditions were also laid down that must be observed when the chart is applied:

- A mission time of 20 years is assumed for the SRP/CS, within which the component reliabilities can be described or approximated by constant failure rates. The actual mission time may fall below the assumed 20 years owing to the use of components subject to severe wear (refer to the T_{10D} value in Annex D) or for other reasons. Application of the bar chart is justified in such cases by preventive replacement of the affected components or SRP/CS. This information must be made available to the user in a suitable form, for example in the information for use and by marking on the SRP/CS. Exceeding of the mission time of 20 years from the outset or its extension retrospectively beyond 20 years result in deviations from the bar chart. Annex G shows how this can be addressed.

- In the bars for Category 2, it has been assumed that the test rate is adequately high (refer also to subclause 6.2.14 and Annex E) and also that the test channel is at least half as reliable as the functional channel.

Owing to capping of the $MTTF_D$ that can be allowed for each channel to 100 years (2,500 years in the case of Category 4), a high PL can be attained only with certain Categories. Although this is related to the simplified approach of the designated architectures and the bar chart, the associated limitations also apply when the average probability of a dangerous failure per hour is calculated by means of other, unrelated methods. As already mentioned, the architecture imposes the following limitations upon certain Categories. These limitations are intended to prevent the component reliability from being overstated in comparison with the other influencing variables:

- In Category B, a maximum PL of b can be attained.
- In Category 1, a maximum PL of c can be attained.
- In Category 2, a maximum PL of d can be attained.
- In Categories 3 or 4, even a PL of e can be attained.

Besides the quantitative aspect of the probability of failure, qualitative aspects must also be considered for attainment of a given PL. Such aspects include systematic failures (see subclause 6.1.2), and software faults, which are discussed in greater detail in subclause 6.3.

6.2.17 Determining the PL for the output part of the SRP/CS (power control elements) in accordance with subclause 4.5.5 of the standard

In response to calls voiced by industry, an alternative, simplified method for determining the PFH_D and quantifiable aspects of the PL was added in the third edition of the standard. This method, described in subclause 4.5.5 of the standard, can be applied only in certain cases, namely:

- for the output part of the SRP/CS (power control elements) and

- when no application-specific reliability data ($MTTF_D$, failure rate λ_D, B_{10D} or similar) are available for mechanical, hydraulic or pneumatic components (or components employing mixed technology, such as a pneumatically driven mechanical brake).

This simplified determining of the PFH_D is based primarily upon the implemented Category including DC_{avg} and CCF. Calculation of the (channel) $MTTF_D$ is not required; in return, well-tried components (in Categories 1, 2, 3 and 4) or proven-in-use components (in Categories 2, 3 and 4) must be used throughout. “Proven-in-use” is a new component property used within the standard and should not be confused with the property of well-tried. The property of proven-in-use is demonstrated based upon an analysis of experience gained in the field with a specific configuration of a component in a specific application. The analysis must show that the probability of dangerous systematic faults is sufficiently low for each safety function using the component to reach its required Performance Level PL_r (new definition in 3.1.39 of the standard). Such a demonstration has not been common in machine construction before now. It is also unclear why the requirement refers only to systematic faults, and fails to consider the random component faults.

Table 6.5 shows the estimated PFH_D value and the PL attainable with it, based upon Table 7 in the new subclause 4.5.5 of the standard, as a function of the implemented Category and subject to the additional conditions placed upon the method.

The method is subject to the following additional conditions:

- Since the estimated PFH_D values are based upon the simplified method for estimation of a PL (bar chart), the same conditions apply as for the designated architectures. A mission time of 20 years and constant failure rates within the mission time are assumed. In

Table 6.5:
PL and PFH_D as an estimation erring on the safe side based upon the Category, DC_{avg} and the use of well-tried or proven-in-use components

	PFH_D in 1/h		Category B	Category 1	Category 2	Category 3	Category 4
PL b	$5.0 \cdot 10^{-6}$	⇦	●	○	○	○	○
PL c	$1.7 \cdot 10^{-6}$	⇦	–	●	●	○	○
PL d	$2.9 \cdot 10^{-7}$	⇦	–	–	–	●	○
PL e	$4.7 \cdot 10^{-8}$	⇦	–	–	–	–	●
●	Applied Category is recommended						
○	Applied Category is optional						
–	Category is not permissible						
Further conditions apply, see Section 6.2.17							

Category 2, the tests must be performed adequately frequently. No provision is made here for a test rate that is only 25 times the demand rate.

- In Category 1: use of well-tried components and well-tried safety principles (as in the past and as established in the Category 1 definition).
- In Category 2: the $MTTF_D$ of the test channel is at least ten years.
- In Categories 2, 3 and 4: use of well-tried or proven-in-use components and use of well-tried safety principles. In Category 2, there is no advantage in extending this requirement to the test channel, since the same result (PFH_D and PL) can be attained with a Category 1 single-channel system.
- In Categories 2 and 3: adequate measures against CCF, and *DC* of each component at least “low”.
- In Category 4: adequate measures against CCF, and *DC* “high” for each component.

The *DC* requirement in the last two of these points applies to each component in the subsystem, and therefore exceeds their respective generic requirements for the Category, which relate to DC_{avg}. Since however this concerns the output part of the SRP/CS with mechanical, hydraulic or pneumatic components, only one component per channel will be involved in most cases. Consequently, the requirement for the *DC* of each component does not in practice constitute tightening of the requirements compared to the DC_{avg} of the subsystem.

The following additional information is provided:

- Category 1: the machine manufacturer must determine the T_{10D} values of safety-related components based upon data for their proven-in-use property, unless failure of these components becomes apparent through the technical process.
- Categories 2, 3 and 4: since recourse cannot be made to formula E.1 of the standard (formula (4) of the present report) for calculation of the DC_{avg} owing to the unavailability of $MTTF_D$ values, the DC_{avg} is formed in this case simply as the arithmetic mean of the individual *DC*s of all components in the functional channels of the output part.

6.2.18 Bus systems as “interconnecting means”

The discrete blocks of a designated architecture – input unit, logic and output unit – must be connected together not only logically, but also physically. For this purpose, the standard defines “interconnecting means”, which are regarded as part of the SRP/CS. The term “interconnecting means” may initially appear strange in the field of electrical or fluid power technology. However, it serves as a generic term for electrical and fluid power lines, and even for such components as mechanical plungers. All requirements of the standard therefore also apply to these forms of “interconnecting means”. In the context of fault consideration, a conductor short circuit for example is an assumed fault. What is the situation however when bus systems are used to transmit safety-related information? Detailed consideration of such a complex subject is of course outside the scope of the standard, particularly since the subject is already covered by DGUV test principles (GS-ET-26, [38]) and a standard (IEC 61784-3 [39]). Bus systems that satisfy the requirements set out in these publications can also be readily employed in the context of EN ISO 13849-1. Numerous bus systems suitable for safety-related applications are already available on the market.

The publications referred to above employ a special fault model in which consideration is given to the use of a black-box channel for the transmission of safety-related data: in other words, no particular requirements for fault detection, for example, are placed upon this transmission channel itself. The model assumes the repetition, loss, insertion, incorrect sequence, corruption and delay of safety-related messages and the coupling of safety-related and non-safety-related messages as possible faults. Further possible aspects include faults that systematically corrupt messages, for example by completely inverting them. Measures in "safety layers" that are then implemented in safety-related parts of control systems enable transmission faults to be excluded with sufficient probability. Suitable measures include, for example, the sequence number, timestamp, time expectations, connection authentication, feedback message and data integrity assurance. Data integrity assurance in particular frequently entails complex calculations. The purpose of these calculations is to determine the residual error probability R, and from it the residual error rate Λ (derived from the lower-case λ for the failure rate for components). Exactly this value can then be calculated as the average probability of a dangerous failure per hour required for a PL as a proportion for the transmission of safety-relevant messages. Both of the above publications limit the residual error rate to 1% of the maximum permissible value for the probability of a dangerous failure per hour. Values stated by manufacturers are in fact frequently related to an SIL (see Chapter 3); in practice, however, these values are compatible for use under a required PL (see also Figure 3.2). The 1% rule results in the contribution to the probability of a dangerous failure per hour being virtually negligible, i.e. it enables it to be added to the values determined for the SRP/CS. Comprehensive information on bus systems for the transmission of safety-related information can be found for example in [40].

Where a bus system (i.e. its components), which is generally tested by an independent body, is employed for the implementation of safety functions, planning of its use and proper implementation with regard to fault avoidance are of great importance. A large number of parameters must be set correctly; this process is supported to a greater or lesser degree by relevant tools.

Should none of the known, already assessed profiles for functional safety be used, the assumed transmission errors stated above must be considered, suitable (counter) measures implemented, and the residual error rate Λ in consideration of the typical bit error rate of 0.01 considered during calculation of the total failure probability PFH_D. Test principles GS-ET-26 [38] provide information on calculation of the residual error rate Λ.

6.3 Development of safety-related software

Comments such as the following are frequently heard: "*Of course, a software programmer with years of experience no longer makes mistakes.*" This hubris is in fact the greatest mistake of all. Software is generally complicated, which is why the number of failures caused by software faults is on the rise, in contrast to the situation for hardware. How often are PC users surprised when a computer peripheral ceases to work, and how often does the problem turn out to have been caused by a part of the software that was not compatible with another piece of software, such as a driver? By contrast, hardware tend to be rare. According to [41], normal software, i.e. simple software for simple functions, contains approximately 25 errors per 1,000 lines of code. Also according to [41], well written software contains around two to three errors per 1,000 lines of code, and the software employed in the Space Shuttle has (according to NASA) fewer than one error per 10,000 lines. What does this mean in practice? A mobile telephone has up to 200,000 lines of code and therefore up to 600 software errors. A PC operating system has 27 million lines of code and therefore up to 50,000 errors; the Space Shuttle up to 300 errors; and the software for the Space Defense Initiative (SDI) up to 10,000 errors. These programming errors lie dormant in the products until, under certain conditions and in certain situations, they impact upon the products' function. Like no other technology, software and therefore also its programmers assume a greater responsibility than ever before.

One of the essential changes in EN ISO 13849-1 compared to its predecessor, EN 954-1, was the formulation for the first time of requirements concerning software and its development. For the sake of emphasis at this point: the requirements in subclause 4.6 of the standard enable safety-related software to be developed for all SRP/CS in the machinery sector and for all required Performance Levels from a to e. This subclause is intended in the first instance for application programmers tasked with developing the safety functions for a machine, for example in an application-oriented language on a programmable logic controller (PLC). By contrast, these requirements in EN ISO 13849-1 are not particularly new to developers of SRESW (safety-related embedded software), i.e. firmware or software tools for electronic safety components. Such "embedded software" developments for the components, which are generally certified, are often subject to the very complex requirements of the IEC 61508-3 basic safety standard [42] (and its further seven parts), which is binding for IEC standards governing functional safety.

IFA Report 2/2016 on safety-related application software for machinery [43] has been published, addressing the programming of SRASW (safety-related application software). This report describes the IFA's matrix method for the specification, verification, validation and documen-

tation of SRASW. The matrix method can also be used with the IFA's SOFTEMA tool [44]. In addition, the report provides detailed further information on the programming of SRASW. The descriptions below are therefore limited to a brief presentation of the normative requirements of EN ISO 13849-1 concerning safety-related software.

The basic principles of this subclause can be applied to both software types. Individual requirements tend to be formulated in detail more for application programming of SRASW. Conversely, the example described in subclause 6.5 of a control system for a paper-cutting guillotine shows the development of SRESW.

The requirements governing software development are geared to the software type (SRASW or SRESW) and the language type. As in other current standards containing requirements for software, a distinction is drawn between the language types FVL (full variability language) and LVL (limited variability language). SRASW is generally programmed in LVL, for example in a graphical language as defined in IEC 61131-3. The requirements contained in subclause 4.6.3 of EN ISO 13849-1 apply in this case.

As soon as SRASW is programmed in FVL (for example, a PLC in the high-level language "C"), however, the requirements for SRESW contained in subclause 4.6.2 of the standard must be met. If the SRASW is required to satisfy a Performance Level of e in this case, EN ISO 13849-1 refers at the end of subclause 4.6.2, once only, but with exceptions, to the requirements of IEC 61508-3:1998.

6.3.1 Error-free software ...

... unfortunately does not exist in the real world. In contrast to hardware faults, which occur as a result of random component failure, the causes of software faults are systematic. It is therefore all the more important that all reasonable steps be taken to avoid errors during the development of safety-related software, the purpose of which is after all that of minimizing risks. What is considered reasonable is determined on the one hand by the required Performance Level PL_r. At the same time, safety-critical faults tend to creep into particular phases of software development, where, devastatingly, they remain undetected until they cause a failure in operation. These phases are known to be those of specification, design and modification. The requirements of EN ISO 13849-1 – and the explanations provided in this subclause – are therefore aimed in particular at fault avoidance in these phases. Sadly, less attention is often paid in practice to these phases of application programming.

In order for the safety-related software produced to be of high quality, it is clear that suitable up-to-date and well-tried "software engineering" development models should be followed. For safety-related systems, reference is generally made in this context to the "V model" [45]. Since the V model familiar from the reference is generally used for very complex software, EN ISO 13849-1, subclause 4.6.1 requires only a more simplified form of it (Figure 6.11).

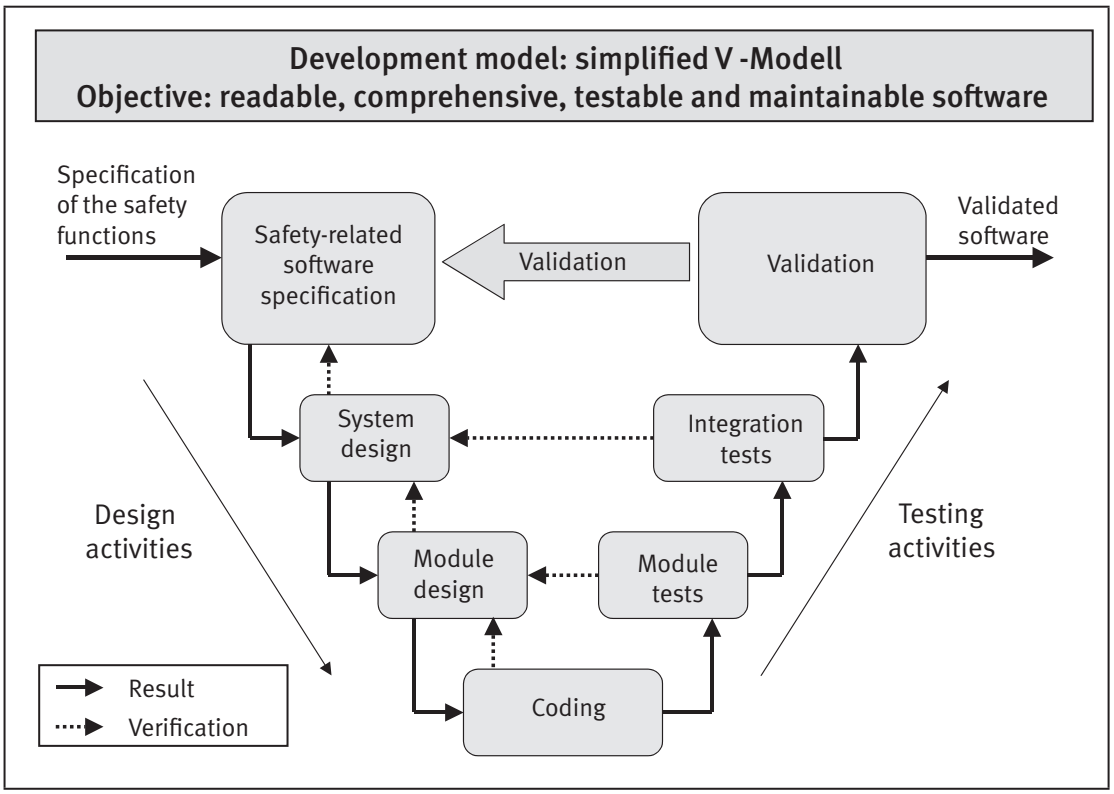


Figure 6.11: Simplified V model for the development of safety-related software

This form is considered to be appropriate for the practical conditions and the objectives for safety-related SRP/CS in the machinery sector and specifically for the development of SRASW. The actual objective here is the creation of readable, understandable, testable and maintainable software. Programmers who do not normally develop safety-related software are likely to consider these requirements tedious. However, they provide them with the certainty of having developed the software to an adequate standard.

In addition to the phases, Figure 6.11 also shows important terminology that must first be defined (in a software context).

Result

Refers to the product of a phase, for example the specification, the software design, the code, and in the case of the final result, the tested, validated software. It may however also refer for example to the result of a specification phase in the form of a test plan that is not required until a much later phase, at which it can be used for systematic validation of the software. The result(s) of the preceding phases serve as inputs for the subsequent phases. This is indicated by the arrow.

Verification

Describes the quality assurance activity by which the result of a phase is checked against the specification of the preceding phase. During or at the end of the coding phase, for example, verification is performed of whether the code actually implements the specified module design, and whether the programming guidelines have been observed in the process.

Validation

In this context, software validation is a concluding, special form of verification of the entire software. A check is performed of whether the requirements of the software specification concerning the functionality of the software have been implemented.

Selected phases of the simplified V model, and thus at the same time the "roadmap" for software development, are described below. The downward-pointing part of the "V" describes the design activities of development, the upward-pointing part the review activities.

6.3.2 Overall safety interface: software specification

This document describes, based upon the higher-level specification of the safety functions of the SRP/CS, the sub-functions of the specification that are to be implemented by the software. In addition, the following are presented:

- Functions that detect and control hardware faults
- Performance characteristics, such as the maximum response time
- Fault-mode responses
- Interfaces provided to other systems, etc.

Besides these functional requirements, the PL to be attained by the safety functions, the PL_r, must be stated, in order to permit selection of the necessary measures for fault avoidance (see further below).

This specification (or "safety-related software requirements specification") must be verified, for example by a review performed by a person not involved in its creation. The reviewer must confirm firstly that the requirements specification complies with the higher-level specification, and secondly that it satisfies the formal requirements governing how a software specification is to be written. The specification should be structured and generated in detail in such a way that it can also serve as a checklist for later validation.

The overall safety of a machine or machinery installation is assured by all safety-related parts of the control system and their functions (components of all technologies, electronics, software). A description is therefore required at this point, in the form of a specification, of the safety for the machine/machinery installation. The document need not run into the hundreds of pages; it is acceptable for it to be limited to the essential points in a comprehensible form. The specifications for the machine or machinery installation as a whole will be followed by a subset of tasks for programmers. The software specification thus forms a part of the overall concept, and can therefore be regarded as a "contract" with a "subcontract" for the programming function.

The software specification begins with provisions concerning design and coding of the software. The other elements involved in assuring safety must be able to rely upon implementation of the functions in the software. The specification is thus also the point of reference for acceptance of the software: validation of the software functions must demonstrate whether the "contractual obligations" have been met. In the area of SRASW, this must be taken literally, since the engineering and programming of a control system are often assigned by the parties responsible for safety as a whole to other companies or corporate divisions. In this case, the specification also serves as a contractually binding interface to external or internal service providers.

6.3.3 System and module design for the "safety-related technical specification"

The software architecture is generally already defined by the operating system or the development tool. The design further defines the structure and modules to be employed for implementation of the specified safety sub-functions. What existing library functions are to be employed must be determined, as must whether new functions may have to be developed specifically for the project. In this sub-clause, the term software function/module also refers in all cases to a function block.

The software design document should describe the structure and process of the software, supported by diagrams, in a way that makes these aspects comprehensible to external parties. The more the program is based upon re-used software functions that have already been validated and are already documented elsewhere, the more concise the software design document can be. The module design also specifies the new software functions that are to be produced specifically for the project, their interfaces, and test cases for their module test. For less complex SRP/CS, the system and module design can be summarized in a "safety-related software technical specification".

6.3.4 Finally: programming

Coding work proper then begins. In the interests of fault avoidance, the following three aspects must be observed:

- Code must be readable and clear, in order to facilitate testing and error-free modification at a later stage. Binding programming guidelines facilitate, among other things, better commenting of the program and the assignment of self-explanatory names to variables and modules.

- Defensive programming, i.e. the assumption that internal or external errors may always be present, and detection of them. If the characteristic of input signals over time is known, for example, this anticipatory approach can be used to detect errors in the peripheral circuitry. If a finite-state machine is being programmed, the state variable is monitored for a valid value range, etc.

- The code must be analysed statically, i.e. without execution: for low PLs, a code review is sufficient; for PLs d and e, the data and control flow should also be examined, ideally with the use of tools. Typical questions are: is the code consistent with the preceding software design? Do any points exist at which signals with a lower PL (for example from a standard PLC) override a signal with a higher PL? Where and by what modules are variables initialized, written to, and then assigned to the safety output? What software functions are executed conditionally?

6.3.5 Module test, integration test and validation

In the module test, the new software functions developed specifically for the project are tested and simulated in order to check whether they are coded as specified in the module design. At the integration test at the latest, for example during the typical commissioning of a machine's PLC, the complete software is tested for proper operation on the hardware (integration) and compliance with the system design (verification). Both are still verification measures, i.e. they involve looking "into" the software. Whether the safety-related sub-functions of the software perform as specified is determined by software validation, which has already been described. For the higher PLs d and e, an extended functional test is also required.

Individual software functions that have been certified or validated by quality assurance measures do not need to be tested again. As soon as a number of these functions are combined for a specific project, however, the resulting new form of safety sub-function must be validated. Even on certified modules, dangerous systematic failures may be caused by errors in parameterization and logic.

6.3.6 Structure of the normative requirements

Once the design process has been outlined, normative requirements are described for the software itself, for the development tools used, and for the development activities. These requirements also contribute towards fault avoidance. The effort involved should be commensurate with the required risk reduction, in the same way as for the hardware of the programmable SRP/CS. The requirements and their effectiveness are therefore increased intelligently in line with rising PL_r.

Figure 6.12 shows that a suitable package of basic measures is first set out for all PLs for both SRASW and SRESW. These basic measures can be regarded as software-specific basic safety principles. They are sufficient for the development of software for PL a or b. For software employed in SRP/CS for PL c to e, the basic measures are supplemented by additional measures for fault avoidance. The latter are required for PL c with lower effectiveness, for PL d with medium effectiveness and for PL e with higher effectiveness. Irrespective of whether the software now acts in only one or in both channels of a desired Category, the PL_r of the implemented safety function(s) is always the yardstick for the requirements.

The aspect of "higher effectiveness" refers to the rising level of fault avoidance. This may be illustrated by the important task of production of the specification. For PL c, for example, it may be sufficient for programmers to write the specification themselves and for it to be reviewed by others (internal review). Should the same software

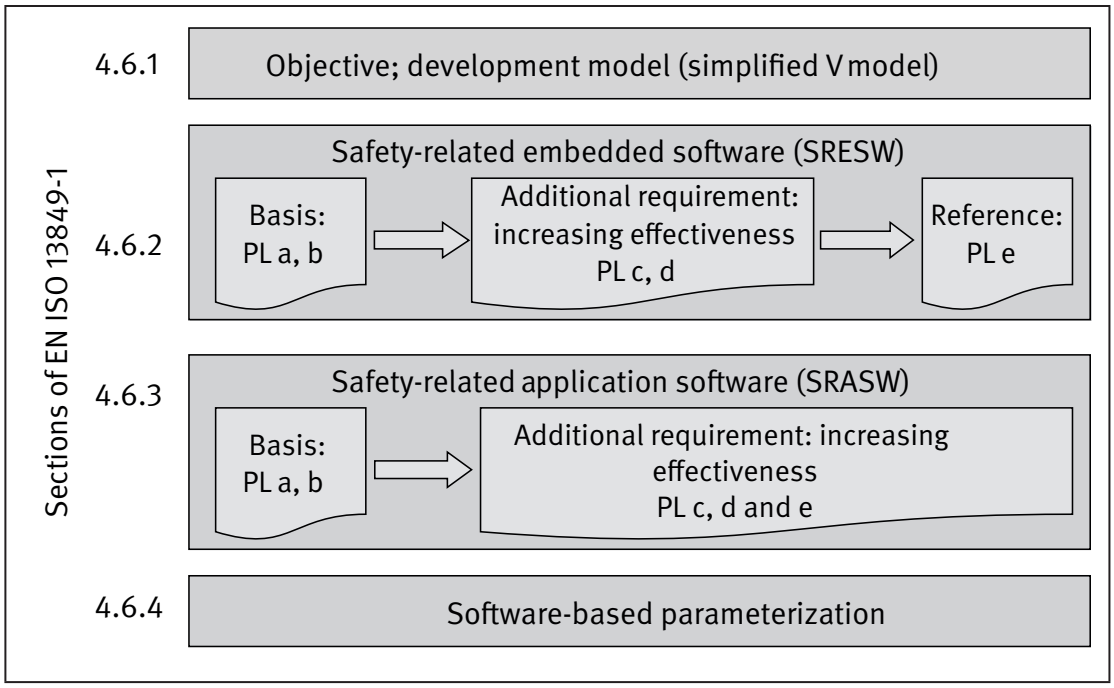


Figure 6.12: Grading of the requirements for safety-related software (EN ISO 13849-1)

be employed for PL e, however, a higher level of fault avoidance must be attained. It may then be necessary for the specification to be written by the software project manager, for example, rather than the programmers. In addition, the review of this specification could be performed jointly with a more independent person, such as the person responsible for hardware engineering. More eyes (generally) find more errors. A comprehensive discussion of the individual requirements and of their greater or lesser effectiveness is unfortunately beyond the scope of the present report. Discussion will therefore be limited to certain particular cases:

- It is not uncommon for cohesive software of SRP/CS to implement several safety functions (SFx) of differing PL_r (e.g. SF1 and SF2 with PL_r c, SF3 with PL_r e). In practice however, it is unlikely to be possible to differentiate between the safety functions of differing PL_r in the development cycle, the tools, or the effectiveness of the activities (e.g. during modifications). In this case, the requirements for fault avoidance are therefore geared towards the highest PL_r (in the example given: e).

- Redundant SRP/CS of which only one channel is programmable: although the programmable electronics constitute only a single channel, the overall structure satisfies Category 3 or 4. Safety functions with a higher PL_r, such as d or e, are frequently implemented by means of these structures. If programmable electronics are employed in one channel of the part of the control system in diverse redundancy with a technology other than programmable electronics (e.g. fluid power technology) in the other channel, the IFA's recommendation is that the normative requirements can be reduced by one PL level, e.g. for PL_r c instead of PL_r d, owing to the lower probability of a dangerous failure caused by systematic faults in this SRASW. Irrespective of this, the normative requirements for the SRESW must also be observed (subclause 6.3.10).

- Use of standard PLCs: the circuit examples in this report (see Chapter 8, Page 99 ff.) demonstrate that standard PLCs can in principle also be used to engineer safety-related control systems. Only for PL e is it likely to be very difficult to attain the required “high” level of diagnostic coverage *DC* of at least 99% for the hardware of a PLC – at least if this diagnostic coverage is to be implemented by the SRASW. For PL a to d, the software requirements for the standard PLC are described in subclause 6.3.10. The requirements for the avoidance of errors in SRASW (subclauses 4.6.1 and 4.6.3 of the standard) in accordance with the PL_r must also be met during application programming. The topic of systematic capability requires particular attention.

- A bonus during the development of diverse SRESW is that on two-channel SRP/CS for one or more safety functions with a PL_r of e, the SRESW of the two channels can be implemented diversely. Should the degree of this diversity be so great that the code, the design, and even the specification have been created differently, this software can also be developed in accordance with the requirements set out in EN ISO 13849-1 for PL d. It is then irrelevant whether the SRP/CS have two different or identical hardware channels.

6.3.7 Suitable software tools

No software without tools: this particularly holds true for safety-related software. The selection and quality of these tools are therefore decisive factors for the avoidance

of errors and thus for the quality of the safety function. EN ISO 13849-1 emphasizes four elements:

- Development tools:
  Development requires tools that are suitable and well-tried for the intended use. Certified tools for safety components are generally employed for SRASW. Features such as the avoidance and detection of semantic errors, the observance of language subsets or the monitoring of programming guidelines relieve programmers of tasks and enhance the quality of the software.

- Libraries of software functions:
  The design of the system should consider existing or supplied libraries and, where practicable, employ validated functions. The following principle applies: the more the program is based upon functions that are already validated or indeed certified, the fewer project-specific software components remain that must be validated internally or by an external organization prior to commissioning. For typical recurring functions, system integrators are well advised to invest the necessary effort in developing suitable modules themselves to EN ISO 13849-1 such that they can also be re-used and tested, including by independent persons, routinely and without error. Discrete library functions also require specification, design, test plan, validation, etc.

- Suitable programming languages:
  For SRASW, application-oriented languages are recommended, for example in accordance with IEC 61131-3 [46]. Even these languages are more comprehensive than necessary, and contain constructs that in some cases are error-prone. Programmers should therefore limit the use of the syntax. Corresponding language subsets are generally specified by the tool.

- Programming guidelines:
  Suitable programming guidelines must be observed for coding of the software functions [47]. The guidelines should be the existing, accepted rules of a recognized organization. Alternatively, a company may draw up suitable programming guidelines of its own, provided they have a sound practical or theoretical basis. Programming guidelines govern the use of critical language constructs, the scope and interface of software functions, the formatting and commenting of the code, symbolic names of functions and variables, etc.

These tools and guidelines should be specified in the design document.

6.3.8 Unloved, but important: documentation and configuration management

Before the manufacturer issues the EC declaration of conformity for a machine, he must draw up its technical documentation. Where safety-related software is concerned, this refers in the first instance to specification of the implemented safety functions (requirements specification), the design document (technical specification), and the well-commented program. In addition, the certified or self-validated library functions used must be listed together with their identification (version number, author, date, etc.). Application of the manufacturer's own programming guidelines and language subsets must also be documented. Should these already be contained in the tool, an appropriate reference to these properties is sufficient. Finally, the test activities must be documented. The integration test and validation of the safety functions are often performed at the same time. These tests must obviously be planned and must be documented together with the test results.

What is meant by configuration management? For safety-related software in particular, it is obvious and therefore a requirement that its development be transparent to all parties involved and for subsequent inspections:

- Who performed specification, programming, commissioning, verification and validation, and when?

- What was used for development, e.g. tools and their settings, re-used functions and their identification, programming guidelines?

- What program versions are loaded on which SRP/CS?

This and other necessary information, including all relevant development documents, must be recorded and suitably archived for later use, for example for the event of modification after several years in operation.

6.3.9 Software is in a constant state of change: modification

Experience has shown that even after having initially been tested, SRASW will still be the subject of fervent extension and adaptation work during commissioning of an installation or machine. This procedure is termed “modification”. These changes are often so extensive that not only the code, but even the original specification is no longer appropriate and should in fact be revised. Changes to safety functions at one end of the installation or machine may also have an impact on the safety functions at the other end that have not been modified that at this stage. Equally, the modifications may reveal gaps in the safety concept. This possibility should be examined, and the necessary phases of the V model repeated if appropriate.

Practical experience also shows however that even after it has been installed, a machine or installation may still require an additional emergency stop facility or guard door, for example. The machining process is also fre-

quently improved: once again, the safety concept must be adapted in this case. The existing software must be "modified". Note: this may be the case on SRP/CS that have already been operated for a longer period of time and for the most part without failures caused by software faults – which could equally mean that a present but "hidden" fault has simply not yet taken effect. Following a modification, however, this situation may change, for example if the software was not adequately structured and individual modules/functions are not therefore entirely without reciprocal influence.

In the situations described, "Murphy's Law" often takes effect: the program was written many years previously, but the original programmers now have more pressing tasks or have already left the company. In this case, it is in the interests of both the safety and economy of the machine or installation for the software to possess the properties stated above: legibility, structure, intelligibility, and also the facility for straightforward, non-error-prone modification – irrespective of whatever programming personnel happen to be available.

In principle, a modification means that the design process must be restarted, i.e. in the V model, at the point at which a change was made (Figure 6.11), for example:

- When the code has been changed, the module and integration test must be repeated, as must validation.
- If changes were also required to the specification, it too must be verified again, for example by review by a colleague, in order to ensure that no faults have crept in at a different point in the specification. Accordingly, all development and verification measures and also validation of the affected safety functions must be repeated.

In view of the effort described, it is understandable that the influence of a modification upon the safety functions must be studied and documented systematically. Since modifications may have a not inconsiderable effect upon proper performance of the safety function, a suitable procedure must be set out from the outset. If appropriate, this should include appointment of the persons responsible.

6.3.10 Requirements for the software of standard components in SRP/CS

Safety-related controls are often implemented by means of standard components for industrial applications. Since the standard formulates requirements for the implementation of SRESW and SRASW, these must also be satisfied with regard to electronically programmable standard components. Restrictions exist however that do not apply to tested safety components.

Requirements for SRESW

The use of externally sourced industrial standard components not developed specifically for use in safety functions and containing embedded software was not previously addressed in EN ISO 13849-1. Numerous examples of SRP/CS exist in practice however that make use of standard components such as PLCs, frequency inverters or sensors and that implement safety for example by diverse redundancy with fault detection at system level. An example employing a standard PLC and a standard frequency inverter is shown in Annex I of the standard. Since observance of the SRESW requirements is not generally confirmed by the manufacturer for such standard components and cannot be performed subsequently by the integrator, satisfaction of the SRESW requirements was not demonstrated in the past.

EN ISO 13849-1, subclause 4.6.2 now dispenses with the need for satisfaction of the SRESW requirements to be demonstrated for such standard components, provided the following conditions are met:

- The SRP/CS is limited to PL a or PL b and uses Categories B, 2 or 3.
- The SRP/CS is limited to PL c or PL d and its use of multiple components for two channels in Categories 2 or 3 is permissible. The components in these two channels employ diverse technologies. The requirement for diverse technologies in the two channels leads to the probability of a dangerous failure of the SRP/CS caused by an error in the SRESW being strongly reduced.

Besides the SRESW requirements, the standard sets out further requirements, more concerning the hardware, that must be met when standard components are used for SRP/CS. These include the avoidance and control of systematic faults, and suitability for the anticipated environmental conditions such as climate, vibration and electromagnetic compatibility (EMC). These additional requirements continue to apply irrespective of SRESW. They also include the requirement for basic safety principles to be applied from Category B upwards and well-tried safety principles from Category 1 upwards. In addition, the basic requirements of Category B must be met for all Categories, namely: the SRP/CS must be designed, constructed, selected, assembled and combined at least in compliance with the relevant standards, for example IEC 61131-2 for PLCs and IEC 61800-1/2 for frequency inverters.

Development with quality assurance in accordance with ISO 900x is not made an explicit requirement by the standard; it can however be regarded as a basic safety principle with regard to the use of standard components.

Table 6.6 shows the possible combinations of PL and Category with standard components, and whether and if so how the requirements upon SRESW are to be met.

It remains to be clarified what is meant by "technological diversity". This means that owing to the diversity between two channels (the difference in the technologies employed), the probability of a dangerous failure of the SRP/CS being caused by an error in the SRESW is strongly reduced. Systematic failures and common cause failures are relevant in this context.

Table 6.6:
Requirements for the SRESW of standard components (to EN ISO 13849-1)

Combination No.	PL	Category	Conditions	Requirements for the SRESW of the standard components
1	a, b	B, 2, 3	• Compliance with relevant product standards • Quality-assured design as a basic safety principle	No SRESW requirements are placed on industrial standard components.
2	a, b, c	1	Implementation with the use of electronic components is generally not possible, since they are not considered well-tried components in the sense of EN ISO 13849-1, Section 6.2.4	
3	c, d	2, 3	• As No. 1 • Two channels employing diverse technology; the required fault detection (*DC*) is implemented by SRASW	No SRESW requirements are placed on industrial standard components.
4	c, d	2, 3	Two channels without diverse technology; the required fault detection (*DC*) is implemented by SRASW	Full SRESW requirements in accordance with EN ISO 13849-1, Section 4.6.2 apply, including to industrial standard components. A safety analysis by the component manufacturer is required.
5	e	3, 4	Section 4.6.2 of the standard states that PL e is not possible for standard components.	

The requirement for "technological diversity" can normally be regarded as satisfied in the following examples:

- One channel (functional channel or test channel) employs components containing embedded software. The second channel employs solely components without embedded software, i.e. mechanical, electronic, electromechanical, pneumatic or hydraulic components.

- The two channels employ diverse embedded software, such as different operating systems running on identical or different hardware.
  Note: when identical hardware is used, particular attention must be paid to the systematic capability of the components for the required Performance Level.

- The two channels employ different hardware (e.g. microprocessors with different processor cores), since it is assumed that the associated embedded software was programmed in different development environments.

The requirement for "technological diversity" can normally be regarded as not being satisfied in the following examples:

- The two channels employ components of the same kind from different manufacturers, without further information on the diversity of the embedded software. In this scenario, it cannot normally be ruled out that the two manufacturers use the same embedded software components, and possibly even identical hardware (brand labelling).

- The two channels employ components of different kinds from the same manufacturer, without further information on the embedded software.

Requirements for SRASW

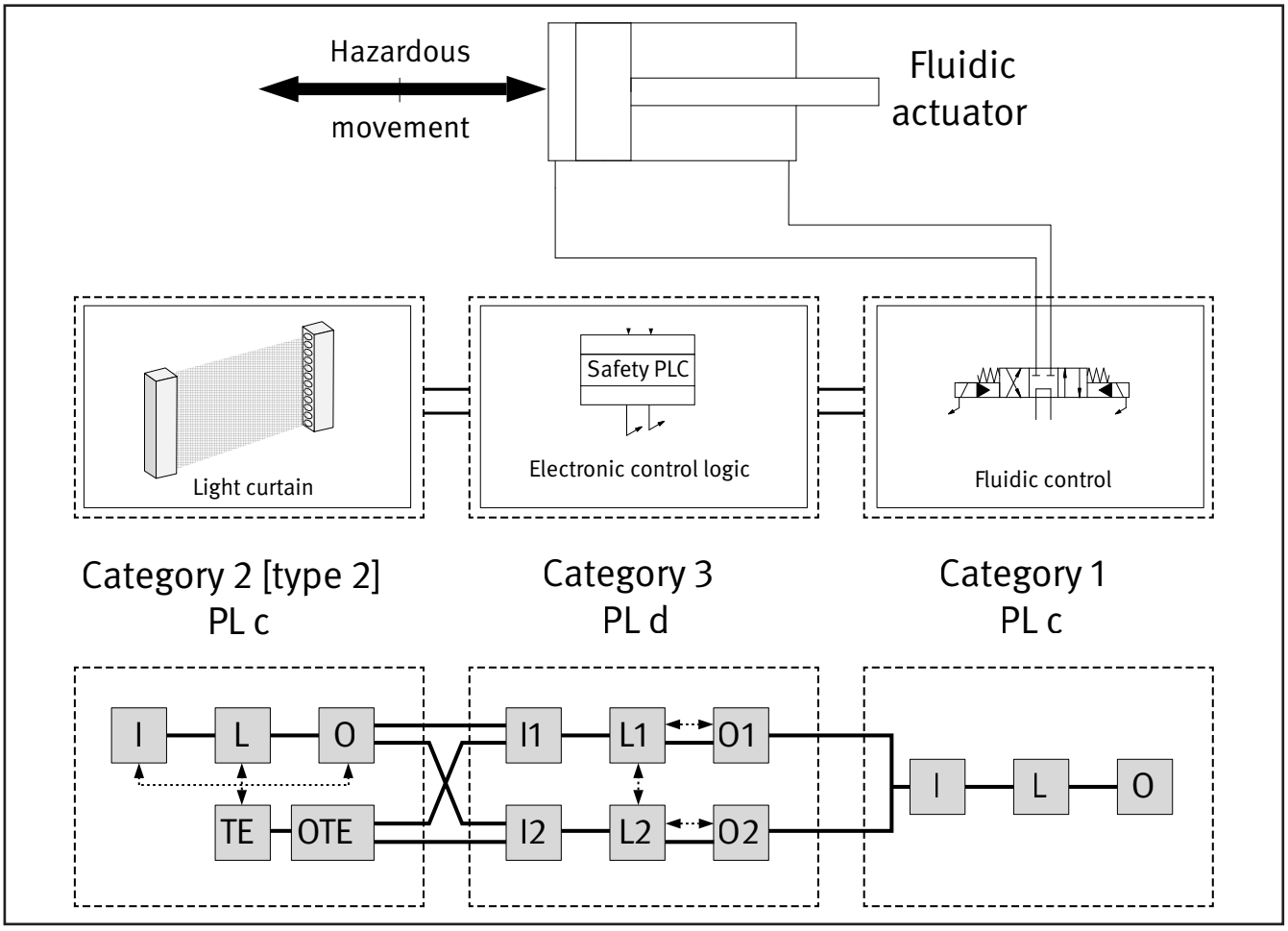
The requirements upon SRASW are geared to the PL that must be attained by the subsystem containing the programmable standard component. If for example a standard component is employed in one channel in diverse redundancy with a different technology (e.g. fluid power) in the other channel in Category 3 or 4, the IFA's recommendation is that the requirements upon SRASW can be reduced by one PL level (e.g. from PL d to PL c) owing to the lower probability of a dangerous failure caused by systematic errors in the SRASW. This can be inferred from subclause 7.4.3, "Synthesis of elements to achieve the

required systematic capability", of IEC 61508-2 [48]. In the case of Category 2, only the requirements upon the SRASW of the test channel can be lowered. Further cases are described in IFA Report 2/2016 [43], Chapter 9.

6.4 Combination of SRP/CSs as subsystems

Up to this point, this chapter has considered an SRP/CS only in the form of a complete control system that can be mapped in its entirety to a Category or designated architecture with a corresponding Performance Level. The safety function is executed entirely by such a control system, beginning with an initiating event through to attainment of the safe state. In reality however, it is often necessary for several SRP/CSs, each of which performs parts of the safety function, to be arranged in series as subsystems. Such subsystems may employ different technologies and/or implement different Categories or Performance Levels. Frequently, for example, different technologies are employed on the sensor/logic level (e.g. electronics in Category 3) to those on the drive level (e.g. hydraulics in Category 1), or bought-in devices are interlinked, e.g. light curtains, electronic controls and pneumatic valve level as shown in Figure 6.13.

Figure 6.13:
Arrangement of subsystems in series for implementation of a safety function



One of the major advantages of the PL concept over the Categories is that it provides a method by which subsystems of differing Category but similar Performance Level can be combined to form an overall system of mixed Categories but with a defined overall PL. In practice, different constellations may occur. These are discussed in greater detail below:

- The entire control system in one Category, no subsystems: for this case, the explanations given above apply, e.g. regarding the designated architectures.
- Control subsystem in one Category: for this case, the above explanations also apply, for example with regard to the designated architectures; the contribution to the safety function and the interfaces to which the further subsystems can be connected in order for the safety function to be completed must however be defined precisely (see below).
- Arrangement of subsystems (e.g. of differing Category) in series: a method is described below by which the PL and the PFH_D of the system as a whole can be calculated from the values for the subsystems (PL, average proba-

bility of a dangerous failure per hour PFH_D). Here too, the precise definition of the contribution to the safety function and of the interfaces must be observed.

- Integration of "encapsulated subsystems", e.g. in the form of externally sourced subsystems for which, of the characteristic data for quantitative determining of the PL, only the PFH_D and PL (or SIL) are known, and possibly informatively the Category (refer to subclause 6.2.9 and Figure 6.14 in this context).

- Treatment of special cases, such as the arrangement of subsystems in parallel or the use of subsystems in only one channel of an entire control system.

The arrangement in series of multiple subsystems, including subsystems differing in their technology, typically takes the form outlined by the example shown in Figure 6.13: the light curtain, electronic control system and pneumatic valve are arranged in series to enable them to perform the safety function (stopping of the hazardous movement in response to interruption of a light beam) together. The pneumatic cylinder itself is not a part of the control system and is not therefore subject to evaluation of its PL.

A chain is only ever as strong as its weakest link: this rule also applies to the interlinking of parts of control systems both of different Categories and of different Performance Levels. As has often been observed in practice, a hydraulic control system of Category 1 may, owing to the high $MTTF_D$ of its components, exhibit a safety level comparable to that of a Category 3 electronic control system with a medium DC_{avg} and low $MTTF_D$. Since positive and negative correction values for the Category are already reflected in the PL via the $MTTF_D$ and DC_{avg}, the PL for the combination is geared to the lowest PL in the series arrangement, and not to the lowest individual Category. A rising number of control elements and their respective contributions to the PFH_D also increases the overall probability of failure PFH_D of the system as a whole. Consequently, the PL of the series arrangement can be reduced by a further level from the lowest subsystem PL if for example addition of the PFH_D values causes the threshold of the PFH_D to the next PL down to be crossed.

Values for the average probability of a dangerous failure per hour PFH_D are normally available for all subsystems (values for SIL and PFH_D to IEC 61508 [10] or IEC 62061 [11] are also suitable). The PFH_D relevant to the overall PL value can then be formed by summation of these values:

$$PFH_D = \sum_{i=1}^{N} PFH_{Di} = PFH_{D1} + PFH_{D2} + \ldots + PFH_N \qquad (5)$$

where

N = number of subsystems involved in the safety function

PFH_D = average probability of a dangerous failure per hour in the system as a whole

PFH_{Di} = average probability of a dangerous failure per hour of the i^{th} subsystem

The overall PL is then limited by:

- The lowest PL of all subsystems involved in the safety function (limitation by non-quantifiable aspects such as software and systematic capability)

- The PL determined in accordance with Table 6.1 on Page 40 from the PFH_D calculated in accordance with Formula 5 (limitation by quantifiable aspects)

If – in rare cases – PFH_D values of the subsystems involved in the safety function are not known, an approximate estimate of the attained overall PL can be produced from the subsystem PL values by means of the following alternative method in EN ISO 13849-1:

- The lowest PL of all subsystems arranged in series is first determined; this is PL_{low}.

- The number of incidences of PL_{low} in the series arrangement of the subsystems is then counted; this is N_{low}.

- The overall PL can then be determined from PL_{low} and N_{low} as shown in Table 6.7.

In the method shown in Table 6.7, a probability of failure of the subsystems that lies precisely in the middle of the valid range (on a logarithmic scale) is assumed by approximation for the PL_{low} in question.

Table 6.7:
Simplified calculation of the PL for series arrangements of subsystems

PL_{low}	N_{low}	Overall PL
a	≥ 4	No PL, not permitted
	≤ 3	a
b	≥ 3	
	≤ 2	b
c	≥ 3	
	≤ 2	c
d	≥ 4	
	≤ 3	d
e	≥ 4	
	≤ 3	e

Since with both methods, all subsystem PLs are always at least as great as the overall PL, it is also ensured that all measures for non-quantifiable, qualitative aspects (e.g. systematic failures or software) are adequately considered in the combination. Particular attention must however be paid here to the interfaces between the subsystems:

- All connections (e.g. conductors or data communication over bus systems) must already be considered in the PL of one of the subsystems involved, or faults in the connections must be excluded or be negligible.
- The subsystems arranged in series must be compatible at their interfaces. In other words, each output status of an actuating subsystem that signals the demand of the safety function must be a suitable initiating event for initiating the safe state of the downstream subsystem.

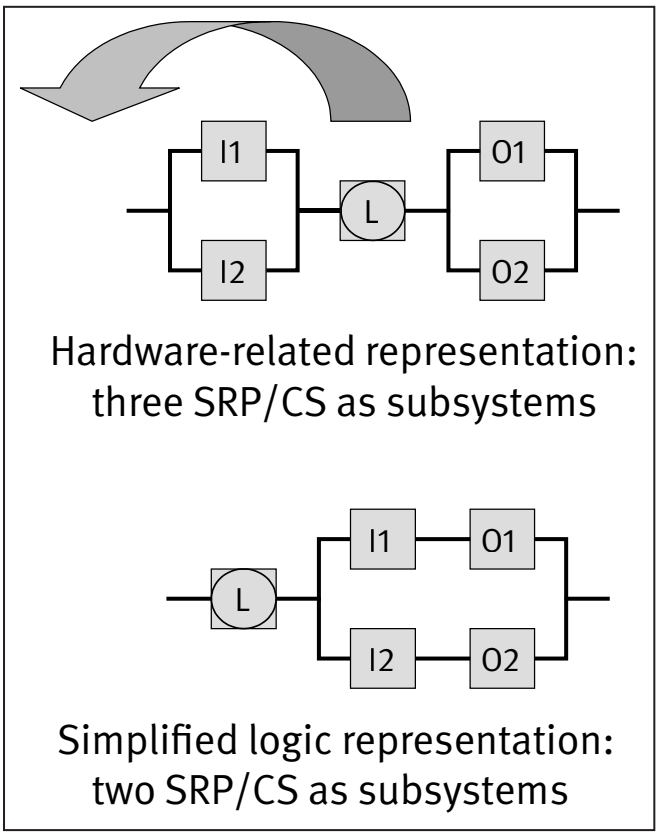
In two-channel systems connected in series, addition of the subsystem PFH_D values may lead to minor arithmetic errors on the unsafe side. Strictly speaking, the two outputs of the first subsystem should additionally be read crossed over into the inputs of the second subsystem, and compared. Crossed-over doubling of the input information, however, is often already implemented internally at the input level of the second subsystem. In order to prevent an unnecessarily high wiring overhead, the minor underestimation of the PFH_D during addition is tolerable.

The rules described up to this point already enable subsystems to be combined much more flexibly than was possible by means of the categories as described in the first edition of the standard in the form of EN 954-1. These subsystems may differ widely in nature, for example with regard to their technology or Category, and may also be developed against other standards for the safety-related parts of machine controls that are based upon an SIL rather than a PL (see Figure 3.2).

Two-channel and (tested) single-channel parts may alternate in linked subsystems. As an example, Figure 6.14 shows an encapsulated logic subsystem (e.g. a safety PLC) to which two-channel input and output elements are connected. Since the hardware level is already abstracted in the safety-related block diagram, the order of the subsystems is in principle interchangeable. It is therefore recommended that subsystems sharing the same structure be grouped together, as shown in Figure 6.14. This makes calculation of the PL simpler, and unnecessary truncation effects, such as multiple capping of the $MTTF_D$ of a channel to 100 years, are avoided.

Special cases nevertheless remain for which only rough rules, if any, can be stated at this time. One special case concerns the arrangement of subsystems in parallel. In this case, simple, generic rules cannot be formulated either for the quantifiable aspects (e.g. Category 1 twice in parallel still does not equate to Category 3, since it lacks fault detection) or with regard to the qualitative aspects (e.g. systematic failures, software, common cause failure). Usually, the only solution is therefore a re-evaluation of the entire system; in some cases it may be possible to exploit the intermediate results (e.g. the $MTTF_D$ or *DC* of blocks).

Figure 6.14:
Mixed subsystems can be re-sorted in the safety-related block diagram, for example by priority being given to encapsulated subsystems ("L" in this case).



A further special case is the integration of subsystems that already possess a PL (or SIL) or an average probability of dangerous failure per hour PFH_D as blocks in an SRP/CS. As an approximate rule without inspection of the internal structure of the subsystem, the reciprocal of the average probability of a dangerous failure per hour PFH_D may be substituted as the $MTTF_D$ for the block. Since any diagnostics measures of the subsystem that may have been implemented internally have already been considered in the probability of failure, only supplementary diagnostics measures acting externally upon the subsystem may be considered for the *DC* of the block. More detailed information can be found in clause 2 of [32]. Clause 3 of this publication also addresses the case in which more than two functional channels are connected in parallel.

A further issue that may arise in this context concerns the assignment of a Category for a complete system that is

created in turn from subsystems for which the only available information is the average probability of dangerous failure per hour PFH_D. Besides information on the internal structure, information on the $MTTF_D$ of each channel and on the DC_{avg}, for which minimum requirements apply depending upon the Category, is also lacking in this case. The same principle therefore applies as to parallel arrangements: the only alternative to a very rough estimation is re-evaluation, possibly with exploitation of intermediate results obtained.

6.5 Determining the PL with reference to the example of a paper-cutting guillotine with diverse redundancy in the logic control (Category 4 – PL e)

This subclause supplements the general description with an illustration of how the PL is determined in practice. At the same time, the example described here in detail facilitates the reader's access to Chapter 8, which contains a large number of circuit examples for diverse PLs, Categories and forms of technology.

The text boxes with grey background shown below correspond to the brief descriptions in the form used in Chapter 8. Additional explanations are also provided; reference to them for each circuit example would be too protracted in Chapter 8.

6.5.1 Safety functions

The example control system for a paper-cutting guillotine described in Figure 5.7 is taken up again here. Of the seven safety functions stated there, the implementation of SF2, for which the required Performance Level was found to be PL_r e, is described by way of example. Since the various safety functions may make use of the same components, all safety functions must be considered during implementation. For example, for safeguarding on the operator side, the product standard governing paper-cutting guillotines, EN 1010-3, requires electro-sensitive protective equipment (ESPE, not shown here) for the safety function SF3, in addition to a two-hand control (THC).

Safety function (SF2):

- Controlled location of the operator's hands outside the danger zone during a hazardous movement

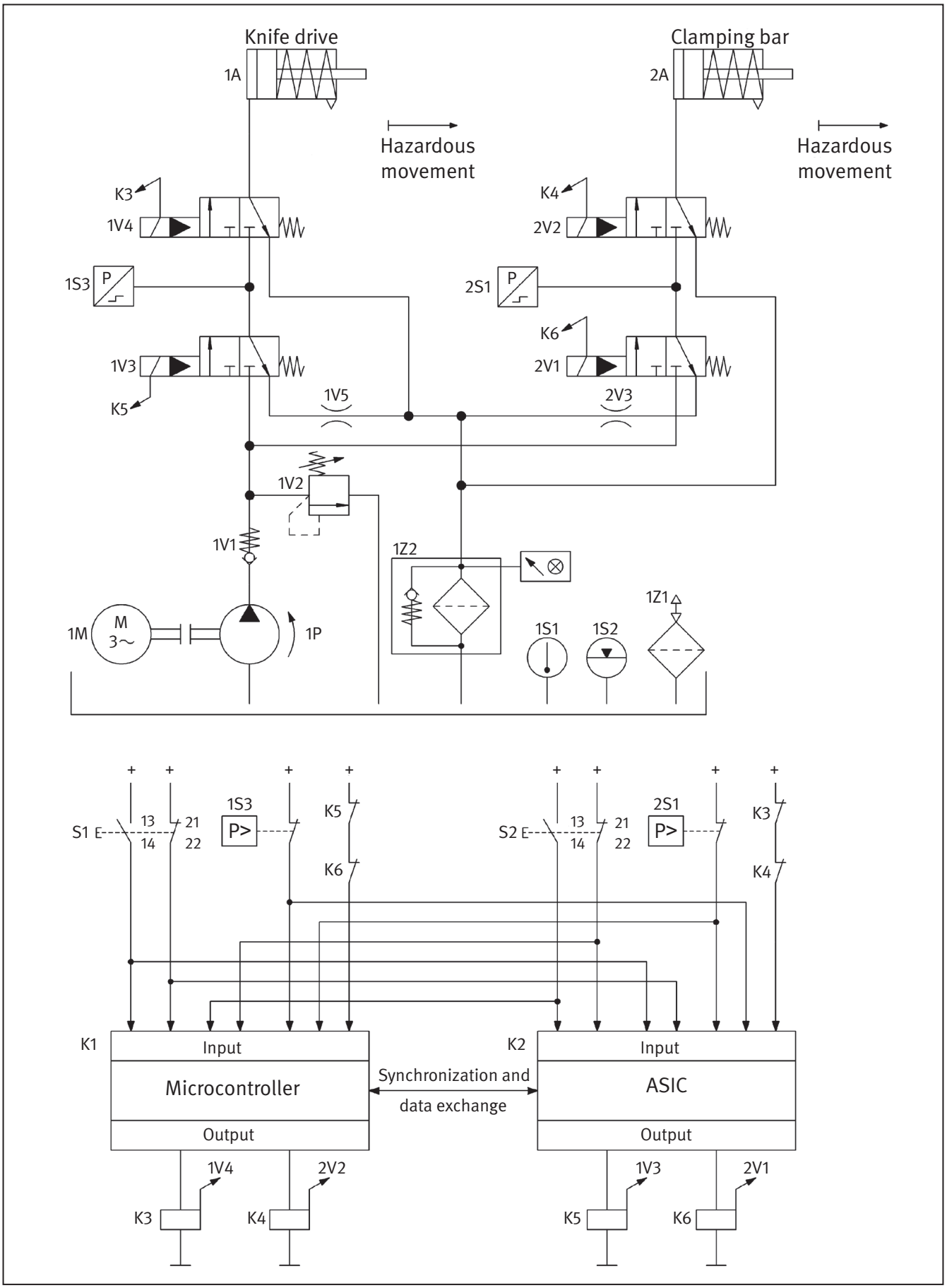
6.5.2 Implementation

Where implementation takes the form of a two-hand control, this safety function can be described as follows: when at least one of the two actuators S1 and S2 is released, the hazardous movement of the clamping bar and knife is interrupted, and both the clamping bar and the knife are returned to their initial positions by spring force. A restart is prevented until both actuators have been released and a new cycle initiated by the two-hand control. Controlled location of the operator's hands is achieved by means of two actuators that must be operated simultaneously for the machine to be started (for details, e.g. concerning immunity to defeating, see EN 574). The timing and logic of the electrical signals must be interpreted; a programmable electronic control system is a suitable solution for this purpose, and will generally also control the movement of the clamping bar and knife. Owing to the high forces required, these parts are driven hydraulically. As described in Chapter 5 (see subclause 5.3.2), the safety function encompasses both actuators – clamping bar and knife – since they are located in the same hazard zone. Figure 6.15 represents an electrohydraulic conceptual schematic diagram showing how the safety-related parts of control systems are implemented in practice. As in Chapter 8, many details have of course been omitted from the schematic diagram shown here in the interests of greater clarity. Besides the majority of functional parts of the control system required for operation of the machine within the process, certain safety-related details such as protective circuits (fuses, EMC) and “peripherals” (power supply, clock signals etc. for the logic) have also been omitted from the diagram. Owing to the required single-fault tolerance and tolerance of an accumulation of undetected faults, decoupling elements for example are also required in practice between the interconnected inputs of the two logic channels, in order for a defective input on one channel not to cause interference on the other channel. It must therefore be appreciated that a conceptual schematic diagram such as this does not constitute documentation from which a replica could be fabricated; rather, its purpose is to illustrate the structure of the safety technology.

6.5.3 Functional description

A functional description explaining the circuit structure and signal paths is essential for an understanding of the circuit diagram. It is intended to permit identification of the functional process during performance of the safety function (which may take place in different channels) and the implemented test measures.

Figure 6.15:
Conceptual schematic diagram of the electronic drive of a hydraulic knife drive and a hydraulic clamping bar (essential components)



Functional description:

- Operation of the actuators S1 and S2 of the two-hand control initiates the hazardous movements (processing cycle) of the clamping bar and the knife. Should either of the actuators of the two-hand control be released during this cycle or a signal change occur in the peripheral system of the machine that is not expected by the control system, the cycle is halted and the machine assumes the safe state.
- Pressing the actuators S1 and S2 causes the rising edges of the signals to be fed to the two processing channels K1 (microcontroller) and K2 (ASIC). Provided these signals satisfy the requirements for simultaneity (500 ms) in accordance with the relevant standard, EN 574, the two processing channels set the outputs (contactor relays K3 to K6) for a valid cut request.
- The two processing channels act synchronously and also mutually evaluate internal intermediate states of the cyclical signal processing operations. Deviations from defined intermediate states cause the machine to be halted. One processing channel is formed by a microcontroller (K1), the other by an ASIC (K2). K1 and K2 perform background self-tests during operation.
- Faults in the actuators S1/S2 and in contactor relays K3 to K6 (with mechanically linked readback contacts) are detected by cross monitoring in the processing channels.
- Failure of the valves 1V3/1V4 and 2V1/2V2 is detected by means of the pressure switches 1S3 and 2S1.
- Failure of the valves or sticking open of 1V4 or 2V2 is detected by a strong reduction in the return speed of the hydraulic cylinders. This situation can also be detected by the control system by suitable interpretation of the pressure signals (duration of pressure drop).
- Failure of the valves or sticking open of 1V3 or 2V1 is detected directly by monitoring of the signal change of pressure switches 1S3 and 2S1: should a valve stick, a pressure is signalled even though no pressure should be present.
- All machine states are monitored by both processing channels. The cyclical nature of the cut operation causes all system states to be cycled through, and faults can thus be detected.

6.5.4 Safety-related block diagram

The description of the circuit arrangement in conjunction with the circuit diagram and where applicable other descriptive documents (comprehensive specification) enables a control Category to be determined and the actual circuit to be mapped to an abstracted safety-related block diagram (Figure 6.16, see Page 78). It quickly becomes clear from this example that the safety function is executed in two-channel mode. Category 3 or 4 may therefore be considered. The high-quality test measures, by which combinations of faults can also be controlled, suggest Category 4. This is demonstrated explicitly by the verification step in Chapter 7, as is checking of the quantitative requirements for the $MTTF_D$, DC_{avg} and CCF (see below). The explanations provided in subclauses 6.2.8 and 6.2.9 are helpful for implementation in the safety-related block diagram. A proven procedure is to track the signal path, beginning at the actuator end, by asking: "How is the hazardous movement driven/prevented?", in order then to follow the logic through to the sensors. SISTEMA Cookbook 1 [34] describes this step "From the schematic circuit diagram to the Performance Level" in more detail. Note in this example that actuators S1 and S2 are not mutually redundant, even though they may initially appear so, since each button independently protects one of the user's hands. Rather, the redundancy begins within each button with the use of electrical break contact/make contact combinations. Each control channel monitors both hands/actuators by interpreting at least one electrical switching contact in each actuator. The safety-related block diagram therefore contains a make contact, e.g. S1/13-14, and a break contact, e.g. S2/21-22, in each channel. The safety-related block diagram differs substantially in this respect from the functional circuit diagram.

Under certain circumstances, the actual implementation of the safety function may result in restrictions or recommendations for the application. For example, the effectiveness of fault detection by way of the work process is by definition closely related to the application.

Remarks

- Application for example on paper-cutting guillotines (EN 1010-3)

6.5.5 Input variables for quantitative evaluation of the attained PL

All basic information for evaluation of the attained PL is available at this point. With knowledge of the Category and of the safety-related block diagram, the $MTTF_D$ and

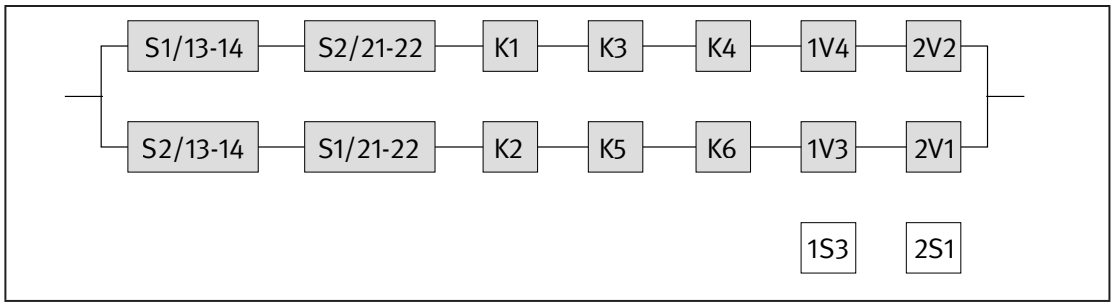


Figure 6.16: Safety-related block diagram of the SRP/CS for the selected safety function SF2 on the paper-cutting guillotine

DC can first be determined for the individual blocks, and the measures against CCF also evaluated for existing redundancies. This is followed by the "mathematical" steps for determining the $MTTF_D$ of each channel, the DC_{avg}, and finally the PL.

Calculation of the probability of failure

- $MTTF_D$: at 240 working days per year, 8 working hours per day and a cycle time of 80 seconds, n_{op} is 86,400 cycles per year. For S1 and S2 and for K3 to K6, a B_{10D} value of 2,000,000 cycles [M] produces an $MTTF_D$ of 232 years. For the microcontroller alone, an $MTTF_D$ of 1,142 years is determined [D]. The same value is also substituted for the ASIC [D]. Together with the associated circuit arrangement, this results in an $MTTF_D$ of 806 years in each case for the blocks K1 and K2. The manufacturer states an $MTTF_D$ of 150 years [M] in each case for the hydraulic valves 1V3, 1V4, 2V1 and 2V2. These values result in an $MTTF_D$ for each channel of 31.4 years ("high").

- DC_{avg}: in accordance with EN ISO 13849-1, Annex E, the *DC* values produced for S1/S2 are: 99% (cross monitoring of input signals without dynamic test with frequent signal change); for K1/K2: 90% (self-test by software and cross monitoring); for K3 to K6: 99% (direct monitoring by mechanically linked contacts); for 1V3/2V1: 99% (indirect monitoring by the pressure sensor); and for 1V4/2V2: 99% (indirect monitoring by the function and measurement of a change in the duration of the pressure drop). These values yield a DC_{avg} of 98.6% ("high").

- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)

- The combination of control elements satisfies Category 4 with a high $MTTF_D$ per channel (31.4 years) and a DC_{avg} of 98.6%, within the "high" tolerance band. This results in an average probability of dangerous failure of $9.7 \cdot 10^{-8}$ per hour. This satisfies PL e.

In order to elucidate calculation of the $MTTF_D$, block "K1" will first be considered: although the conceptual schematic diagram (Figure 6.15) shows only the microcontroller, this block includes further elements that are necessary for the practical functionality (e.g. crystal oscillator). All elements the dangerous failure of which could prevent performance of the safety function in the affected channel must be considered. This generally encompasses all elements in the signal path critical to safety, e.g. for decoupling, readback, EMC protection or protection against overvoltage. These elements are generally necessary for the implementation of basic and well-tried safety principles or for attainment of the *DC*. Figure B.2 (see Page 253 shows this approach with reference to a further simple example. The parts count method shown in Table 6.8 is suitable for use as a simple tabular method for determining the block $MTTF_D$ based upon the element $MTTF_D$. (For comparison, Figure B.3 on Page 255 shows the procedure for a failure mode and effects analysis.)

The failure rates for the elements stated in the second column were determined by means of the SN 29500 database [49], as denoted by the code [D] under "calculation of the probability of failure" (see subclause 7.6). Validation is described in greater detail in the continuation of this example in subclause 7.6. Since identical elements may occur more than once (third column), the total failure rate for each element type is calculated and indicated in the fourth column. The global approximation that only half of the failures are dangerous yields the halved value in Column 5. Finally, simple summation produces the total rate of dangerous failures for block K1. Column 6 shows the associated $MTTF_D$ values in years, derived as the reciprocals of the dangerous failure rates (from Column 5, following conversion from hours to years). This value is rounded to 806 years for block K1. Since the database employed states identical failure rates for the microcontroller and the ASIC and the circuitry is similar, the $MTTF_D$ value of 806 years also applies to block K2.

Table 6.8:
Parts count method for the "microcontroller" block K1, based upon failure rates λ taken from the SN 29500 collection of data [48] (stated in FIT, i.e. 10^{-9} per hour)

Component	Failure rate λ in FIT to SN 29500	Number	Total failure rate λ_D in FIT	Total rate of dangerous failures λ_D in FIT	$MTTF_D$ in years as a reciprocal of λ_D
Resistor, metal film	0.2	7	1.4	0.7	163,079
Capacitor, no power	1	4	4	2	57,078
Diode, general purpose	1	3	3	1.5	76,104
Optocoupler with bipolar output	15	2	30	15	7,610
Microcontroller	200	1	200	100	1,142
Crystal oscillator	15	1	15	7.5	15,221
Transistor, low-power bipolar	20	1	20	10	11,416
Plastic-sealed relay	10	1	10	5	22,831
Total for the "microcontroller" block K1				141.7 FIT	806 years

Manufacturers' data ("[M]") are used for blocks S1/S2 and K3 to K6. Since the reliability data are available only for S1/S2 overall (operating mechanism and break and make contact), these values can be used as an estimation erring on the safe side for each of the channels, even though only either the make contacts (e.g. S1/13-14) or the break contacts (e.g. S2/21-22) are considered in each channel, in addition to the operating mechanism. The assumed B_{10D} values are converted to $MTTF_D$ values by means of the formulae familiar from Annex D:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{cycle}} \cdot 3{,}600\,\frac{s}{h} = \frac{240\ \text{days/year} \cdot 8\ \text{h/day}}{80\ \text{s/cycle}} \cdot 3{,}600\,\frac{s}{h} = 86{,}400\,\frac{\text{cycles}}{\text{year}} \tag{6}$$

$$MTTF_D = \frac{B_{10D}}{0.1 \cdot n_{op}} = \frac{2{,}000{,}000\ \text{cycles}}{0.1 \cdot 86{,}400\ \text{cycles/year}} = 231.5\ \text{years} \tag{7}$$

The operation time of electromechanical components is limited to the T_{10D} value (time after which 10% of the components under analysis have failed dangerously). Since in this case, however, the T_{10D} value is greater than the assumed mission time of 20 years, it is not relevant for further analysis.

$$T_{10D} = \frac{B_{10D}}{n_{op}} = \frac{2{,}000{,}000\ \text{cycles}}{86{,}400\ \text{cycles/year}} = 23.2\ \text{years} \tag{8}$$

The manufacturer also states an $MTTF_D$ of 150 years [M] in each case for the hydraulic valves 1V3, 1V4, 2V1 and 2V2.

In accordance with subclause 6.2.13, the total for one channel (S1, S2, K1, K3, K4, 1V4, 2V2) yields an $MTTF_D$ of 31.4 years, i.e. "high":

$$\frac{1}{MTTF_D} = \frac{1}{232\ \text{years}} + \frac{1}{232\ \text{years}} + \frac{1}{806\ \text{years}} + \frac{1}{232\ \text{years}} + \frac{1}{232\ \text{years}} + \frac{1}{150\ \text{years}} + \frac{1}{150\ \text{years}} = \frac{1}{31.4\ \text{years}} \tag{9}$$

Since the second channel exhibits the same $MTTF_D$, symmetrization is not required as would otherwise be the case.

Validation of the assumed *DC* values is also described in greater detail in Chapter 7. High-quality self-tests for example are performed for K1 and K2 by software and cross monitoring, including the special measures for variant and invariant memory and the processing unit that are

required for microprocessor systems. Altogether, a DC_{avg} of 98.6% is produced for the SRP/CS according to subclause 6.2.14. With exploitation of the 5% tolerance, this value is in the "high" range.

$$DC_{avg} = \frac{2 \cdot \left(\frac{99\%}{232\ \text{years}} + \frac{99\%}{232\ \text{years}} + \frac{90\%}{806\ \text{years}} + \frac{99\%}{232\ \text{years}} + \frac{99\%}{232\ \text{years}} + \frac{99\%}{150\ \text{years}} + \frac{99\%}{150\ \text{years}} \right)}{2 \cdot \left(\frac{1}{232\ \text{years}} + \frac{1}{232\ \text{years}} + \frac{1}{806\ \text{years}} + \frac{1}{232\ \text{years}} + \frac{1}{232\ \text{years}} + \frac{1}{150\ \text{years}} + \frac{1}{150\ \text{years}} \right)} = 98{,}6\% \quad (10)$$

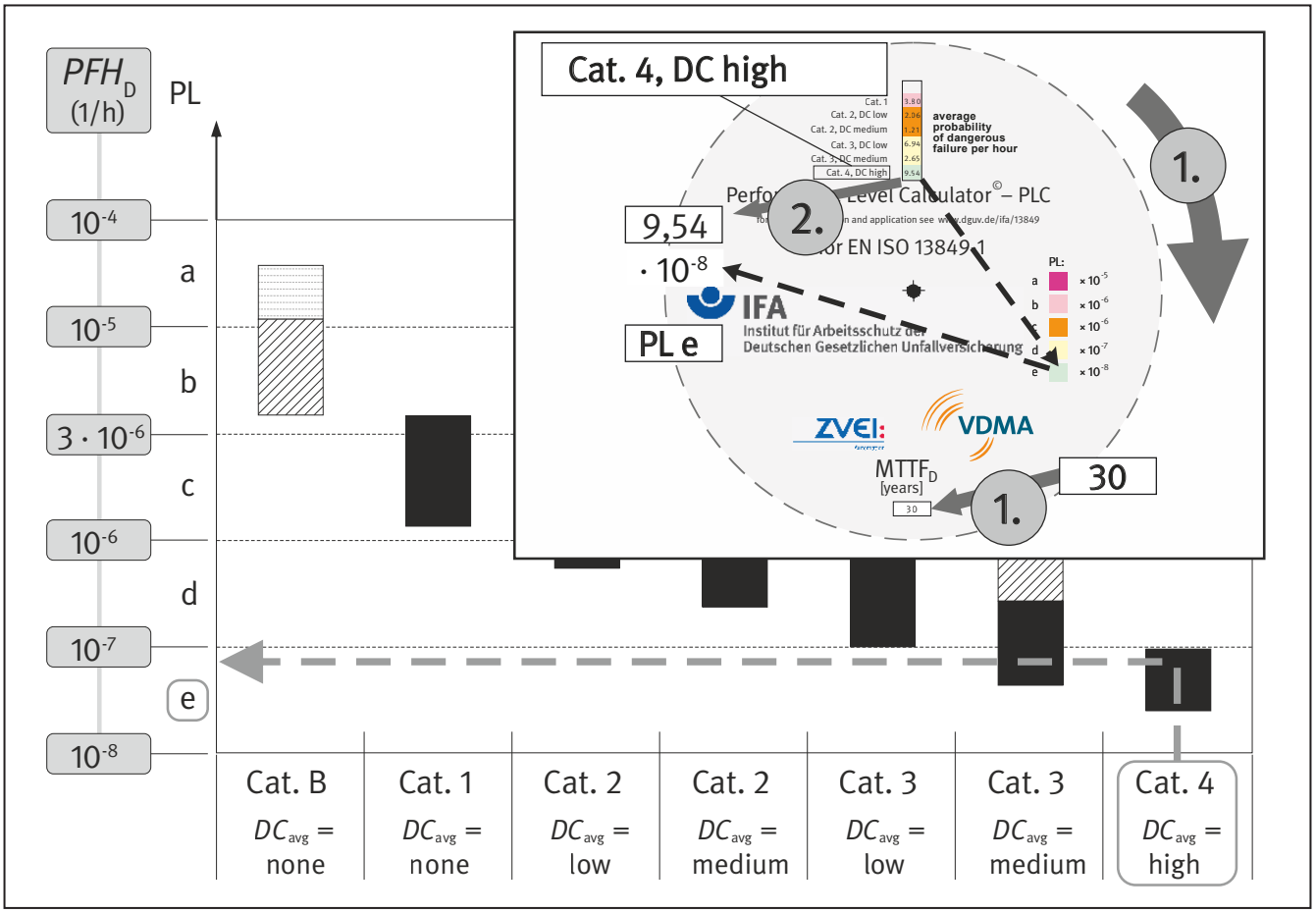
The measures against common cause failure (CCF) stated in the grey box on Page 78 are largely self-explanatory. Validation is nonetheless explained in greater detail in Chapter 7. In addition, the "diversity" measure and the "use of well-tried components" measure take effect in the electrical and hydraulic subsystems respectively (see Annex F). With satisfaction of the requirements for CCF, a DC_{avg} of "high" and an $MTTF_D$ of "high", the quantitative requirements for Category 4 are also met.

6.5.6 Several approaches for quantitative calculation of the PL

Determining of the PL on the basis of quantifiable aspects is now almost complete at this stage. The results for the Category, DC_{avg} and $MTTF_D$ can be used for graphical confirmation by means of the bar chart that PL e is attained (see Figure 6.17). The tabular values in Annex K of the standard or the IFA's PLC disc calculator [16] based upon them yield the following result:

Category	CCF	DC_{avg}	$MTTF_D$	PFH_D
4	OK	"High"	"High" (rounded down: 30 years)	$9.5 \cdot 10^{-8}$ per hour (PL e)

Figure 6.17:
Determining of the PL by means of the bar chart/disc calculator



The SISTEMA software (see Annex H), available free of charge from the IFA, is much more convenient for the administration, documentation and calculation of all intermediate results. All quantitative requirements for determining the PL that have been described thus far can be handled easily with this software, and all calculations including mathematical determining of the PL are automated. Use of the exact DC_{avg} and $MTTF_D$ values for calculation is possible as a special option. For DC_{avg}, the exact (in this case poorer) value of 98.6% is employed for calculation rather than exploitation of the 5% tolerance for a DC_{avg} of "high" and substitution of a rounded 99% (for the tolerances for *DC* and $MTTF_D$, cf. Note 2 in Tables 4 and 5 of the standard). Dropping below the 99% mark for Category 4, still within the tolerance band, initiates a warning message by SISTEMA, however. Use of the precise $MTTF_D$ value of 31.4 years for calculation yields a result comparable to that from calculation with the rounded value of 30 years for $MTTF_D$ "high". The result is an average probability of a dangerous failure per hour of $9.7 \cdot 10^{-8}$ per hour (see Figure 6.18).

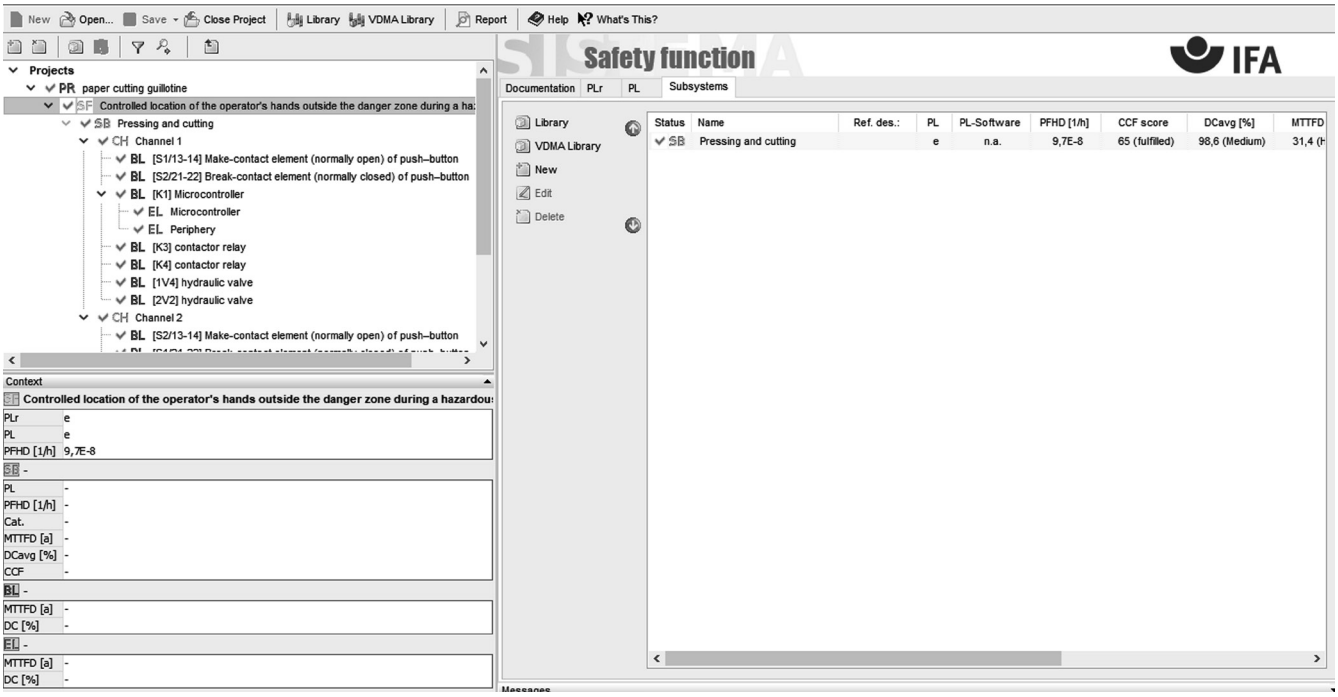
This is now followed by evaluation of the non-quantifiable qualitative aspects for determining the PL, firstly for systematic failures.

6.5.7 Systematic failures

With its diversity-oriented approach for the logic control, the selected design of the control system employs a highly effective measure against the influence of systematic failures. Further measures are of course required in the course of implementation, for example in order to control the effects of a voltage breakdown, fluctuations in voltage, overvoltage and undervoltage. Some of the necessary measures are already evident in the selected design. These include:

- Use of the closed-circuit current principle: this ensures that the de-energized state cannot give rise to an actuation signal (e.g. in the event of wire breakage).
- Fault detection by automatic tests: in this case, tests – differing between the two channels – are performed that are capable of detecting faults at an early stage and of initiating the safe state independently of the respective adjacent channel.
- Testing by redundant hardware: the diversity by design provides additional control of faults caused by environmental influences that differ in their effects upon the different channels.
- Use of contactor relays with mechanically linked contacts: status detection of suitable contacts enables dangerous faults of the contactor relays and in some cases of other circuit components to be detected.
- Program sequence monitoring: the ASIC for example is used to monitor the program sequence of the microcontroller channel.

Figure 6.18:
Determining of the PL by means of SISTEMA



The reader's attention is drawn in particular to two details concerning systematic failures, the first relating to the application, the second to the design process:

- During design of the hydraulic system for paper-cutting guillotines, consideration must be given to the incidence of paper dust. Contamination of hydraulic fluid with paper dust may for example jeopardize the safe function of a paper-cutting guillotine. For this reason, particular attention must be paid to effective filtration of the pressure medium. In addition, the ingress of paper dust into the hydraulic system from outside must be prevented, for example by tank vent filters and wiper rings on cylinder rods.

- Fault-avoidance measures during development of the ASIC in accordance with the ASIC development life cycle of IEC 61508-2. This standard makes provision for a V model for the development of an ASIC, following the V model familiar from software development.

6.5.8 Ergonomic aspects

In this example, a safety-related interface exists between the user and the control system: the two-hand control (THC) device, with actuators S1 and S2. Certain ergonomic aspects must be considered here in order to prevent any person from being endangered, either directly or over time as a result of impairing strain, during the intended use and reasonably foreseeable misuse of the machine. For the majority of machines, these user interfaces can be checked by means of the ergonomic machine design checklist, DGUV Informative publications 209-068 and 209-069 [30]. Aspects to be observed in this context include the following:

- Height and orientation of the actuators in relation to the operator

- Legroom and area of reach during operation, normally in a standing position

- Arrangement matched to the operating task and good accessibility outside the danger zone

- Ease of observation of the cutting process from the location of the THC

- Minimum dimensions and shape of the actuators (ergonomic design in consideration of the requirements of EN 574)

- Easy operation with low forces, but with design measures for the prevention of unintended operation

- Robust design of the buttons, and suitable marking and colouring

- THC designed to prevent defeating and thus circumvention of the controlled location of the operator's hands

6.5.9 Requirements concerning the software, specifically SRESW

The following description is of a model implementation of safety-related firmware for the microcontroller K1. The software is embedded software (SRESW) for which the PL_r is e. Owing to the diversity-oriented approach of the logic control – the second channel takes the form of an ASIC – the requirements in accordance with the note in subclause 4.6.2 of the standard can be scaled down: "*When using diversity in specification, design and coding, for the two channels used in SRP/CS with Category 3 or 4, PL_r e can be achieved with the above-mentioned measures for PL_r of c or d.*"

The design process for the firmware is based upon the V model in Figure 6.11, and is embedded in the manufacturer's certified quality management system. Based upon the specification for the safety-related control system as a whole, the specification for the software safety requirements for the firmware (safety related software requirements specification) is first written. This document describes the contribution made by the firmware to the safety functions of the machine, the required response times with regard to K1, responses to detected faults, interfaces to other subsystems, dependencies upon operating modes, etc. In addition, all fault-avoidance measures required under subclause 6.3.2 of the standard for PL c or d are defined. The specification is then reviewed, for example by the safety project manager, and amendments made if appropriate. Once the specification has been approved, system design can commence.

Software architecture: an operating system is not installed on the microcontroller; instead, a number of tasks are defined which, controlled by simple task management, are executed by timer interrupt at defined intervals. Some low-priority tasks are reserved for the standard functions of the paper-cutting guillotine, whilst the high-priority tasks are executed by the safety-related functions specified above. The determinacy of these task calls is necessary for the required high synchronicity of the two channels and the short response times. The cyclical self-tests for the control of random hardware failures are executed during task idle times.

The design of the software architecture and of the software modules and functions required for implementation of the software described above are summarized in a further document, the technical specification for the system and module design. For fault avoidance over the entire life cycle, suitable modularization and in this case also clear separation of the SRESW from the non-safety-related software are particularly important. Where neces-

sary for the sake of clarity, the structure and flow of the software are shown by diagrams. Further requirements are laid down concerning the programming language to be used, in this case ANSI C with compiler-specific language extensions, and the development tools, e.g. compiler, version management, configuration management; all have been used successfully for many years. The programming guidelines and methods for tools-based static analysis for verification of coding are also specified. Planning of module and integration testing is also set out in this document. Following a further review, for example by the software development manager, the technical specification is approved as a specification for coding. This review also verifies whether the requirements of the software specification are met.

Coding proper now begins, in compliance with the programming guidelines. Besides rules for better code legibility, the provisions of the programming guidelines specify such things as constraints upon the use of critical language constructs. Observance of the programming guidelines during coding is assured in-process by the use of suitable tools. For semantic verification (of the content) of the finished code against the technical specification, the programmer conducts a walk-through with colleagues in which execution of the program and the data flow of critical signals are analysed at the same time.

The usual module tests are performed to check the functions and interfaces, firstly for correctness and secondly for compliance with the module design. This is followed by integration of the software and tests together with the hardware of the microcontroller K1. K1 is then connected to the ASIC channel K2 in order to test synchronization, data exchange and fault detection of the two channels in combination. All tests are documented.

This integration test may reveal that the microcontroller's performance is not as good as previously assumed. Should this be the case, the software architecture, specifically scheduling of the tasks and the assignment of functions to them, must be modified. This would not result in changes to the specification of the software safety requirements; the system and module design, however, would have to be adapted and subjected once again to review in order to assure compliance with the specification. This is one example of how technical changes which become necessary during development may result in the V model being repeated in order for the modifications to be implemented in accordance with the QA requirements. The code for such modifications would be written and both the module and integration tests would have to be repeated.

For the event of the firmware having to be modified after the first production batch has already been shipped, suitable measures such as an impact analysis of the modifications and appropriate development activities in accordance with the V model should be defined within the organization of development itself.

6.5.10 SRP/CS in combination

Since the entire SRP/CS are structured end-to-end in a single Category and no subsystems are combined, corresponding analysis in accordance with subclause 6.4 is not required. It is obvious nevertheless that the various components and technologies must be compatible at their interfaces. Validation aspects regarding integration are addressed in Chapter 7.

6.5.11 Further details

Even in this detailed circuit example, numerous safety-related design aspects can only be touched upon. A reference is therefore provided here, as in the majority of the circuit examples that follow, of useful reference containing further explanations and referring to additional requirements.

More detailed references

- EN 1010-3: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 3: Cutting machines (2002) +A1 (2009)
- IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (2010)
- EN 574: Safety of machinery – Two-hand control devices – Functional aspects; principles for design (1996) +A1 (2008) (to be replaced by EN ISO 13851:2019)

Further details, in particular concerning verification and validation, follow in Chapter 7 in the continuation of this example of a paper-cutting guillotine.

7 Verification and validation

Changes with respect to the second edition (BGIA Report 2/2008e):

- The entire subclause has been comprehensively edited.
- Further details on the typical content of the verification and validation plan has been added to subclause 7.1.2. subclause 7.1.3 now contains further information (references) on fault lists. The usual forms taken by the documentation required for V&V activities have also been added in subclause 7.1.4.
- The information on verification of the specification and technical documentation have now been merged in a dedicated subclause in subclause 7.2.
- Listing of required content has now been deleted for, subclause 7.5 concerning the information for use. Instead, references are provided to standards governing the content and presentation of information for use.
- Reference is made in subclause 7.6 to the commissioning test.
- The aspect of verification of the user interface is addressed by the new subclause 7.7, which follows the treatment of the subject in EN ISO 13849-2, 4.1. c).
- The example of verification and validation of the paper-cutting guillotine in subclause 7.8 has been updated.

The report does not discuss the "Example of validation of fault behaviour and diagnostic means" addressed informatively in the new Annex E of EN ISO 13849-2 [6].

Despite the dated reference in EN ISO 13849-2 [6] to ISO 13849-1:2006, this subclause of the report is also based upon the more recent edition of EN ISO 13849-1:2015.

Verification and validation refer to quality assurance measures for the avoidance of faults during the design and implementation of safety-related parts of control systems (SRP/CS) that perform safety functions. Part 2 of EN ISO 13849 [6] in particular deals comprehensively with this subject.

Verification encompasses analyses and tests of SRP/CS and their sub-aspects that have the purpose of determining whether the results attained by a phase of design or development satisfy the requirements for the phase concerned, i.e. whether for example the circuit layout corresponds to the circuit design, or whether the requirements relevant to the intended applications are compiled comprehensively (in full) in the specification.

Validation refers to demonstration of whether suitability is assured with regard to the imposed requirements. In other words, examination is performed during or at the end of the development/design process of whether the specified functional and design requirements upon the safety-related part of the machine control have in general been attained, or in the context of EN ISO 13849, whether the SRP/CS satisfies the relevant requirements of this standard for each safety function.

The process of assessment of a safety function in its implementation by SRP/CS is therefore a combination of verification and validation steps that deal with both the SRP/CS as a whole, and specific aspects of them. The terms verification and validation are also described below as V&V activities.

Note: this chapter (Chapter 7) addresses the verification and validation process for SRP/CS in the sense of a process for demonstrating compliance with the standard EN ISO 13849. Details of the methods of stated V&V activities cannot be "taught" here, nor can all sub-tests required for conformity of the product with the Machinery Directive be discussed, such as those concerning protection against electric shock, the technical (electrical, hydraulic, pneumatic) equipment, or ergonomics.

7.1 Verification and validation procedure

Figure 7.1 (see Page 86) shows the relevant details of the iterative process for SRP/CS design set out in EN ISO 13849-1 [5], Figure 3, which deals with the activities of verification and validation.

Figure 7.1:
V&V activities of EN ISO 13849-1

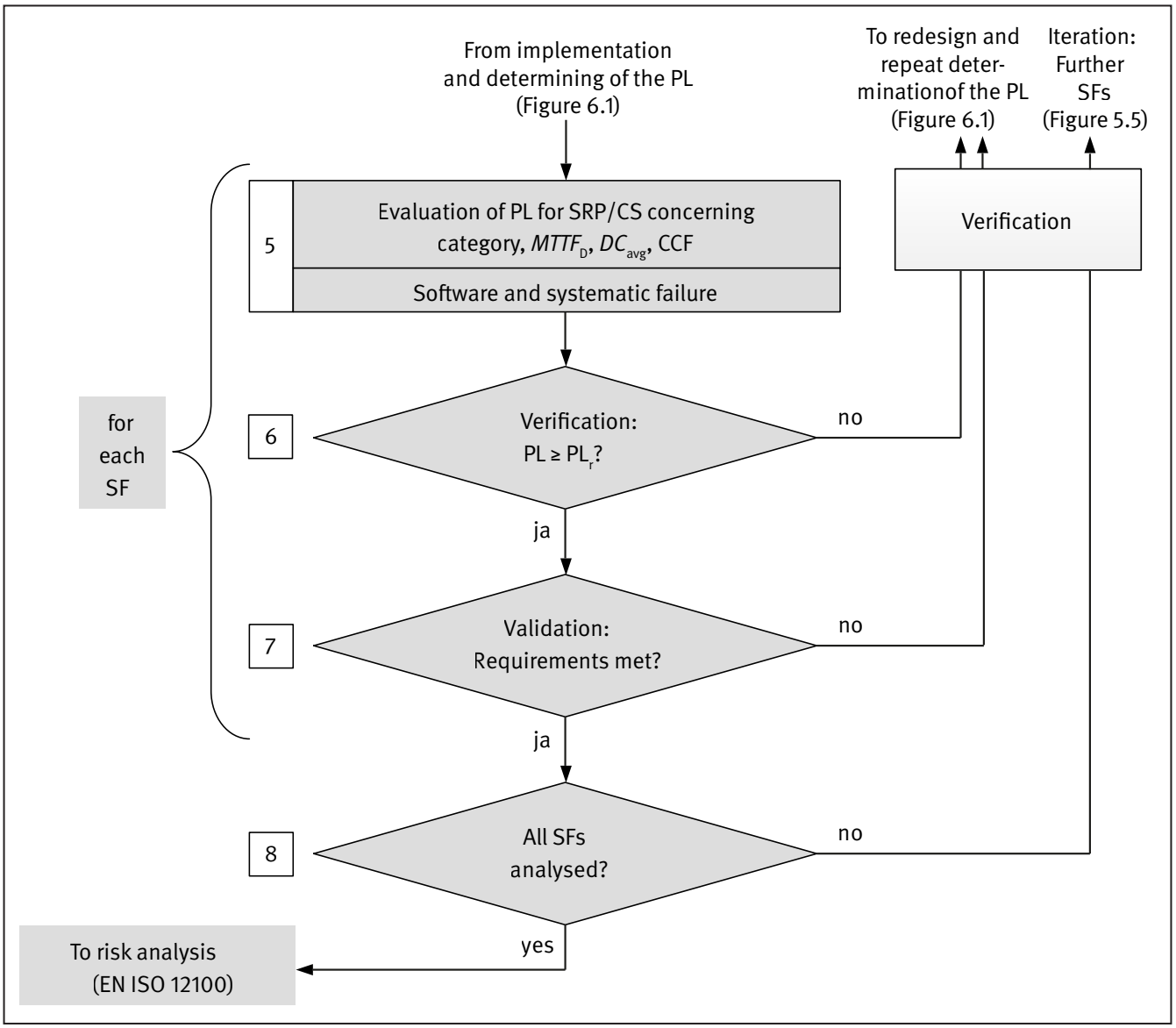


Figure 7.2 can be used for planning of the execution of V&V activities including the corresponding relevant tasks and a reasonable constructive procedure. The figure is taken from Part 2 of EN ISO 13849, but has been simplified graphically in order to present the V&V activities more clearly.

The most important aspects of the verification and validation procedure are explained below.

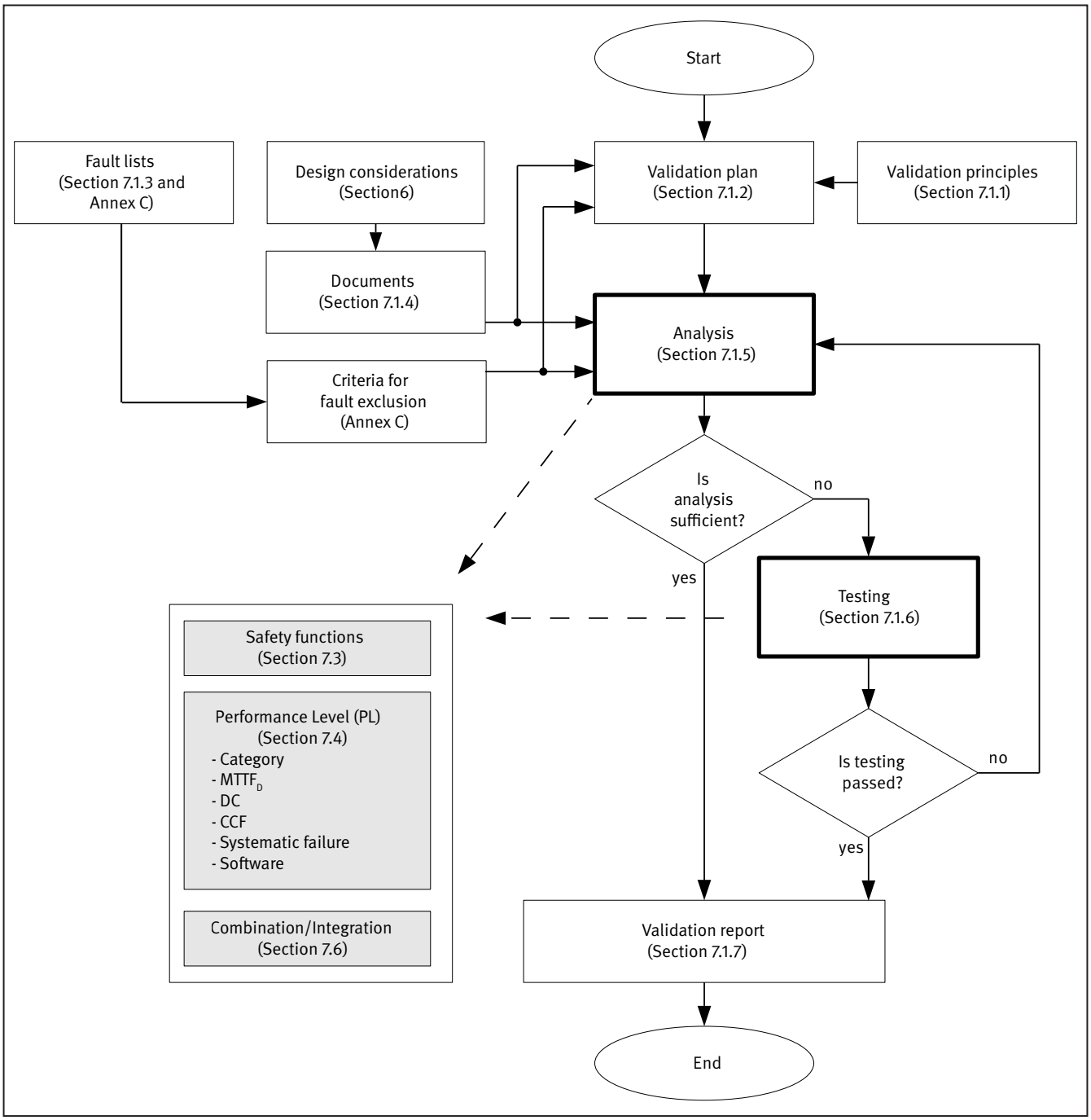
7.1.1 Principles for verification and validation

Verification and validation are intended to assure conformity of the design of the SRP/CS with the reference standards. Since EN ISO 13849-1 is harmonized under the Machinery Directive as a Type B standard for machine controls, the V&V activities must demonstrate that each safety-related part and each of the safety functions that it performs satisfies the requirements of EN ISO 13849-1.

The focus lies here upon the specified properties of the safety functions and the requirements for the specified Performance Level (refer also to subclauses 7.3 and 7.4). EN ISO 13849-2 also specifies that ergonomic design of the user interface(s) shall be addressed by the V&V process.

These activities should be begun as early as possible during development/design, in order to detect and eliminate faults and deviations to the specification in time. The personnel tasked with measures for verification and validation should if possible not be involved in the process of designing the safety-related parts, i.e. they should be able to act independently of the design and development process. The parties concerned may be other persons, departments or bodies that are not subordinate to the design department within the organization's hierarchy. The level of independence should be commensurate with the risk, i.e. the required Performance Level (PL_r).

Figure 7.2:
Overview of the verification and validation procedure according to EN ISO 13849-2



Verification and validation are performed methodically by analysis and testing.

7.1.2 Verification and validation plan

A verification and validation plan has the purpose of describing execution of the V&V process for the specified safety functions, the safety integrity, and all operating and environmental influences that are to be taken into account. The “validation process” in accordance with EN ISO 13849-2, which of course also includes the verification activities, assumes the generation of a verification and validation plan, but specifies neither its form nor its content in detail. All V&V activities accompanying the development/design process are set out in binding form in a verification and validation plan (V&V plan). The plan should contain the following information:

- Identification of the SRP/CS under analysis, if appropriate their components, and possible variants/variations
- Identification of the safety functions with their assignment to the SRP/CS involved
- Reference list of all documents referred to (including the standards and technical rules to be applied) with

descriptions of the requirements, specifications , and obligations in the area of application for the SRP/CS under analysis, together with internal company design rules, such as company hardware design rules and programming rules/guidance documents

- Reference list of the test standards to be applied (i.e. standards governing test methods and performance of testing, not product requirements: for example, the IEC 60068 series governing environmental influences)
- The analyses and tests to be performed; with additional information on the sequence in which the analysis and test methods are to be performed, where specified
- Indication whether and if so what demonstrations of compliance already exist for individual components; including statement of the references to the legacy certificates
- Fault lists to be applied (refer also to subclause 7.1.3 and Annex C)
- Further references to documents concerning the generation of confirmations, for example: QM manual, procedural instructions, forms/samples for V&V activities
- Personnel responsible for the respective analyses and tests (persons, department or body/test institute where applicable)
- Specified (test) environment conditions and equipment/test apparatus/tools/auxiliary equipment for performance of the analyses and tests, together with further operating conditions to be observed; this information may also be listed in the documentation for the results of the individual V&V activities
- The specified documentation of the test results (test reports/protocols) and detailed further documentation of performance of the V&V activities (e.g. test specifications, test case specifications, checklists)
- Evaluation criteria for the analysis and test results, including the measures to be taken in the event of failure to pass an analysis/test
- Formal aspects such as document identification, versioning and modification history, authors/persons responsible, release note(s), signature(s), etc.

The verification and validation plan should reasonably be generated at an early stage of development (recommended: parallel to the specification), thereby delivering the full benefit for ongoing project management. It is also proven good practice to have the V&V plan reviewed or inspected by a person competent in issues of quality management (QM) and quality assurance (QA).

Where larger or more complex overall SRP/CS are being designed, an option is for the V&V plan to set out which validation activities are to be performed only once the systems concerned have been installed within a machine, or whether alternatively automatic test machinery or substitute simulators can be used (for example by means of “hardware in the loop” simulation).

7.1.3 Fault lists

The V&V process must examine and demonstrate the failure mode behavior of the SRP/CS. The principles of fault analysis are stated in Annexes A to D of EN ISO 13849-2 as faults to be considered (modes of failure) and fault exclusions. Annex C of the present report describes the subjects of fault lists, assumed faults/modes of failure and fault exclusions in detail. These general fault lists are based upon past experience. A small number of further standards, such as IEC 61800-5-2 [20] governing the functional safety of electrical power drive systems and IEC 61784-3 [39] governing functionally safe transmission on field buses, contain specialist fault lists. Annex A.2, Table A.1 of IEC 61508-2 governing the functional safety of programmable electronic systems also contains certain precise details of faults in CPU, RAM, ROM and clock. The fault model for highly integrated microelectronic components (microprocessors, DSPs, ASICs, FPGAs, SoCs etc.) is however generally somewhat abstract in its characterization. It is highly advantageous for standard elements (in both software and hardware) to be used for fault diagnostic measures (self-tests, monitoring routines, monitoring components), both for implementation and for demonstration. Examples of such standard elements are the standard CPU self-tests stated in BGIA Report 7/2006, Self-tests for microprocessors incorporating safety functions [50]; RAM self-tests such as Galpat, March, Checkerboard, and numerous others; and commercial watchdog/monitoring modules for IEC 61508/ISO 26262 applications. For components/elements not stated in the fault lists of EN ISO 13849-2, for example for novel technology, the manufacturer should add corresponding lists of faults and fault exclusions of his own. Where fault exclusions are assumed, they shall be supported by adequate reasoning. The fault lists supplemented by the manufacturer then form part of the technical documentation requiring review.

Fault lists exist in standards neither for SRESW nor SRASW (see subclause 6.3). In the general reference, too, software faults are generally discussed with reference to examples rather than in the form of comprehensive fault lists. PC-based tools for static software analysis (for syntax, semantic and code-rule testing) provide very useful support and comprehensive information on faults.

In principle, the same faults shall be considered with regard to common cause failures (CCF), in conjunction with the possible causes of CCF and the relevant countermeasures stated in Annex F.

7.1.4 Documents for V&V activities

As can be inferred from Figure 7.1, detailed documentation is required for the execution of each V&V activity. This concerns technical documentation of relevance throughout the V&V process (particularly the specifications), or documentation that has been produced in the course of design and creation of the SRP/CS and that may be required only for single or selected analyses/tests. The following content (summary) should be given adequate consideration:

- Complete specification of the requirements upon the safety functions and of the requirements upon the design of the SRP/CS. The description of the requirements shall include all performance characteristics, properties, operating modes and anticipated states and processes from which evaluation criteria can be derived
- Operating and environmental conditions with rating data, derived from the intended applications or from the applicable standards; rating data for components
- Functional description of the execution of all safety functions with description of states and processes: The handling of failures/faults in the SRP/CS, i.e. the responses to and states of the SRP/CS in the possible modes of failure/fault, shall be included, as shall the operating concept including all user interactions
- Design description of the SRP/CS (with specifics of the mechanical, electrical, electronic, hydraulic and pneumatic components employed) by means of suitable drawings/sketches, diagrams, plans, data and explanatory text: This includes, for example, general drawings, structure and block diagrams, process/state transition diagrams, wiring plans, descriptions of connections and interfaces, conceptual schematic diagrams, circuit diagrams, electrical plans, fluid power circuit plans, assembly plans, tables of technical data/rating data for components, if applicable data sheets
- Fault analysis/failure mode and effects analysis (FMEA) or failure mode, effects and diagnostics analysis (FMEDA), in consideration of the applied fault lists; for Category 4, including accumulation of faults
- Description of the technical measures taken for the control of faults (fault diagnostics measures)
- Basic and well-tried safety principles observed during the design process, and documented determining of the quantifiable aspects PFH_D, $MTTF_D$, DC_{avg} and CCF for the Performance Level PL of each SRP/CS (quantification documentation), including the list of measures against common cause failures
- Complete software documentation (refer also to subclause 6.3)
- Design rules followed for design and implementation, such as design rules for analog and digital circuits, programming guidelines, etc.
- Substantiating documentation (certificates, test reports, technical records) of components, units or SRP/CS that have already been validated. Also: substantiating documentation of attained reliability values where these were attained by means other than in accordance with EN ISO 13849. Data and where applicable substantiating documentation concerning well-tried components

The documents shall be complete, their content free of contradictions, logically structured, easily comprehensible and verifiable.

7.1.5 Analysis

An SRP/CS or sub-aspects of it are evaluated largely by analysis. This entails both the use of analysis methods that can be performed manually, such as inspections, reviews or walk-throughs for the specification of technical documentation and of the accompanying information; and the use of analysis tools (often PC-based), such as circuit simulators, tools for static and dynamic hardware/software analysis, or FMEA/FMEDA tools and fault simulators for the analysis of components and circuits in fault mode. Verification concerning operating and environmental conditions pushes the scope of analysis to its limits. New methods and processes in product development (such as model-based or virtual development methods) will doubtless lead to the appearance of new analysis methods and analysis tools. The necessary decision regarding where analytical methods shall be accompanied by tests is documented in simple form in the V&V plan.

7.1.6 Tests

Wherever analyses are not possible for the sub-aspect under consideration or evaluation by analysis alone is not adequate, tests shall be performed in order to demonstrate that the requirements are met. Testing shall be planned systematically and executed logically, generally with reference to development stages that can be implemented in practice, such asprototypes, functional models or software/code. The tests shall be performed on a configuration resembling the intended operating configuration as closely as possible. The environmental conditions

under which the tests are to be performed shall be defined in advance. The tests may be performed either manually or automatically.

Where testing is employed for verification, the measurement uncertainty shall be reasonable. EN ISO 13849-2 provides information on the limits that are to be observed.

Subclauses 7.3 to 7.7 describe the typical V&V activities of the individual aspects: safety functions, PL, Category, $MTTF_D$, *DC* and CCF, software, user information and user interface; subclause 7.8 then describes them with reference to the example of a paper-cutting guillotine.

7.1.7 Documentation of results

All analysis and test activities shall be documented together with their results. During documentation of the results, it is important that the technical specifications and assessment standards referred to are dated or referenced by versioning; that the item under analysis/under test (document, software, test specimen, etc.) is uniquely identified; that selected configurations are recorded; that the analysis/test conditions including their setup and procedure are included; and that all verification/validation points/cases are recorded together with the results. Formal information such as document identifiers, persons performing the test/analysis, date, signature, etc. shall of course be documented. Depending upon the level of automation and the tools and equipment used for the V&V measure, the documentation of the results will vary. The content referred to above should however be regarded as the minimum scope of documentation. Documentation management consistent with the need arising from the V&V process is therefore appropriate. Support and resources of any kind used for this purpose, ranging from record forms to document management systems, may be considered valuable.

7.1.8 Completion or iteration

The combination of different SRP/CS involved in a safety function attains a Performance Level PL. At the end of the V&V process, this PL shall be compared to the required Performance Level PL_r for the safety function in question. An adequate safety quality has been attained when the evaluation of "PL ≥ PL_r?" as shown in Figure 7.2 yields a positive result.

If the requirements set out in the specification of the SRP/CS are not met in full, the design and implementation process shall also be reverted to at this stage. If the V&V activities for all safety functions have been completed with a positive result, evaluation of the SRP/CS is deemed by the standard to have been completed. If not, the V&V process shall be continued with respect to the as-yet unresolved safety functions.

Returning to the design and implementation process also means identifying the elements of the V&V process that were not passed and assigning them to V&V activities to which they must once again be subjected. For this purpose, the V&V plan (see subclause 7.1.2) may contain suitable elements, and entries be made in it.

The scenario of negative results shall therefore be addressed in the processes of SRP/CS design and development. Accordingly, processes and measures for the management of defective software are required (for documents, records, data, configurations, software, samples/prototypes, etc.).

7.2 Verification of the specification and the technical documentation

By a wide margin, the document most frequently named (not only in this report) with respect to implementation of an SRP/CS is the specification. This refers to the specification of all requirements (technical specification), specification of the safety functions, specification of the design (with respect of course to safety) with its focus upon software integrity, and specification of the intended operating, environmental and application conditions. Chapter 6 of this report, specifically Box 6.1, contains comprehensive information on the required content of the technical specification. The use of computer-aided specification tools and formal methods for the generation of the specification is possible, albeit unusual.

Verification thus addresses the "specification" document and takes the form of inspection and review. Division of the procedure into two parts has proved effective. Verification is first performed by experienced personnel in the manufacturer's operation. This is followed by verification by a competent external body, such as a test institute.

Verification of the entire development and design documentation is covered by clause 12 of EN ISO 13849-2. This clause is cross-referenced to the required content of the technical documentation (clause10 of the standard). Analyses are suitable activities for verification of the development/design documents (technical documentation). Inspection, review and walk-through constitute typical methods for this purpose; refer necessary for example to IEC 61508-7 [10].

7.3 Validation of the safety function

Validation of the implemented safety function(s) encompasses the activities that demonstrate full compliance with the functional characteristics and performance criteria set out in the specification. Review of implementation

of the points listed in subclause 5.3.1 regarding the specification of safety functions is also useful for determining whether the safety function(s) have been correctly defined and implemented.

To permit an evidence of whether the functional requirements have been met, the following sub-tests shall be performed:

- functional test
- Extended functional test of the behaviour of the SRP/CS in response to input signals, operator processes or inputs that are atypical, unexpected, procedurally incorrect, or lie outside the specification (are invalid)
- Simulation (where possible)
- Performance tests (functional parameters, response time, etc.)

However, final assessment of proper integration of all safety functions on the complete machine includes a series of further aspects, such as the dimensioning of overruns and safety clearances.

7.4 Verification of the PL of the SRP/CS

This subclause describes the activities normally performed for demonstration of the attained Performance Level PL of a single SRP/CS. The procedure to be followed for combinations of several SRP/CS is explained in subclause 7.6.

The PL of an SRP/CS is determined on the one hand by quantifiable aspects/values such as the $MTTF_D$, *DC*, CCF and the Category, and on the other by qualitative aspects such as the behaviour under fault conditions of the safety function, the design measures for the safety-related software and systematic failures, and the functional behaviour under the anticipated (maximum) operating and environmental conditions. Evaluation of the individual aspects is followed by a description of a procedure for checking the estimation of the PL. Like EN ISO 13849-1 and -2, the present report and this subclause assume that the "simplified method" is selected for estimation of the PL. This method has already been described.behaviour

7.4.1 Verification of the Category

The objective of verifying the Category is to confirm that all requirements placed upon the Category are met in the development step under analysis; refer to subclauses 6.2.2 to 6.2.7 in the behaviourpresent report and subclauses 9.2.1 to 9.2.5 in [6].

The following analyses shall be performed:

- Structure and signal path analysis of the technical circuit documentation
- Evaluation of implementation and effectiveness of the fault diagnostics measures
- Inspection of the observance of basic safety principles
- Inspection of the implementation of well-tried safety principles (Category 1 and higher)
- Inspection of the use of well-tried components (Category 1 only)
- Evaluation of faults to be analysed and permissible fault exclusions including their reasoning where added to fault lists on a case-by-case basis

The annexes in Part 2 of the standard, and also Annex C of this report, provide detailed assistance in execution of the last four of the analyses stated.

The following sub-tests shall be added if the preceding analyses are not sufficient or fault analyses performed on the test specimen are to be confirmed:

- Tests of the behaviour under fault conditions of the SRP/CS with fault injection, i.e. testing of the safety functions under fault conditions (test of the effect of failure); alternatively, fault simulation where the test cases with fault injection are not practicable
- Use of extended functional tests to test the behaviour of the SRP/CS in the event of input signal states that are rare, unexpected, lie outside the specification or are defective, and defective processes/inputs during operation

7.4.2 Verification of the $MTTF_D$ values

The $MTTF_D$ values employed for determining of the PL should be checked at least for plausibility. This typically includes evaluation of whether suitable sources are stated for the origin of the values. Review of the precise reasoning given for the values is also recommended for the dominant components and otherwise by random selection for all other components. The data sources stated in subclause 6.2.12 and Annex D can for example be used for this purpose. Suitable determining of the B_{10D}, T_{10D} and n_{op} values is verified analytically, and correct calculation subsequently checked, at least for plausibility.

7.4.3 Verification of the *DC* values

The diagnostic coverage (*DC*) assigned to the blocks or, where applicable, components shall be dimensioned reproducibly. Here too, the stated origin of the values and the reasoning for them is typically analysed. Annex E provides guidance concerning estimation of the *DC* values. This can also serve as a basis for verification.

The implemented design shall be analysed regarding whether the fault diagnostics measures described have been implemented. For this purpose, it is generally necessary for the fault diagnostics functions and modules to be identified in the development documentation, and toestimate their effectiveness . In addition, tests of the behaviour under fault conditions of the SRP/CS (failure mode and effects testing/testing by fault injection) should show that proper fault detection is assured by the fault diagnostics functions. Finally, calculation of the DC_{avg} is to be checked at least for plausibility.

7.4.4 Verification of the measures against CCF

EN ISO 13849-1, Annex F contains a points-based method for evaluation of the selected measures against common cause failures (CCF). Besides checking of attainment of the total number of points and clarification that the selected measures are described comprehensively in the associated documents, analysis or testing shows that the measures have actually been implemented. The typical V&V activities employed for this purpose include static hardware analysis and functional testing under environmental conditions (limit conditions).

7.4.5 Verification of the technical measures against systematic failures

V&V activities concerning technical measures for the avoidance and control of systematic failures assess whether the required design measures described in EN ISO 13849-1, Annex G and explained further in subclause 6.1.2 of this report have been implemented. Confirmation can typically be provided by:

- Functional testing at limit values and with modified rated values, and failure mode and effects testing/testing by fault injection on the supply units (e.g. voltage breakdown, voltage fluctuation, overvoltage, undervoltage, changes in AC current and frequency, clock change and other phenomena and operating stresses that may lead to failure)

- Testing of the resistance to interference caused by ambient influences, i.e. functional testing under specified environmental conditions (climatic conditions, mechanical stress, electromagnetic compatibility, etc.); see clause 10 in [6]

- Analysis of implementation of program execution monitoring

- Inspection and testing of the safety-related properties of data communications systems; where used, identification of certified components

- Inspection of development documents that confirm the application of basic and well-tried safety principles and further measures taken, such as hardware diversity

The present report does not address the evaluations of organizational measures required by EN ISO 13849-2 [6] for the avoidance of systematic failures, such as quality management systems for the manufacturing process (subclause 9.4 e in [6]).

7.4.6 Verification and validation of the software

The verification activities performed in the course of specification, design and coding of the software (inspection/review for software specification, software design and code, static software analysis, module test, software simulation, integration test) have already been described comprehensively in subclause 6.3. For verification of the software, too, graded software design measures shall be specified in this context according to the PL to be attained.

The final development activity in the simplified “V model” is that of software validation. Whether the requirements stated in the safety-related software specification concerning the functional behaviour and the performance criteria (e.g. time-related specifications) have been implemented correctly shall be examined. At this stage, validation no longer considers the internal workings of the software, but its “external” behaviour, i.e. the behaviour at the output in response to changes at the inputs, with the complete software integrated into the hardware. The software is considered here as a “black box”, and is validated by the “black-box test”. Supplementary I/O tests ensure that the safety-related input and output signals are used correctly. The functional test is then performed at system level (on the SRP/CS). Performance of an extended test case with (possibly simulated) fault cases serves to demonstrate the effectiveness and correct implementation of fault detection and fault handling (reaction in the event of a fault) implemented by the software.

Individual software functions that have already been certified or validated by quality assurance measures in the form of safety function blocks do not require re-testing. Evidence shall however be furnished that validation has already been performed. Where a number of such safety function blocks are combined for a specific project, how-

ever, the resulting safety function shall be validated as a whole.

In the particular case of SRESW used in SRP/CS with PL e and not developed with diversity for the two channels, the requirements for SIL 3 set out in clause 7 of IEC 61508-3 [42] shall be satisfied in full during software development. This includes the V&V activities required in the clauses concerned.

Should the safety-related software subsequently be modified, it shall be reverified and revalidated on an appropriate scale. The verification and validation plan described in subclause 7.1.2 can and should serve as an aid to planning for this purpose.

A further area of software verification concerns configurable, parameterizable and programmable SRP/CS. Where parameterization and programmability are software-based, implementation and effectiveness of the measures shall also be demonstrated consistent with the requirements of EN ISO 13849-1, subclause 4.6.4, and thus with the configuration tools employed (parameterization/programming programs where applicable) as a mandatory part of the V&V activities. These activities involve both analyses of the documentation of these tools and tests on the items themselves.

7.4.7 Checking of the assessment of the PL

Checking that the PL has been assessed properly for each SRP/CS particularly entails comprehension of proper application of the assessment method employed, including correct calculations.

If the PL was assessed by means of the simplified procedure, a check can be performed with reference to Figure 6.10 of whether the correct PL for the SRP/CS was determined from the Category, $MTTF_D$ and DC_{avg} values confirmed beforehand.

7.5 Verification of the information for use

Important information on safe use of the SRP/CS shall be made available in the form of instruction handbooks, assembly instructions, rating plates and maintenance instructions. These documentation elements, described in their entirety as the information for use, and according to the Machinery Directive, also including the sales brochures(!), shall be evaluated to ascertain whether they include all the content stated in clauses 9 and 11 of EN ISO 13849-1. EN ISO 13849 does not set out any rules of its own concerning the form of the documentation (language, digital or print form). The requirements (and committee decisions) at the level of the Machinery Directive apply. General guiding principles such as those of IEC 82079-1, Preparation of instructions for use [51], can be followed for the presentation (layout, typography, etc.) of information for use. Their application during evaluation is however not mandatory. Information supplied with the product is usually analysed by inspection and/or review.

7.6 Validation of the combination and integration of SRP/CS

Individual SRP/CS shall be validated separately prior to combination. In order for systematic faults to be avoided during the combination/integration of SRP/CS, the following V&V activities shall be performed:

- Inspection of the design documents that altogether describe implementation of the safety function concerned
- Comparison of the characteristic data for the interfaces between the SRP/CS (e.g. voltages, currents, pressures, information data)
- FMEA/fault analysis of the combination/integration
- Functional test
- Extended functional test
- Checking of simplified determining of the overall PL from the PLs of the individual SRP/CS, as described in subclause 6.4.

Integration of (multiple) SRP/CS is not – yet – synonymous with their commissioning with the associated commissioning tests on a machine. The validation activities stated here, supplemented by the highly advantageous interface test/"I/O test", are however suitable for this purpose without restriction.

Retrofitting safety technology or integrating new SRP/CS into existing machine controls may present a particular challenge. Planning of the above V&V activities in good time, applying them thoroughly irrespective of the pressures that may arise, possibly not before installation on site, and documenting the activities from end to end contribute substantially to SRP/CS being integrated reliably.

7.7 Verification of the user interface (ergonomic design)

Requirements set out in EN ISO 13849 concerning the ergonomics of the user interface refer to universal design targets such as the prevention of hazardous action, circumvention/manipulation of the SRP/CS, general ergonomic principles such as simplicity, and the ergonomic principles referenced in EN ISO 12100 [3] and ISO 9355 [52]. At the same time, it explicitly requires consideration to be given to foreseeable incorrect operation.

If further guidance documents are required for verification of the user interfaces, application of design guidelines such as the following may be advantageous: VDI/VDE 3850, Development of usable user interfaces for technical plants [31]; the VDMA guide to software ergonomics and the design of user interfaces [53]; and EN ISO 9241-11, Ergonomics of human-system interaction – Part 11: Usability [54].

Finally, this subclause is intended to confirm the view that the use of SRP/CS – and also software modules and tools – that have already been certified or type-examined considerably simplifies and accelerates verification and validation of circuitry for safety functions.

7.8 Verification and validation with reference to the example of a paper cutting guillotine with diverse redundancy in the logic control (Category 4 – PL e)

The general description of verification and validation of safety functions and PL is supplemented in this subclause by an explanation of the V&V activities for the practical example of the paper cutting guillotine described in subclauses 5.7 and 6.5. It is assumed at this point that all necessary documents and a prototype of the machine are available. Based upon the documents, the steps of verification and validation will be shown here for a representative example of the safety functions, "SF2 – Controlled location of the operator's hands outside the danger zone during a hazardous movement" (subclause 5.7.3). The available documents include the verification and validation plan, which describes the activities required in the various phases (subclause 7.1.2). Owing to the level of the hazard potential, it is advisable to have the work performed by independent persons, for example from a different department (subclause 7.1.1).

This subclause observes the definition of verification and validation stated in the introduction in clause 7. Frequently however, the boundaries are blurred, and precise classification difficult. An example is testing, for example of software. These tests are also referred to in the reference as validation, the purpose of which is to determine whether the program or parts of it fulfil their function (as stated in the specification). These steps could also be described as verification.

7.8.1 Verification of the attained PL (refer also to Block 6 in Figure 7.1)

An estimation of the risk showed that a Performance Level PL_r of e shall be attained for the desired safety function SF2. This analysis is consistent with the requirement in EN 1010-1 [28], which further details the technical requirements with reference to the requirements of the relevant standard governing two-hand controls, EN 574 [55]. The underlying conditions to be met are stated in the system specification and confirmed by validation. The verification now being performed confirms proper implementation of the terms, in this case by calculation of the PL with the aid of the SISTEMA software tool. This PL is attained in the calculation of the probability of failure in consideration of all quantifiable aspects. All requirements concerning the qualitative aspects, such as the behaviour under fault conditions of the safety function, including the measures for fault detection implemented in the safety-related software, the measures against systematic failures and the behaviour under environmental conditions, are also adequately met for PL e.

The above conclusions were clearly reached at different points in time during development, or could in fact only have been reached during certain phases. Demonstration of satisfaction of the EMC requirements, for example, is not possible until a prototype has been fabricated.

The validation/verification activities below do not constitute a sequence that must be strictly followed. Rather, the intention here is to demonstrate the work entailed by the relevant phases of the V&V model with reference to the example of the SF2.

7.8.2 Validation of the safety-related requirements (refer also to Block 7 in Figure 7.1)

Fault lists

The PL is determined based upon the fault lists according to EN ISO 13849-2 [6].

Documents

As already stated in subclause 7.1.4, analysis/testing is conducted with reference among other things to circuit diagrams, parts lists, the complete specification, functional description, and also the design description, fault/failure mode effects analysis, the software specification and software documentation.

Documentation

All analysis and test results shall be documented in writing. The criteria for evaluation of whether a test has or has not been passed are important and are contained in the verification and validation plan.

Validation of the safety function

In order to check the functional requirements upon the safety function, a functional test is performed, supplemented by an extended functional test for testing of the

behaviour of the safety function in response to rare or non-defined inputs. A possible example of such a test is testing of the response of the SRP/CS when a valid cut request from the two-hand control is accompanied by a fault signal, for example on peripheral equipment or initiated by a stop command from a light curtain. Performance tests of functional aspects are also conducted. These include, for example, a check of the time to be observed for synchronous actuation in accordance with EN 574 [55]. Only when the two actuators S1 and S2 are operated within an interval of ≤ 0.5 seconds may output signals be generated for actuation of the clamping bar and the knife.

The tests and analyses stated above for the specified safety characteristics have been passed.

Verification of the PL of the SRP/CS

- Verification of the Category

  The essential terms of reference for the Category of the SRP/CS are laid down at an early stage of development, based upon the complete or binding specification. Category 4 was also selected for the determined PL_r e. Verification of the specification showed that the circuit structure based upon it (diverse redundancy, see also subclause 6.5.2) satisfies the requirements for a Category 4.

  For the two-hand control, as envisaged in this case, tests of the behaviour under fault conditions are performed on a prototype with reference to the development documentation. This verifies whether the requirements overall for a Category 4 are also met in this case. Testing is performed by the controlled injection of faults. The SRP/CS shall respond to the injected faults in the manner specified. An analysis is first performed, followed by testing, to ascertain the behaviour when, for example, individual contactor relays are no longer capable of executing switching commands, or of how the SRP/CS react when one of the two actuators S1 or S2 is actuated with a delay, or not at all. The safety function shall be assured at all times when a single fault is injected into the SRP/CS. A single fault shall be detected at or prior to the next execution of the safety function. Should the fault not be detected, an accumulation of further faults shall not result in loss of the safety function. The expected safe response for each injected fault is described in the associated test protocol and the behaviour of the SRP/CS commented with the evaluation criterion of “passed” or “not passed”.

  Observance of the de-energization principle as an example of basic safety principles can be demonstrated by the injection of interruptions and evaluation of the response to them. Should for example the supply voltage fail, the clamping bar and the knife are returned to their initial positions by spring force.

  Plausibility tests can be cited in this context as an example of well-tried safety principles: mechanically linked contacts in the contactor relays K3 to K6 are read back by both channels. Tests are performed to demonstrate proper functioning of readback.

- Verification of the $MTTF_D$ values

The value of 150 years, substituted for the valves 1V3, 1V4, 2V2 and 2V1, is considered here by way of example for verification of the $MTTF_D$ values (see Figure 6.15). The manufacturer's figure was obtained from a reliable source, and its plausibility was confirmed by comparison with the corresponding value in Table C.1 of EN ISO 13849-1 [5] (see Table D.2 of the present report). The conditions stated by

Design features

- The requirements of Category B, basic and well-tried safety principles, are observed. Owing to diversely redundant processing channels (microcontroller and ASIC), a single fault does not result in loss of the safety function, and systematic faults are largely prevented.
- The safety-oriented switching position is assumed from any position by cancellation of the control signal.
- All electrical signals, including those of the pressure sensors, are processed in a multi-channel control system.
- The actuators S1 and S2 of the two-hand control satisfy IEC 60947-5-1.
- K3 to K6 possess mechanically linked contacts according to IEC 60947-5-1, Annex L [56]. The associated break contacts for monitoring of the make contacts are monitored in the respective adjacent channel.
- All conductors carrying signals are laid either separately or with protection against mechanical damage.
- The software (SRESW) is programmed in accordance with the requirements for PL d (downgraded owing to diversity) and the guidance in subclause 6.3.
- Fault-avoidance measures in development of the ASIC are performed in accordance with the ASIC development life cycle (V model) of IEC 61508-2 [48].

the manufacturer for assumption of the $MTTF_D$ value (e.g. oil changes) are described in the instruction handbook and it is assumed that these conditions are observed in operation.

- Verification of the *DC* values

  A *DC* of 90% is confirmed for K1 and K2, based upon self-diagnostics. This includes a cross monitoring of input signals and intermediate results (from the microcontroller and the ASIC), monitoring of the timing and logic of program execution, and detection of static internal and peripheral failures. Further tests are a CPU test in the channel containing the microcontroller, in which all commands used are tested, and tests of adequate quality of the random-access memory (RAM) and read-only memory (ROM). Tests of comparable quality to those in the parallel channel are performed in the second channel (ASIC). It shall be demonstrated by verification that the measures described in the specification have been implemented correctly.

  The contactor relays K3, K4, K5 and K6 are assigned a *DC* of 99%. This is appropriate owing to the plausibility testing by readback of the mechanically linked contacts of the contactor relays. The plausibility tests that have already been checked during verification of the Category also serve at this point to demonstrate proper operation.

  The pushbuttons S1 and S2 are assigned a *DC* of 99%. The reasoning for this is cross monitoring and a frequent signal change. This assumption is confirmed by verification. This assumption will be proven by a fault-case test at another point.

  The valves 2V1, 2V2, 1V3 and 1V4 are monitored cyclically indirectly by the pressure switches 2S1 and 1S3. Since the positions of the valves can be queried for their plausibility parallel to the machine cycle, a value of 99% for the *DC* is regarded as reasoned. Here too, the assumption is confirmed on the prototype by fault tests on the valves.

- Verification of the measures against CCF

  The minimum requirements for measures against common cause failure are satisfied, with at least 65 points. Further measures are also effective in parts of the control system. 15 points are allowed for implementation of the measure “physical separation between the signal paths”. Correct implementation of the measure shall be demonstrated by an analysis of development documentation such as circuit diagrams, and by tests on the hardware. The diversity employed for K1 and K2 makes a substantial contribution to the CCF: the different technologies of K1 and K2 are the reasoning for the 20 points assigned for diversity.

- Verification of the measures against systematic failures

  The observance of basic and well-tried safety principles is a highly effective measure against systematic failures. The activities for verification of the Category also encompass checking of whether both types of safety principle have been observed. The results of the analyses and tests performed for that purpose can thus also be used for assessment in this phase.

  Besides the tests, an inspection is performed during development of the documentation describing the basic and well-tried safety principles applied and the measures for the control and avoidance of systematic failures according to subclause 6.1.2 of this report and Annex G of the standard. The purpose of this inspection is assessment of whether the principles and measures have been adequately considered during the development process.

  An example of the control of systematic system failures is that the safety-related software monitors execution of the program sequence for errors. The effectiveness of process monitoring is tested by injected faults.

  In order to demonstrate the capacity of the SRP/CS to withstand the specified environmental conditions, tests are performed under all anticipated and predictable adverse conditions for factors including temperature, humidity and electromagnetic interference. This constitutes an example of a measure for the avoidance of systematic failures. The limits for the temperature and humidity under which the paper-cutting guillotine may be operated are set out in the specification, which is confirmed by verification of the document.

- Verification of the software

  Development and validation of the software are described in detail in subclause 6.3. At this point, the software is also verified, i.e. testing is performed of proper operation and also of the response times of the software integrated in the hardware. Testing takes the form of functional tests (black box tests) and extended functional tests in which firstly, the safety-related input signals shall be processed correctly to safety-related output signals, and secondly, test cases with injected faults are executed in order to verify the specified fault-mode responses of the firmware of the microcontroller K1. In other words: it is clarified whether the requirements of the specification have been implemented correctly in the software.

- Checking of the assessment of the PL

  The simplified procedure according to EN ISO 13849-1 was applied for estimation of the PL. Its correct application is confirmed. Calculation of the $MTTF_D$ in accordance with subclause 6.2.11 and Annex D and of the average diagnostic coverage DC_{avg} in accordance with Annex E is checked, as is correct determining of the PL from the previously confirmed Category, $MTTF_D$, and DC_{avg} values by means of the bar chart shown in Figure 6.10.

- Verification of the information for use

  The information for use shall be reviewed concerning the two-hand control. This also includes explanation of the function in conjunction with the safety objectives that are to be attained. It is immaterial when the information for use of the SRP/CS passes review, including with regard to the following points: description of the intended use; statement of information on the PL and the Category (including dated reference to the standard); explanation of all operating modes; description of the safeguards and safety functions with response times, environmental conditions for operation and external interfaces; information and technical data on transport, safe erection, commissioning and maintenance. Here too, the result of the review shall be recorded in writing.

- Validation of the combination and integration of SRP/CS

  The safety function described is implemented by an SRP/CS. Since the different technologies, electronic and hydraulic, are however combined within this SRP/CS, certain tests that are necessary when SRP/CS are combined should also be performed here, unless they have already been included in validation of the Category. These tests include comparison of the interface data between the technologies employed, and functional tests and extended functional tests.

7.8.3 Examination of whether all safety functions have been analysed (see also Block 8 in Figure 7.1)

The V&V activities shown here for SF2 are conducted for all safety functions performed by the SRP/CS (SF1 to SF6). The additional effort is however low, since many safety functions employ the same hardware. The analyses and tests shall show that the safety functions have been implemented correctly. Once all safety functions have been analysed, evaluation according to EN ISO 13849-1 and -2 is complete.

8 Circuit examples for SRP/CS

Changes with respect to the second edition (BGIA Report 2/2008e):

- Example Nos 8, 26 and 36 deleted
- New example No 38 on hydraulic valve drive inserted
- Substantially modified examples: Nos 17, 19 and 24

This report began by addressing the design of safe control systems in general terms. Subclauses 5.7, 6.5 and 7.6 then illustrated, with reference to the example of a paper-cutting guillotine, how the methods for the design of safe control systems can be implemented. The methods for determining the PL are described step by step here and in EN ISO 13849-1; some of these steps however, such as deriving the safety-related block diagram from the circuit diagram, require some practice. SISTEMA Cookbook 1 [33] provides guidance on deriving the safety-related block diagram and the SISTEMA file from the circuit diagram. However, owing to the variety of possible safety functions and their implementation, the individual steps do not lend themselves to generic description. For this reason, this chapter will now present the evaluation of numerous circuit examples that implement the safety functions in various Categories and Performance Levels and by means of different technologies. In the circuit examples, the concept of a control system generally covers only the safety-related parts of control systems. The examples are limited to essential aspects, and therefore serve primarily to illustrate the methodology. Importance was attached in their selection to a wide spectrum of technologies and possible applications. Readers familiar with the 1997 report [9] on the Categories for safety-related control systems to EN 954-1 will recognize some of the examples, to which for example calculation of the probability of failure has been added. Compared to the BGIA Report 2/2008e [57], certain examples that are no longer up to date have been deleted; one new example has however also been added. The examples are an interpretation of the Categories, and have been compiled by the authors based upon many years of experience with safety-related machine control systems and work on national and European standards committees. The examples serve to provide designers with effective guidance for their own developments. Since the examples were created by different authors, some variation inevitably exists, for example in their presentation of details or in the reasoning behind certain numerical data. All calculations for the circuit examples were performed with the aid of Version 2.0 of the SISTEMA software application (see Annex H), the version available at the time of production of this report. Further circuit examples, including SISTEMA files, are also described in IFA Report 4/2018e, “Safe drive controls with frequency inverters” [22].

The description in each example is structured as follows:

- Safety function
- Functional description
- Design features
- Remarks
- Calculation of the probability of failure
- More detailed references

Under “safety function”, the name of the safety function is stated together with the events that trigger it and the required safety responses.

The “functional description” describes the essential safety-related functions, based upon a conceptual schematic diagram. The behaviour in the event of a fault is explained, and measures for fault detection are stated.

The particular characteristics in the design of the example in question, such as the application of well-tried safety principles and the use of well-tried components, are listed under the “design features”.

The circuit diagrams are conceptual schematic diagrams that are limited solely to presentation of the safety function(s) with the relevant components required for this particular purpose. In the interests of clarity, certain additional circuitry that is normally required has been omitted, for example that for the assurance of electric shock protection, for control of overvoltage/undervoltage and overpressure or low pressure, for the detection of insulation faults, short-circuits and earth faults for example on lines routed externally, or for assurance of the required resistance to electromagnetic disturbance. Circuit details that are not essential for determining the safety-related block diagram have thus been deliberately omitted. Such details include protective circuitry in the electrical system, such as fuses and diodes, for example in the form of free-wheeling diodes. The diagrams also omit decoupling diodes in circuits in which sensor signals, for example, are read in redundantly into multiple logic units. This arrangement is intended to prevent an input becoming an output on redundant systems in the event of a fault, and thus influencing the second channel. These components are all essential in order for a control system to be implemented in accordance with a Category and a Performance Level. In accordance with the fault lists in EN ISO 13849-2, issues such as the influence of conductor short circuits must of course also be considered in relation to the safety function concerned and the conditions of use. All components used must therefore be selected with consideration for their suitability according to their specification. Overdimensioning is one of the well-tried safety principles.

Further examples are listed in the technology-specific remarks on fluid power technology.

Design features are stated only where they are relevant to the safety functions described. This is generally a "safety-related stop function, initiated by a safeguard". Other safety functions, such as the "prevention of unexpected start-up" or a "manual reset function" and "start/restart function" are not considered in all examples. If manually operated equipment (pushbuttons) is used for the implementation of such safety functions, it must be ensured that where the safety function is implemented in conjunction with electronics, in particular, it must be initiated by the release (break operation) of a button already pressed.

Where relevant to the example concerned, particular reference is made under "Remarks" to aspects specific to a possible application.

Under "Calculation of the probability of failure", a description is provided of calculation of the PL from the parameters Category, $MTTF_D$, DC_{avg} and CCF, based upon the safety-related block diagram derived from the conceptual schematic diagram. The Category is determined from the functional description and the design features.

The $MTTF_D$ values employed in the calculations are marked as manufacturer's values ("[M]" for manufacturer), typical values from databases ("[D]" for database), or values from EN ISO 13849-1 ("[S]" for standard). In accordance with the standard, priority should be given to manufacturers' data. For certain components, neither reliable manufacturers' data nor database values were available at the time of production of the report. In this case, use was made of the parts count method for estimation of typical example values (marked "[E]" for estimated). The $MTTF_D$ values in this chapter should therefore be regarded in some cases more as estimates.

The presentation of the assumed measures for diagnostics (*DC*) and against common cause failure (CCF) is limited to general information. Specific values for these two criteria are dependent upon the implementation, the application and the manufacturer. It is therefore possible for different *DC* values to be assumed for similar components in different examples. Here too, all assumptions regarding *DC* and CCF must be reviewed in real-case implementations; the assumed values are not binding and are intended solely for the purpose of illustration.

The focus in the presentation lies more upon the Categories in the form of the "resistance to faults", the block diagram and the "mathematical" methods for determining the PL. Conversely, some sub-steps, such as fault exclusion, basic and well-tried safety principles or measures against systematic faults (including software) are mentioned only briefly. During implementation, appropriate attention must be paid to this aspect, since misjudgements or inadequate implementation of these measures could lead to a deterioration in the fault tolerance or probability of failure. As an aid to understanding of the circuit examples and for their practical implementation, the reader's attention is therefore drawn to Chapter 7 and Annex C, in which, for example, the basic and well-tried safety principles are described in detail.

Finally, reference is made to "more detailed references", where available.

For each form of technology, certain comments of a general nature are made in the following technology-specific subclauses in order to provide a better understanding of the examples and for implementation of the Categories. Some of the circuit examples represent "control systems involving multiple technologies". These "mixed" circuit examples are based upon the concept, enshrined in the standard, that a safety function is always implemented by "reception", "processing" and "switching", irrespective of the technology employed.

8.1 General technology-related remarks on the example control systems

8.1.1 Electromechanical controls

Electromechanical controls primarily employ electromechanical components in the form of control devices (e.g. position switches, selector switches, pushbuttons) and switchgear (contactor relays, relays, contactors). These devices have defined switching positions. They do not generally change their switching state unless actuated externally or electrically. When selected properly and used as intended, they are largely immune to disturbance, such as electrical or electromagnetic interference. In this respect they differ, in some cases considerably, from electronic equipment. Their durability and failure mode can be influenced by suitable selection, dimensioning and arrangement. The same applies to the conductors employed, when suitably routed within and outside the electrical compartments.

For the reasons stated above, the electromechanical components generally satisfy the "basic safety principles", and in many cases are also to be regarded as "well-tried components" for safety applications. This holds true, however, only when the requirements of IEC 60204-1 [25] for the electrical equipment of the machine/installation are observed. In some cases, fault exclusions are possible, for example on a control contactor with regard to pick-up in the absence of a control voltage, or non-opening of a break contact with direct opening action on a switch to IEC 60947-5-1 [56], Annex K.

Detailed information on the modelling of electromechanical components can be found in Annex D.

8.1.2 Fluid power controls

On fluid power installations, the area of valves, i.e. valves controlling hazardous movements or states, should in particular be considered a “safety-related part of the control system”. The fluid power circuits listed below constitute example arrangements only. As a rule, the required safety functions can also be implemented by means of alternative control logic employing appropriate valve types, or for that matter in some cases by additional mechanical solutions such as hold devices or brakes.

On hydraulic systems (see Figure 8.1), measures for pressure limitation in the system (1V2) and for filtration of the hydraulic fluid (1Z2) must also be considered in this context. The components 1Z1, 1S1 and 1S2 shown in Figure 8.1 are present in the majority of hydraulic systems and are of great importance, particularly for the condition of the hydraulic fluid and consequently for the valve functions. The reservoir breather filter 1Z1 arranged on the fluid reservoir prevents the ingress of external dirt. The fluid level indicator 1S2 ensures that the fluid level remains within the specified limits. The temperature indicator 1S1 constitutes suitable measures for limitation of the operating temperature range and thus the operating viscosity range of the hydraulic fluid. If necessary, heating and/or cooling equipment must be provided in conjunction with closed-loop temperature control (refer also to Annex C in this context).

The drive elements and the components for energy conversions and transmission in fluid power systems generally lie outside the scope of the standard.

On pneumatic systems (see Figure 8.2, Page 102), the components for the prevention of hazards associated with energy conversion and the maintenance unit for compressed air conditioning must be considered from a safety perspective in conjunction with the valve area. In order for the possible energy conversions to be controlled with consideration for safety aspects, an exhaust valve is frequently used in conjunction with a pressure switch. In the circuit examples in this chapter, these components are marked 0V1 (exhaust valve) and 0S1 (pressure switch). The maintenance unit 0Z (see Figure 8.2) generally consists of a manual shut-off valve 0V10, a filter with water separator 0Z10 with monitoring of the contamination of the filter, and a pressure control valve 0V11 (with adequately dimensioned secondary venting). The pressure indicator 0Z11 satisfies the requirement for monitoring of the system parameters.

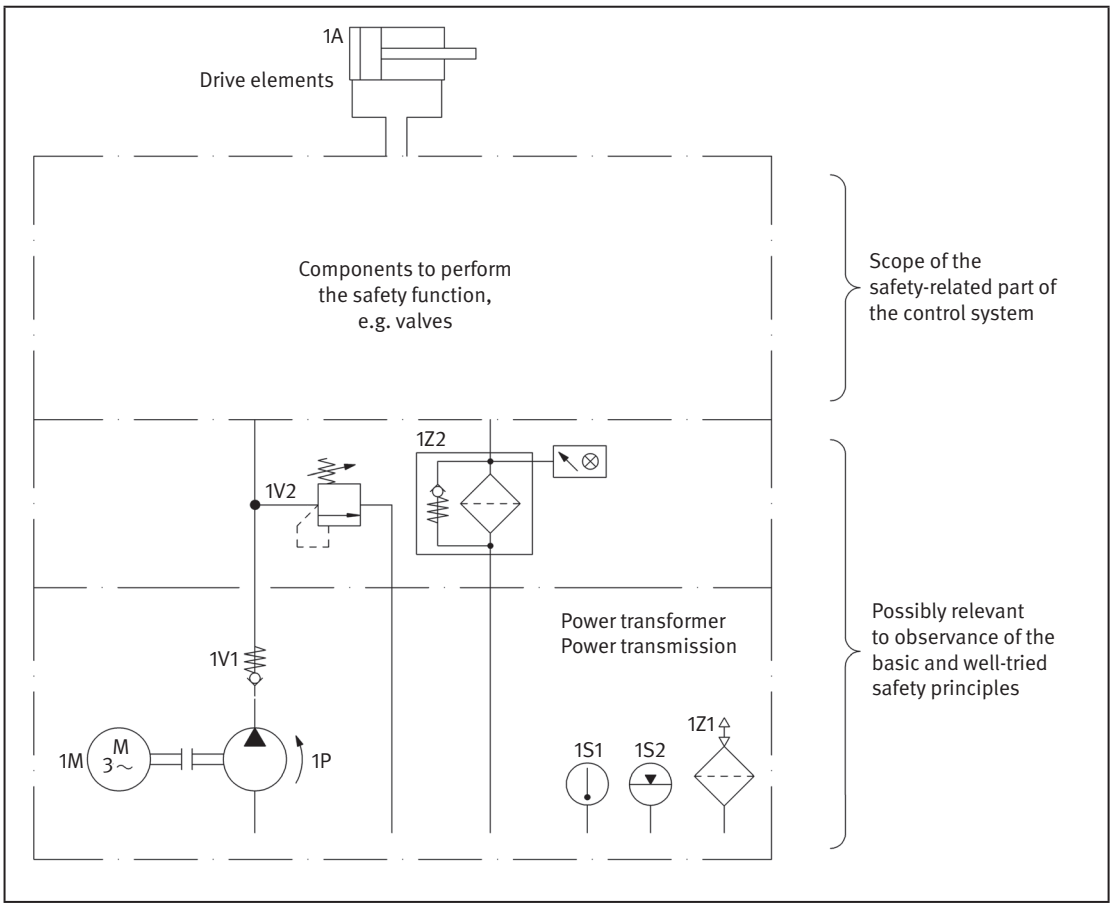


Figure 8.1: Scope of EN ISO 13849 for hydraulic systems

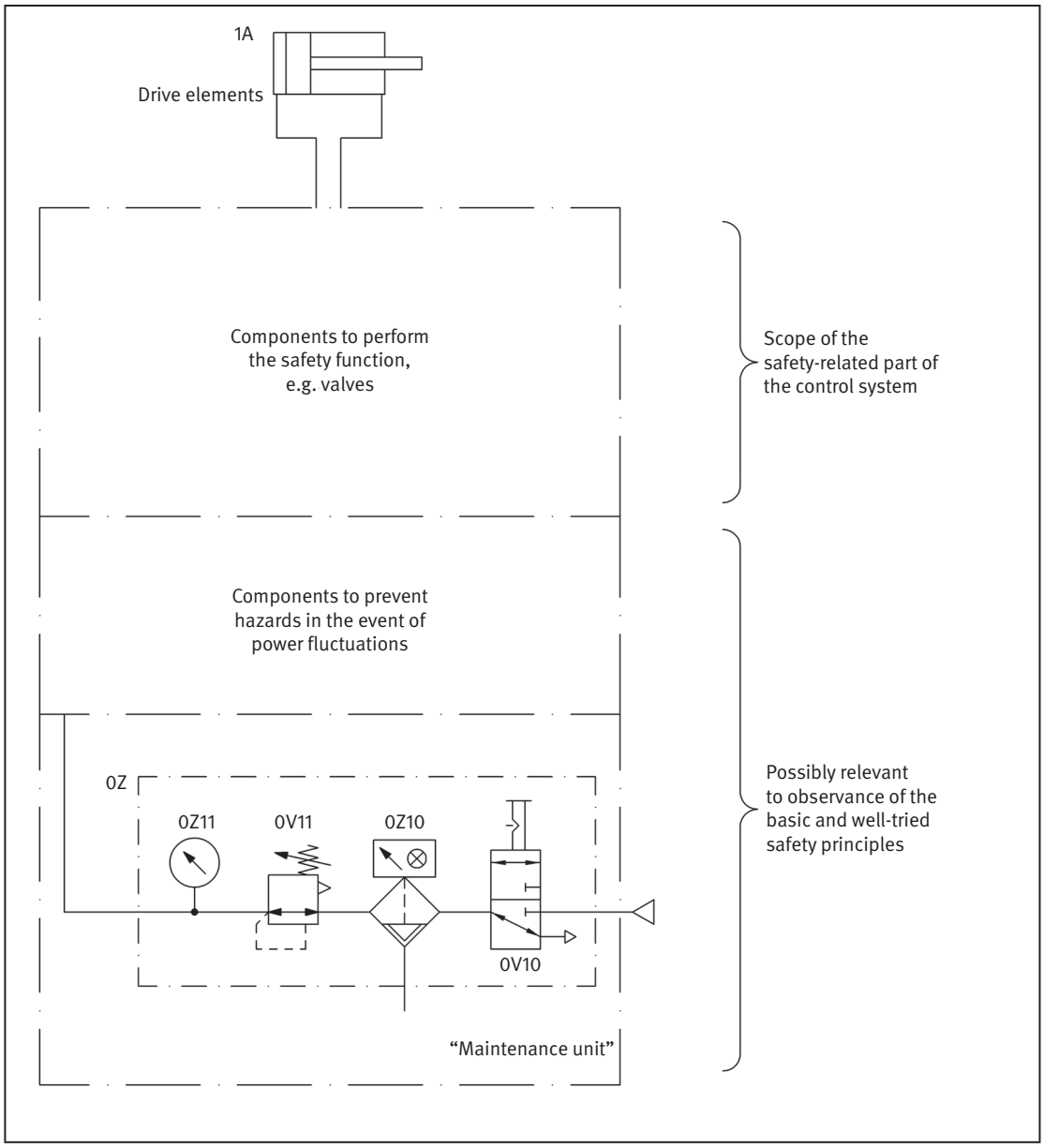


Figure 8.2: Scope of EN ISO 13849 for pneumatic systems

Besides the safety-related part of the control system, the fluid power circuits presented as examples in this chapter contain only the additional components that are required for an understanding of the fluid power system or are directly related to the control technology. The requirements that must be met by fluid power systems are described in full in [58; 59]. [60 to 63] are further relevant standards.

The majority of control system examples are electrohydraulic or electropneumatic controls. A range of safety requirements on these control systems are satisfied by the electrical part of the control system, for example the requirement for energy changes on electrohydraulic control systems to be controlled.

On the control examples described here, the required safety function is the stopping of a hazardous movement or the reversal of a direction of movement. Prevention of unexpected start-up is implicitly included. The required safety function may however also be a defined pressure level or a pressure release, for example.

The structures of most fluid power control systems are engineered in Categories 1, 3 or 4. Since Category B already requires observance of the relevant standards and of the basic safety principles, Category B and 1 fluid power control systems do not differ essentially in their control structure, but only in the higher safety-related reliability of the relevant valves. For this reason, this report does not present any Category B fluid power control systems. Further information on hydraulics and pneumatics can be found on the IFA website (www.dguv.de/ifa, Webcode: d1029520).

8.1.3 Electronic and programmable electronic control systems

Electronic components are generally more sensitive to external environmental influences than electromechanical

components. If no particular measures are taken, the use of electronic components at temperatures below 0°C is subject to substantially greater constraints compared to electromechanical components. In addition, environmental influences exist that are virtually irrelevant to electromechanical circuit elements but that present crucial problems for electronic systems, namely any electromagnetic disturbances that are coupled into electronic systems in the form of conducted disturbance or electromagnetic fields. In some cases, greater effort is required in order for adequate resistance to disturbance to be attained for industrial use. Fault exclusion is virtually impossible on electronic components. In consequence, safety cannot in principle be guaranteed by the design of a particular component, but only by certain circuit concepts and by the application of appropriate measures for the control of faults.

According to the fault lists for electrical/electronic components to EN ISO 13849-2, the faults of short circuit, open circuit, change of a parameter or a value, and stuck-at faults are essentially assumed. These are without exception fault effects that are assumed to be permanent. Transient (sporadically occurring) faults such as soft errors caused by charge reversal of a capacitor in a chip owing to high-energy particles such as alpha particles can generally be detected only with difficulty and controlled for the most part by structural measures.

The failure mode of electronic components is frequently difficult to evaluate; generally, no predominant failure mode can be defined. This can be illustrated by an example: if a relay or contactor is not actuated electrically, i.e. current does not flow through its coil, there is no reason for the contacts to close when the component is used within the constraints of its specification. In other words, a de-energized relay or contactor does not switch on of its own accord in response to an internal fault. The situation is different for the majority of electronic components, such as transistors. Even if a transistor is blocked, i.e. in the absence of a sufficiently high base current, the possibility still cannot be excluded of it suddenly becoming conductive without external influence as a result of an internal fault, and consequently under certain circumstances initiating a hazardous movement. This drawback, from a safety perspective, of electronic components must also be controlled by a suitable circuit concept. Where highly integrated modules are used, in particular, it may not be possible to demonstrate that a device or item of equipment is completely free of faults even at the beginning of its mission time, i.e. at commissioning. Even at component level, manufacturers are no longer able to demonstrate freedom from faults with 100% test coverage for complex integrated circuits. A similar situation exists for the software of programmable electronics.

In contrast to electromechanical circuits, purely electronic circuits often have the advantage that a change of state can be forced dynamically. This permits attainment of the required *DC* at appropriately short intervals and without alteration of the state of external signals (forced dynamics).

Decoupling measures are required between different channels in order to prevent common cause failures. These measures generally consist of galvanically isolated contacts, resistor or diode networks, filter circuits, optocouplers and transformers.

Systematic failures may lead to simultaneous failure of redundant processing channels if this is not prevented by timely consideration, in particular during the design and integration phase. The use of principles such as closed-circuit current, diversity or overdimensioning enables electronic circuits to be designed to be robust. Measures that render the processing channels insensitive to the physical influences encountered for example in an industrial environment should not be ignored. Such influences include temperature, moisture, dust, vibration, shock, corrosive atmospheres, electromagnetic influences, voltage breakdown, overvoltage and undervoltage.

A Category 1 SRP/CS must be designed and manufactured with the use of well-tried components and well-tried safety principles. Since complex electronic components such as PLCs, microprocessors or ASICS are not deemed well-tried in the sense of the standard, this report contains no corresponding examples of Category 1 electronics.

The circuit examples include a statement of the effectiveness, i.e. the associated Performance Level, of the required measures for fault avoidance/fault control for the programmable electronics. Further details can be found in subclause 6.3. Should ASICs be employed in a development, measures for fault avoidance are required in the development process. Such measures can be found for example in IEC 61508-2 [48], which specifies a V model for the development of an ASIC, based upon the V model familiar from software development.

The following points are worthy of mention, since such issues arise in practice:

- Generally, two channels of an SRP/CS must not be routed through the same integrated circuit. For optocouplers, this requirement means for example that they must be housed in separate enclosures when they are used to process signals from different channels.

- The influence of operating systems etc. must also be considered where programmable electronics are employed. A standard PC and typical commercial ope-

rating system is not suitable for use in a safety-related control system. The required freedom from faults (or realistically, low incidence of faults) cannot generally be demonstrated with reasonable effort, or will not be attainable, on an operating system that was not designed for safety-related applications.

8.2 Circuit examples

Table 8.1 shows an overview of circuit examples 1 to 38. Further examples can be found in [22]. Table 8.2 (Page 105) contains an alphabetical list of the main abbreviations used in the circuit examples.

Note: In the examples containing multiple safety functions (17, 19, 23, 24), only the first safety function of the example is shown in the safety-related block diagram.

Table 8.1:
Overview of the circuit examples

Attained PL	Implemented Category	Technology/example No.		
		Pneumatics	Hydraulics	Electrics
b	B			1, 4
c	1	2	3, 38	5, 6, 7
c	2			9
c	3			10, 24
d	2	11	12	13
d	3	14	15, 16	15, 16, 17, 18, 19, 20, 21, 22, 23, 24
e	3	25	27	28, 29, 30
e	4	31	32, 33	33, 34, 35, 37

Table 8.2:
Overview of the abbreviations employed in the circuit examples

Abbreviation	Full form
[D]	B_{10D} or $MTTF_D$ values from databases (refer for example to Section D.2.6)
[E]	Estimated B_{10D} or $MTTF_D$ values (see above)
[M]	B_{10D} or $MTTF_D$ values based upon manufacturers' information
[S]	B_{10D} or $MTTF_D$ values based upon data listed in EN ISO 13849-1 (refer for example to Table D.2 of this report)
µC	Microcontroller
B_{10}	Nominal lifetime: the average number of switching cycles (operations) until 10% of the considered components fail
B_{10D}	Nominal lifetime (dangerous): the average number of switching cycles (operations) until 10% of the considered components fail dangerously
CBC	Clutch/brake combination
CCF	Common cause failure
CPU	Microprocessor (central processing unit)
DC	Diagnostic coverage
DC_{avg}	Average diagnostic coverage
ESPE	Electro-sensitive protective equipment
FIT	Number of failures in 10^9 component hours (failures in time)
FMEA	Failure mode and effects analysis
FI	Frequency inverter
M	Motor
MPC	Multi-purpose control
$MTTF_D$	Mean time to dangerous failure
n_{op}	Mean annual number of operations
PFH_D	Average probability of a dangerous failure per hour
PL	Performance Level
PL_r	Required Performance Level
PLC	Programmable logic controller
RAM	Random-access memory (variable memory)
ROM	Read-only memory (invariable memory)
SBC	Safe brake control; provides an output signal to control a brake/clamping device
SDE	Safe de-energization; exhausting of part of an installation
SLS	Safely limited speed (see Table 5.2)
SRASW	Safety-related application software
SRESW	Safety-related embedded software
SRP/CS	Safety-related part of a control system
SS1-r, SS1-t	Safe stop 1 (see Table 5.2)
SS2-r, SS2-t	Safe stop 2 (see Table 5.2)
SSC	Safe stopping and closing, trapping of compressed air in the piston chambers without closed-loop position control
STO	Safe torque off (see Table 5.2)
T_{10D}	Mean time until 10% of the considered components fail dangerously
THC	Two-hand control

8.2.1 Position monitoring of movable guards by means of proximity switches – Category B – PL b (Example 1)

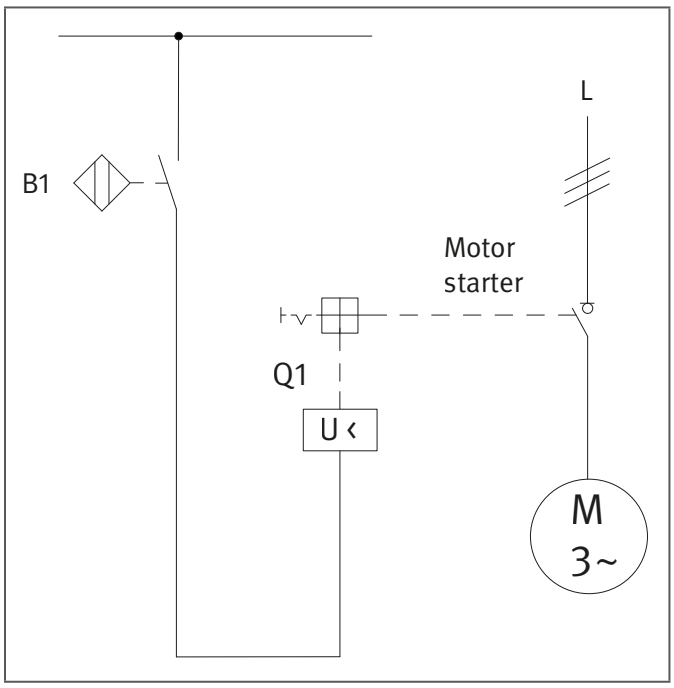


Figure 8.3:
Position monitoring of movable guards by means of proximity switches

Safety function

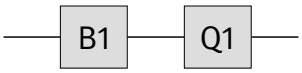
- Safety-related stop function, initiated by a safeguard: actuation of the proximity switch when the movable guard (safety guard) is opened initiates the safety function STO (safe torque off).

Functional description

- Opening of the movable guard (e.g. safety guard) is detected by a proximity switch B1 that acts upon the undervoltage release of a motor starter Q1. The dropping out of Q1 interrupts or prevents hazardous movements or states.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- Removal of the protective device is detected.
- B1 contains no internal monitoring measures. No further measures for fault detection are implemented.

Design features

- Basic safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle of the undervoltage release is employed as the basic safety principle.
- A stable arrangement of the safeguard (safety screen) is assured for actuation of the proximity switch.
- Depending upon the design of the proximity switch, bypassing of safe operation may be possible in a reasonably foreseeable manner. Bypassing can be made more difficult, for example by particular conditions for installation, such as shrouded installation (see also EN ISO 14119).
- The power supply to the entire machine is switched off (stop Category 0 to IEC 60204-1).



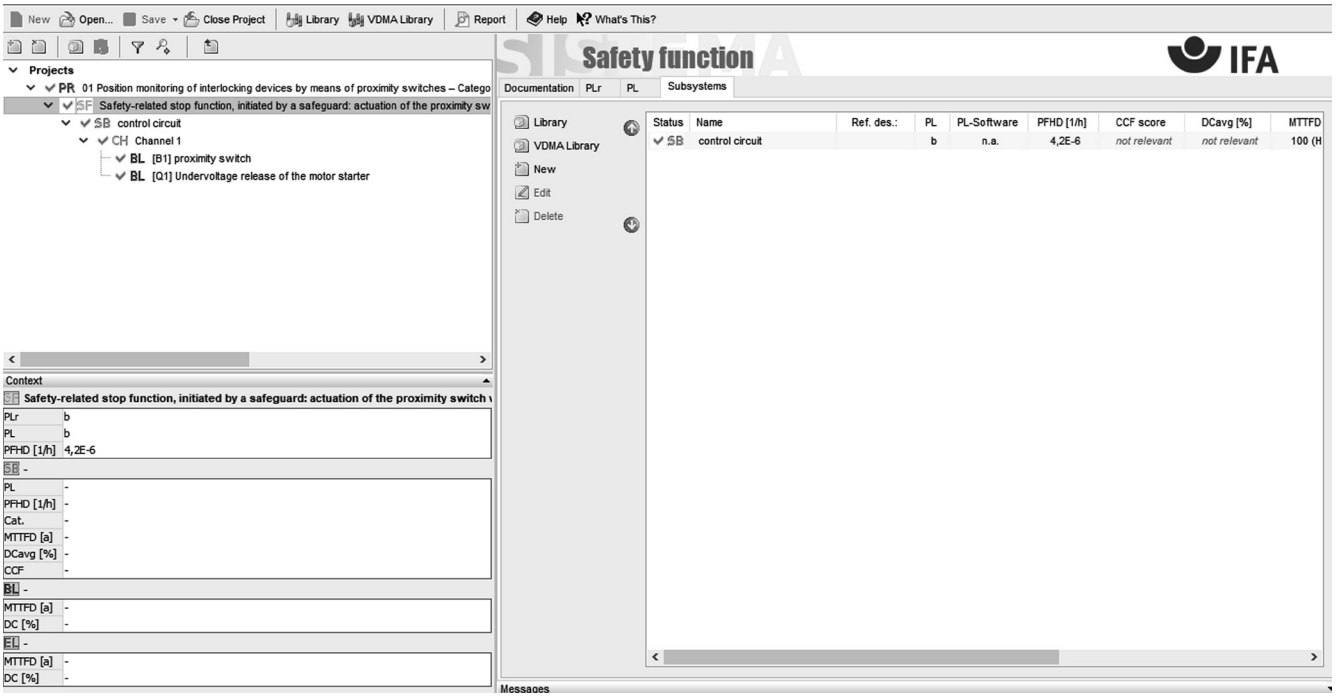
Calculation of the probability of failure

- $MTTF_D$: B1 is a conventional proximity switch on a safety screen with an $MTTF_D$ of 1,100 years [M]. For the undervoltage release of the motor starter Q1, the B_{10} value approximates to the electrical durability of 10,000 switching cycles [M]. On the assumption that 50% of failures are dangerous, the B_{10D} value is produced by doubling of the B_{10} value. Assuming actuation once daily of the proximity switch, an n_{op} of 365 cycles per year for Q1 produces an $MTTF_D$ of 548 years. For the combination of B1 and Q1, the $MTTF_D$ for each channel is 365 years. This value is capped to the arithmetical maximum value for Category B, i.e. 27 years (“medium”).
- DC_{avg} and measures against common cause failures are not relevant in Category B.
- The electromechanical control system satisfies Category B with a medium $MTTF_D$ (27 years). This results in an average probability of dangerous failure of $4.2 \cdot 10^{-6}$ per hour. This satisfies PL b.

More detailed references

- EN ISO 14119: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection (2013)
- IEC 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (2016)

Figure 8.4:
Determining of the PL by means of SISTEMA



8.2.2 Pneumatic valve (subsystem) – Category 1 – PL c (Example 2)

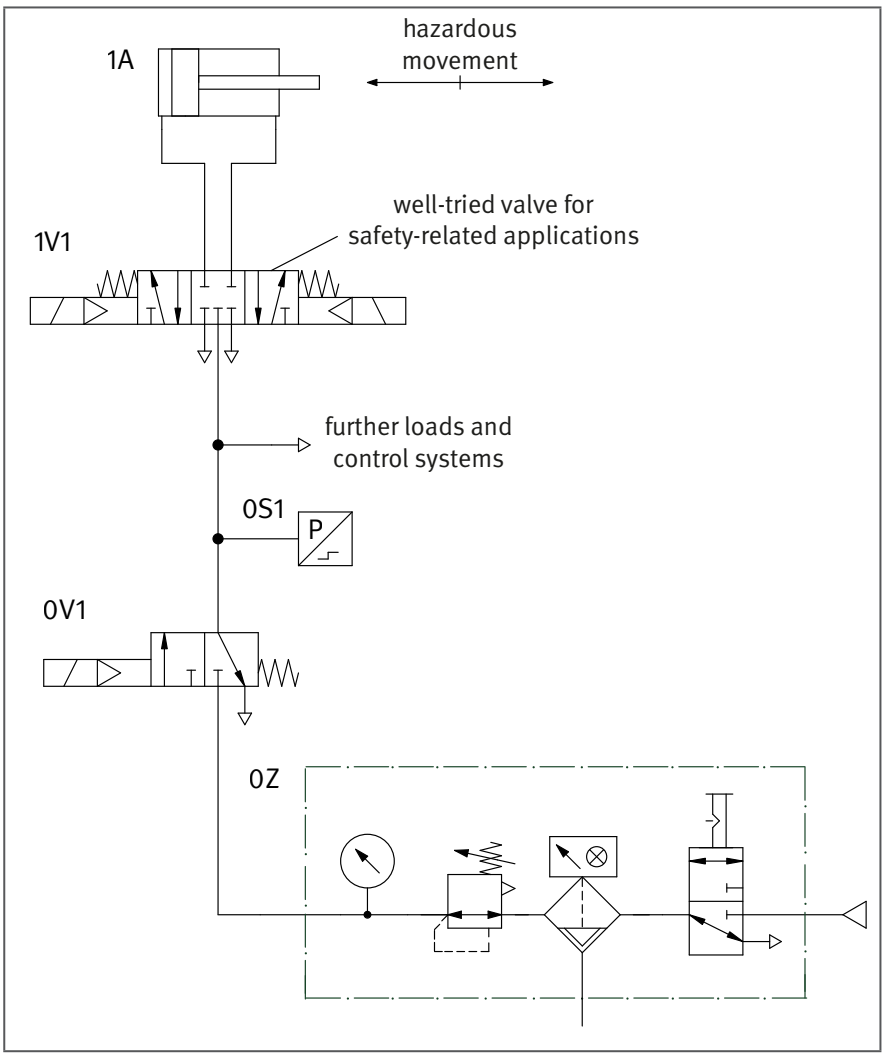


Figure 8.5:
Pneumatic valve for the control of hazardous movements

Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position, implemented by safety sub-function SSC.
- Only the pneumatic part of the control system is shown here, in the form of a subsystem. Further safety-related parts of control systems (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled by a directional control valve 1V1 that is well-tried for safety applications.
- Failure of the directional control valve may result in loss of the safety function. The failure is dependent upon the reliability of the directional control valve.
- No measures for fault detection are implemented.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.

- 1V1 is a directional control valve with closed centre position, sufficient overlap, spring-centred central position and fatigue-resistant springs.
- The safety-oriented switching position is attained by cancellation of the control signal.
- The manufacturer/user must confirm that the directional control valve is a component that is well-tried for safety applications (of sufficiently high reliability).
- The safety function can also be attained by a logical arrangement of suitable valves.

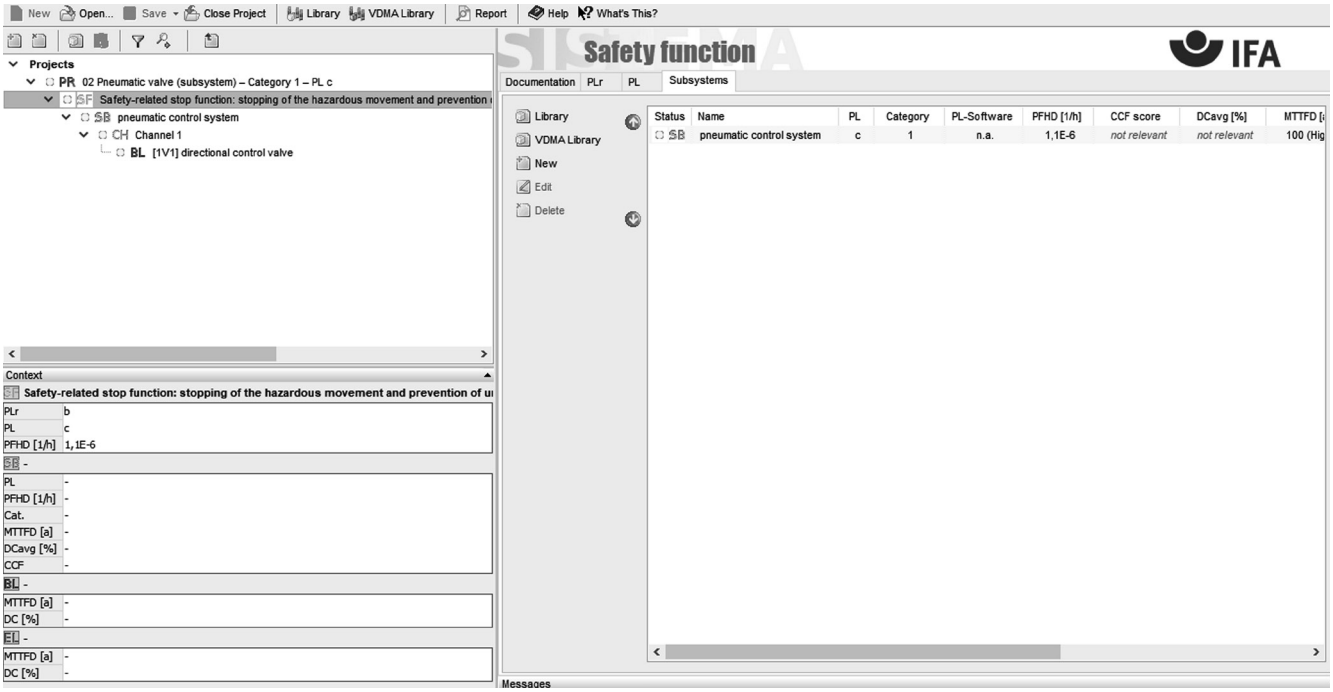
Calculation of the probability of failure

- $MTTF_D$: a B_{10D} value of 20,000,000 switching cycles [S] is assumed for the directional control valve 1V1. At 240 working days, 16 working hours and a cycle time of 10 seconds, n_{op} is 1,382,400 cycles per year and the $MTTF_D$ is 145 years. This is also the $MTTF_D$ value per channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The pneumatic control satisfies Category 1 with a high $MTTF_D$ (100 years). This results in an average probability of dangerous failure of $1.1 \cdot 10^{-6}$ per hour. This satisfies PL c. Following the addition of further safety-related parts of control systems in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower. In consideration of the estimation erring on the safe side as described above, a value of 14 years is produced for the operation time (T_{10D}) before the wearing directional control valve 1V1 must be replaced.

More detailed reference

- VDMA technical rule 24584: Safety functions of regulated and unregulated (fluid) mechanical systems (08.16)

Figure 8.6:
Determining of the PL by means of SISTEMA



8.2.3 Hydraulic valve (subsystem) – Category 1 – PL c (Example 3)

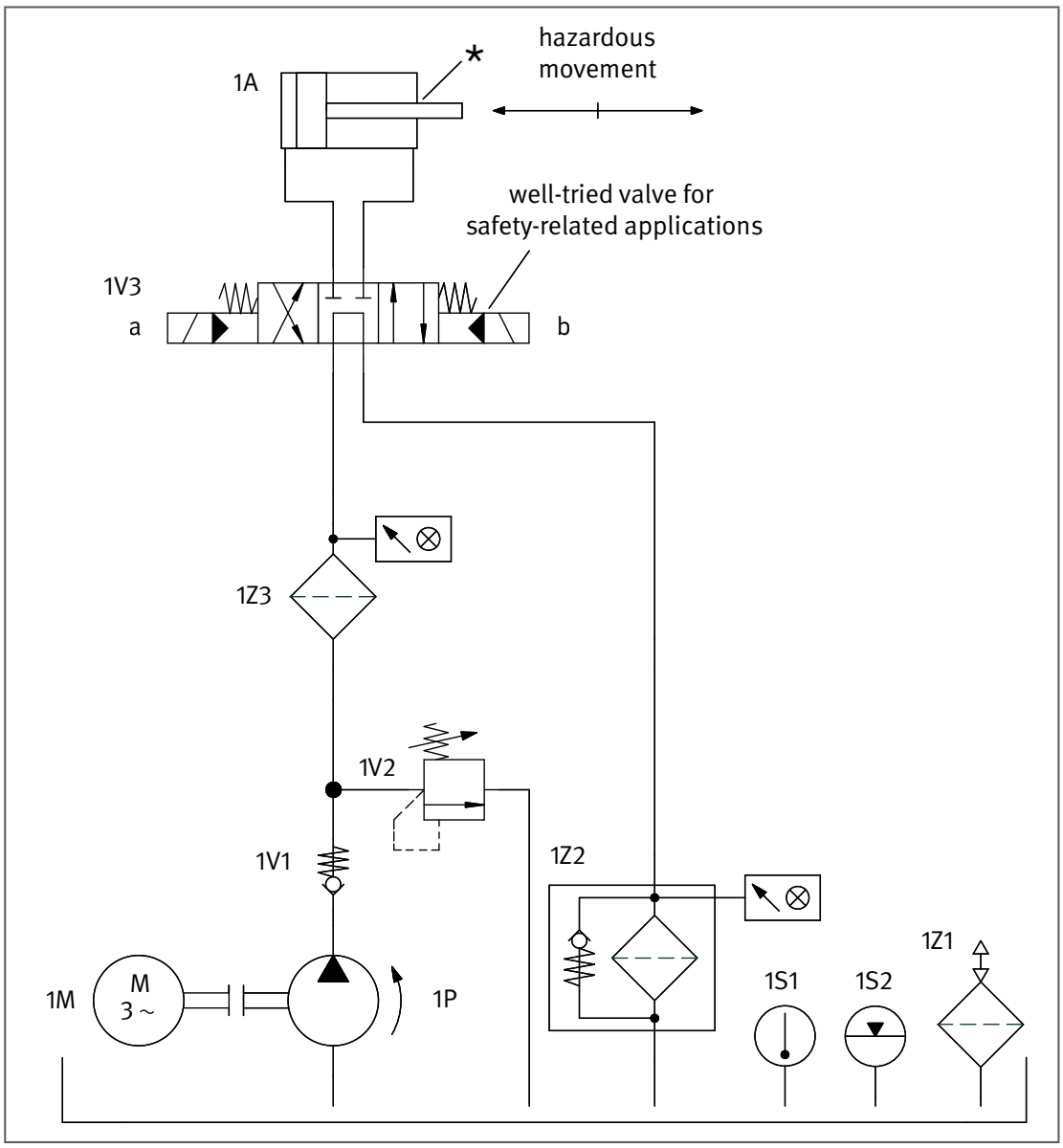


Figure 8.7: Hydraulic valve for the control of hazardous movements

Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control system is shown here, in the form of a subsystem. Further safety-related parts of control systems (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled by a directional control valve 1V3 that is well-tried for safety applications.
- Failure of the directional control valve may result in loss of the safety function. The failure is dependent upon the reliability of the directional control valve.
- No measures for fault detection are implemented.

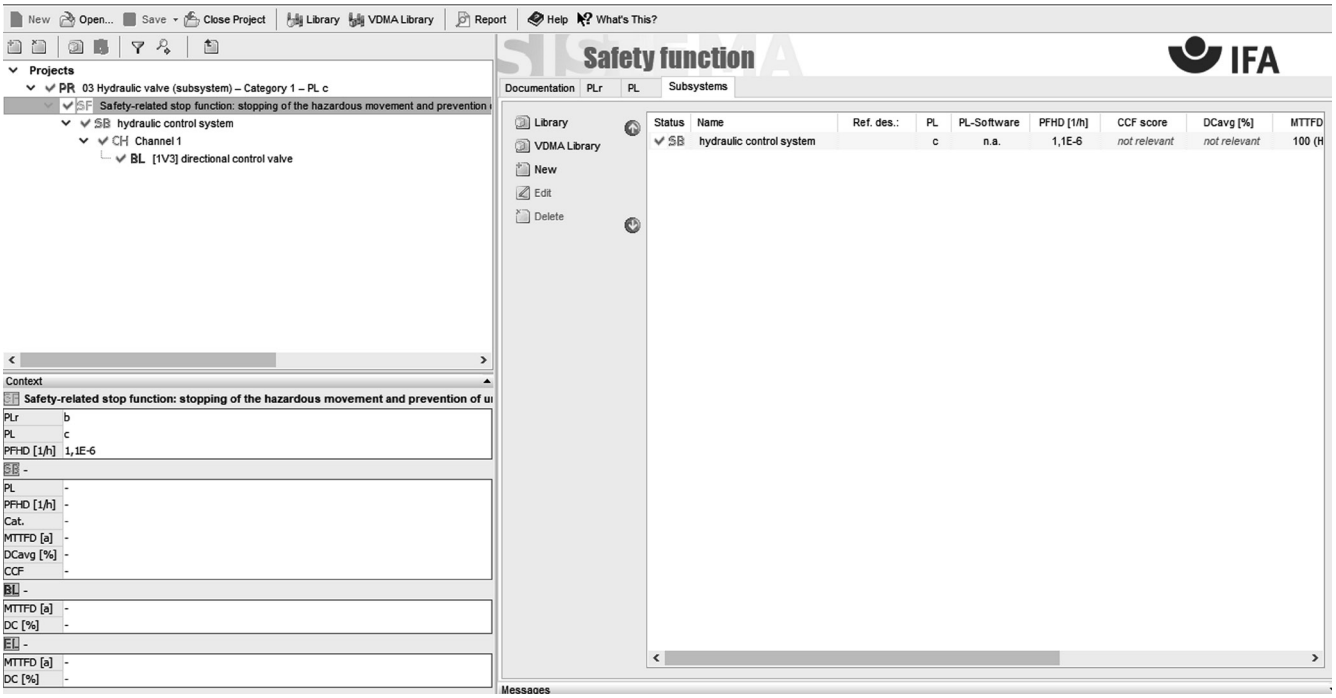
Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V3 is a directional control valve with closed centre position, sufficient overlap, spring-centred central position and fatigue-resistant springs.
- The safety-oriented switching position is attained by cancellation of the control signal.
- Where necessary, the manufacturer/user must confirm that the directional control valve is a component that is well-tried for safety applications.
- The following specific measures are implemented to increase the reliability of the directional control valve: a pressure filter 1Z3 upstream of the directional control valve, and suitable measures on the cylinder to prevent dirt from being drawn in by the piston rod (e.g. effective wiper on the piston rod, see * in Figure 8.7)

Calculation of the probability of failure

- $MTTF_D$: an $MTTF_D$ of 150 years is assumed for the directional control valve 1V3 [M]. This is also the $MTTF_D$ value per channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The hydraulic control satisfies Category 1 with a high $MTTF_D$ (100 years). This results in an average probability of dangerous failure of $1.1 \cdot 10^{-6}$ per hour. This satisfies PL c. Following the addition of further safety-related parts of the control system in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.

Figure 8.8:
Determining of the PL by means of SISTEMA



8.2.4 Stopping of woodworking machines – Category B – PL b (Example 4)

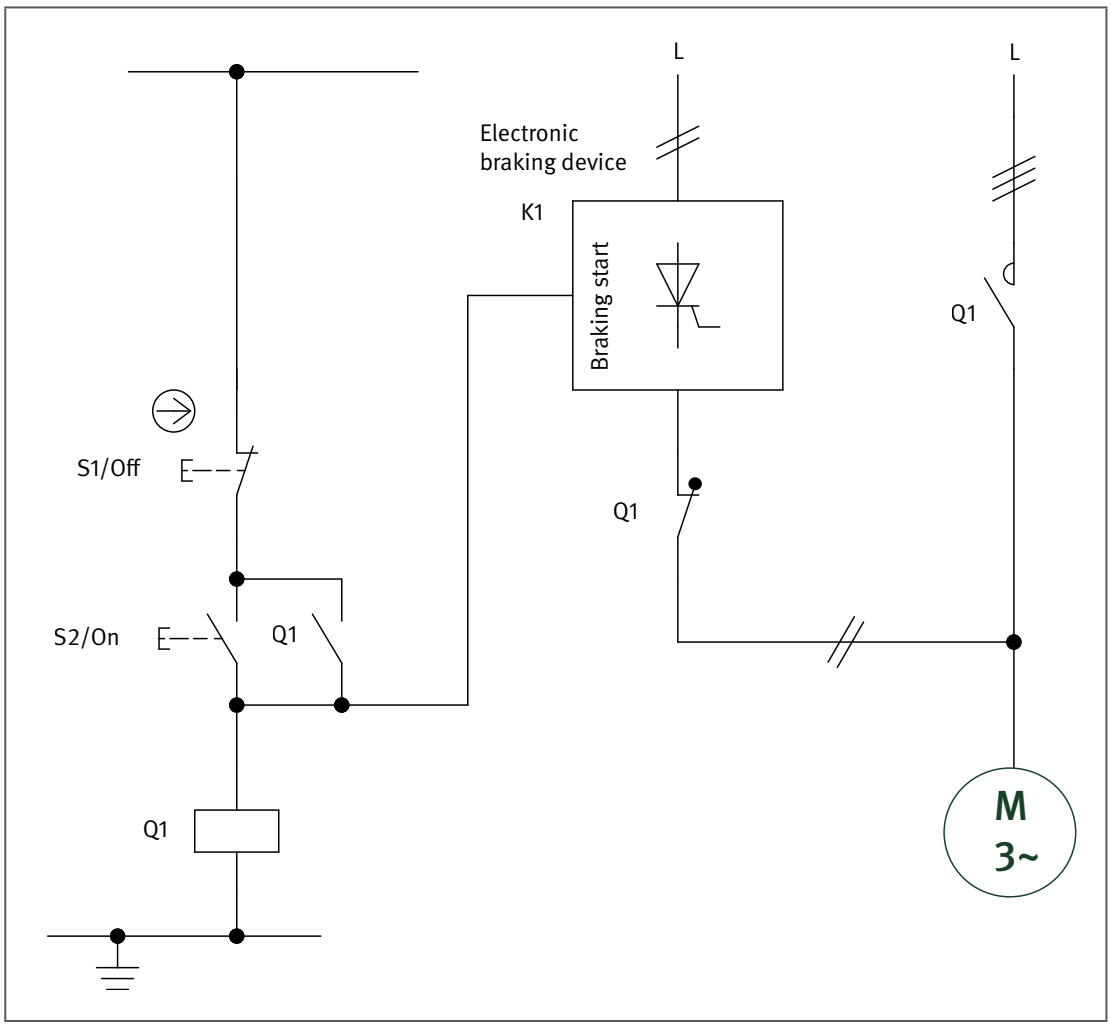


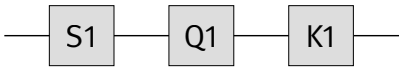
Figure 8.9: Combination of electromechanical control equipment and a simple electronic braking device for stopping of woodworking machines

Safety function

- Actuation of the Off pushbutton leads to SS1-t (safe stop 1, time controlled), a controlled stopping of the motor within a maximum permissible time.

Functional description

- Stopping of the motor is initiated by actuation of the Off button S1. The motor contactor Q1 drops out and the braking function is initiated. The motor is braked by a direct current, which is generated in the braking device K1 by a phase-angle control with thyristors, generating a braking torque in the motor winding.
- The stopping time must not exceed a maximum value (e.g. 10 seconds). The level of braking current required for this purpose can be set by means of a potentiometer on the braking device.
- After expiration of the maximum braking time, the thyristor is no longer activated and the current path for the braking current is interrupted. The stopping process corresponds to a stop of Category 1 in accordance with IEC 60204-1.
- The safety function cannot be maintained with all component failures, and dependents upon the reliability of the components.
- No measures for fault detection are implemented.



Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The de-energization principle (closed current principle) is applied as a basic safety principle. For protection against unexpected start-up after restoration of the power supply, the control system is provided with a latching.
- S1 is a pushbutton with direct opening action to IEC 60947-5-1, Annex K. S1 is therefore considered as a well-tried component.
- Contactor Q1 is a well-tried component in consideration of the additional conditions in accordance with Table D.3 of EN ISO 13849-2.
- The braking device K1 is constructed entirely from simple electronic components such as transistors, capacitors, diodes resistors and thyristors. The safety-related behaviour is determined by the selection of the components. Internal measures for fault detection are not implemented.

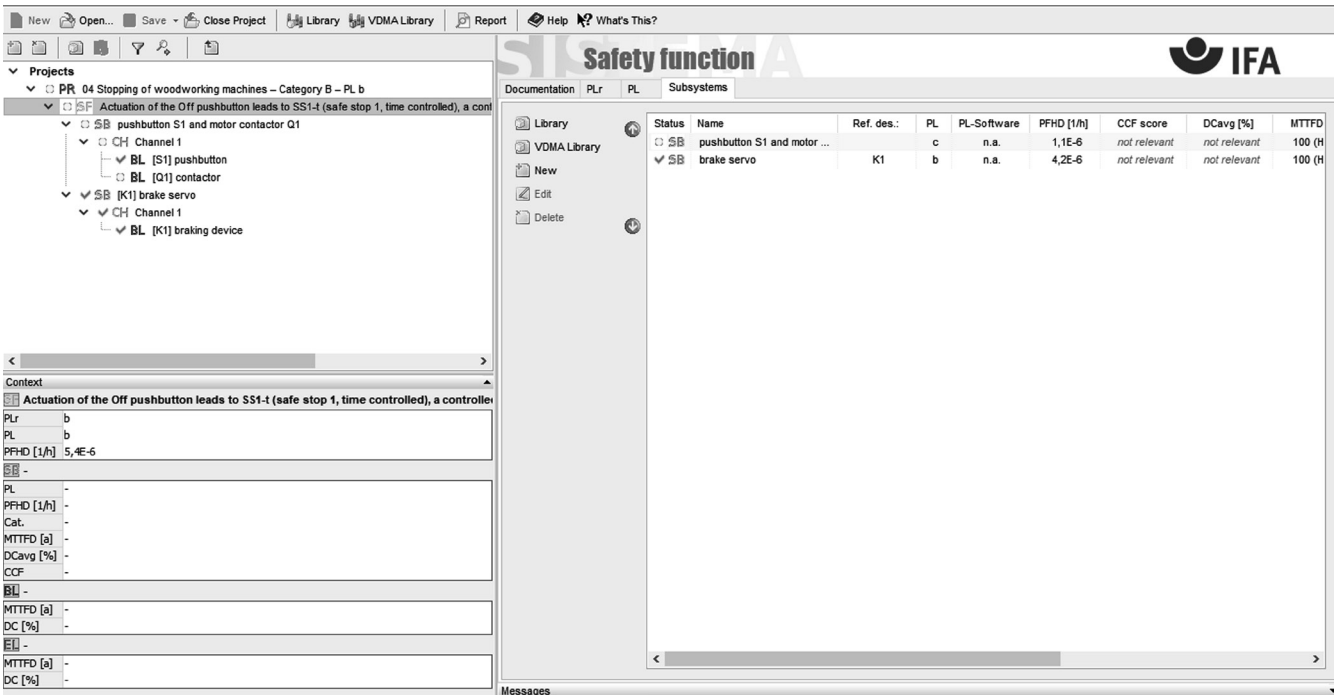
Application

- On woodworking machines or comparable machines on which unbraked stopping would result in an impermissibly long run-down of the hazardous tool movements. The control of the braking function on woodworking machines must be designed such that at least PL b is achieved (prEN ISO 19085-1:2014).

Calculation of the probability of failure

- The pushbutton S1 and the contactor Q1 are combined for the calculation in SISTEMA to a subsystem that meets the requirements of Category 1. The braking device K1 forms a separate subsystem in Category B.
- S1 is a pushbutton with direct opening action according to IEC 60947-5-1, Annex K.
- $MTTF_D$: A B_{10D} value of $20 \cdot 10^6$ switching cycles [M] is specified for the pushbutton S1. B_{10D} value of 1,300,000 switching cycles [S] at nominal load is assumed for the contactor Q1. At 300 working days, 8 working hours and a cycle time of 2 minutes, n_{op} is 72,000 cycles per year. The $MTTF_D$ is 2,777 years for the pushbutton S1 and 180 years for Q1. Together, this results to an $MTTF_D$ of 169 years, which in accordance with the standard is reduced to 100 years (“high”) for the subsystem. The contactor Q1 has a limited operation time (T_{10D}) of 18 years. Its replacement in good time is recommended. The $MTTF_D$ for the braking device K1 was determined using the parts count method. The component information from the parts list and the values from the SN 29500 database [48] yield an $MTTF_D$ of 518 years [D]. This is also reduced to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category B and Category 1.
- The subsystem S1/Q1 satisfies Category 1 with a high $MTTF_D$ (100 years). This results in an average probability of dangerous failure of $1.1 \cdot 10^{-6}$ per hour. This satisfies PL c.
- The subsystem K1 satisfies Category B with a high $MTTF_D$ (100 years). This results in an average probability of dangerous failure of $4.2 \cdot 10^{-6}$ per hour. This satisfies PL b.
- For the safety-related stop function, the resulting average probability of dangerous failure is $5.4 \cdot 10^{-6}$ per hour. This satisfies PL b.

Figure 8.10:
Determining of the PL by means of SISTEMA



8.2.5 Position monitoring of movable guards – Category 1 – PL c (Example 5)

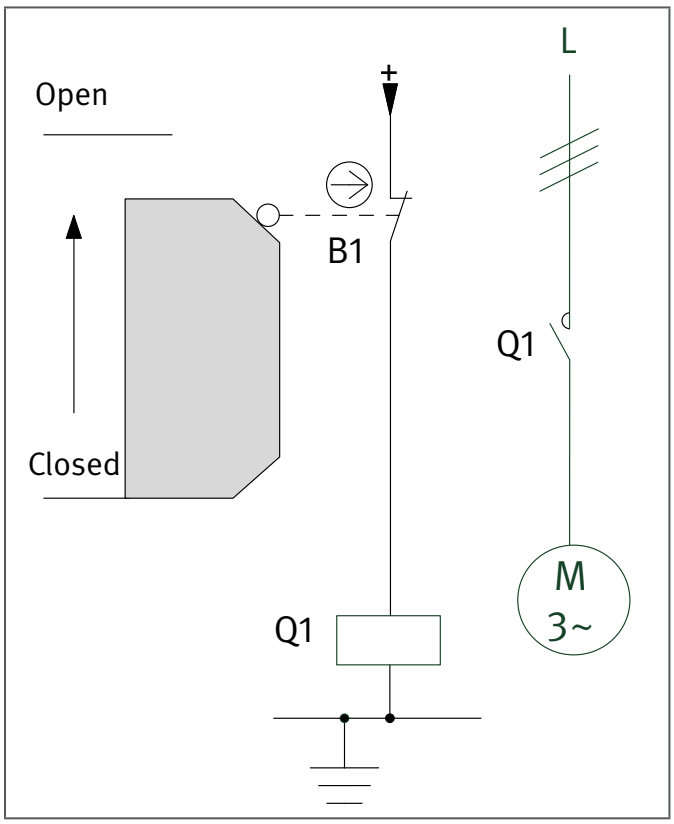


Figure 8.11:
Position monitoring of movable guard for the prevention of hazardous movements (STO – safe torque off)

Safety function

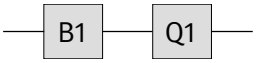
- Safety-related stop function, initiated by a guard: opening of the movable guard initiates the safety function STO (safe torque off).

Functional description

- Opening of the movable guard (e.g. safety guard) is detected by a position switch B1 with direct opening contact, which actuates a contactor Q1. The dropping out of Q1 interrupts or prevents hazardous movements or states.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.
- Removal of the protective device is not detected.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle is employed as a basic safety principle. Earthing of the control circuit is regarded as a well-tried safety principle.
- Switch B1 is a position switch with direct opening contact in accordance with IEC 60947-5-1, Annex K and is therefore regarded as a well-tried component. The break contact interrupts the circuit directly mechanically when the safeguard is not in the safe position.
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.3 of EN ISO 13849-2 are met.



- A position switch is employed for position monitoring. A stable arrangement of the safeguard is assured for actuation of the position switch. The actuating elements of the position switch are protected against displacement. Only rigid mechanical parts are employed (no spring elements acting in the direction of the actuating force).
- The actuating stroke for the position switch complies with the manufacturer‘s specification.

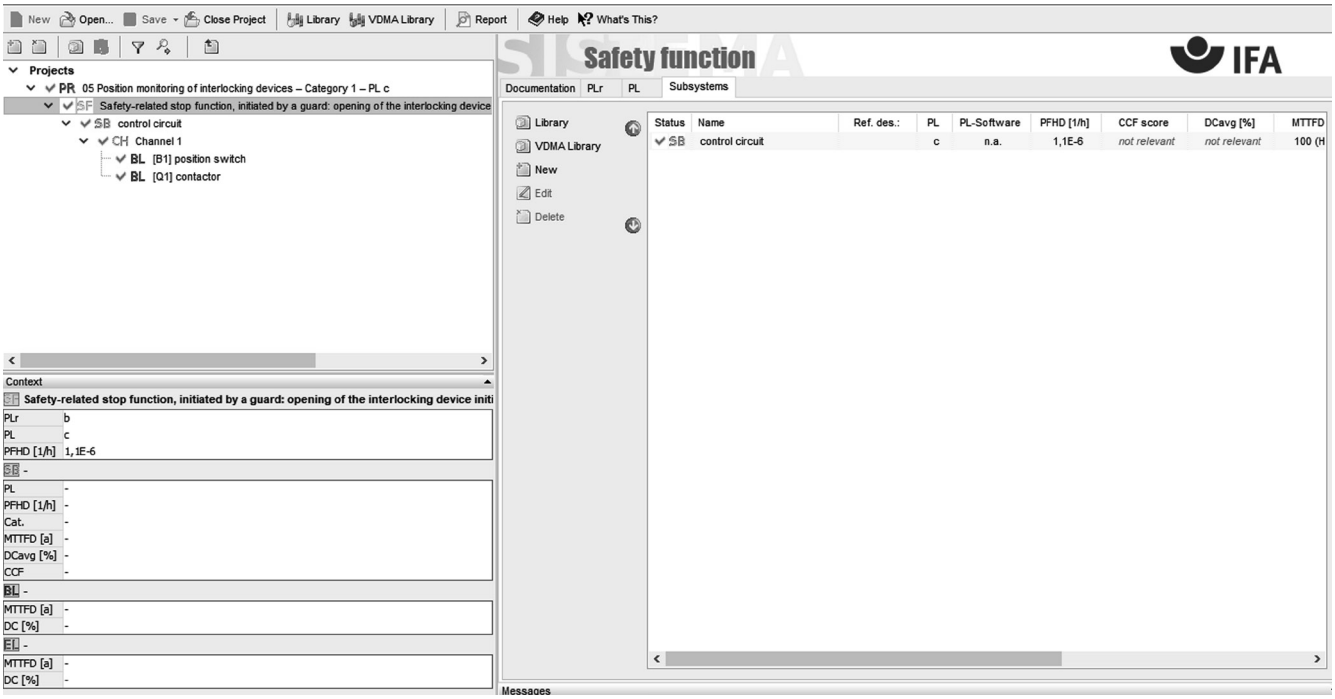
Calculation of the probability of failure

- $MTTF_D$: an $MTTF_D$ of $20 \cdot 10^6$ switching cycles [M] is stated for B1. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, the n_{op} for these components is 35,040 cycles per year, and the $MTTF_D$ is 5,707 years. For the contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical durability of 1,300,000 switching cycles [M]. If 50% of failures are assumed to be dangerous, the B_{10D} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_D$ of 742 years for Q1. The combination of B1 and Q1 results in an $MTTF_D$ of 656 years for each channel. This value is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system satisfies Category 1 with a high $MTTF_D$ (100 years). This results in an average probability of dangerous failure of $1.1 \cdot 10^{-6}$ per hour. This satisfies PL c. The PL_r of b is therefore surpassed.

More detailed reference

- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2009) + A1 (2012)

Figure 8.12:
Determining of the PL by means of SISTEMA



8.2.6 Start/stop facility with emergency stop device – Category 1 – PL c (Example 6)

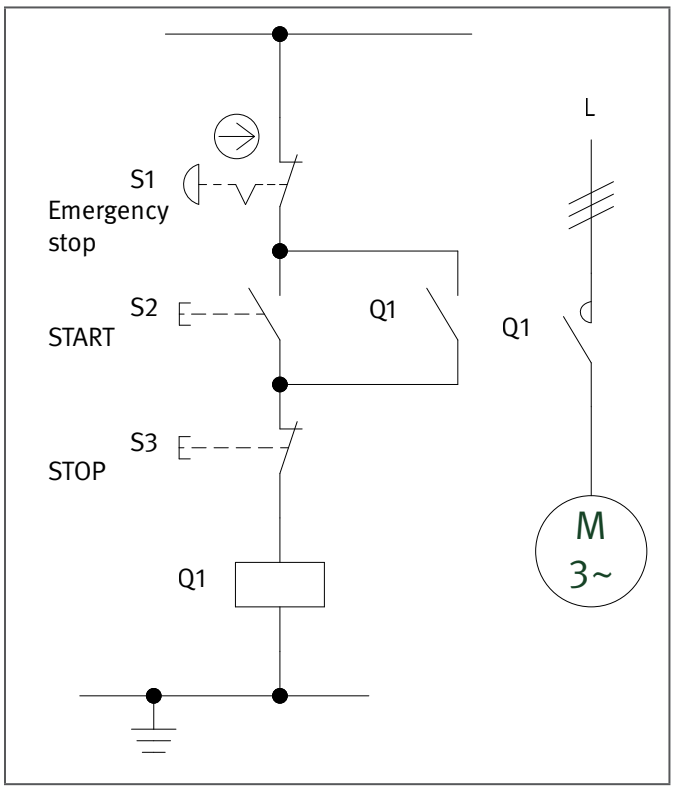


Figure 8.13:
Combined start/stop facility with emergency stop device

Safety function

- Emergency stop function, STO – safe torque off by actuation of the emergency stop device

Functional description

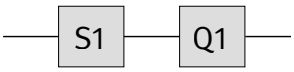
- Hazardous movements or states are de-energized by interruption of the control voltage of contactor Q1 when the emergency stop device S1 is actuated.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle is employed as a basic safety principle. The control circuit is also earthed, as a well-tried safety principle
- The emergency stop device S1 is a switch with positive mode of actuation in accordance with IEC 60947-5-5, and is therefore a well-tried component in accordance with Table D.3 of EN ISO 13849-2.
- The signal is processed by a contactor (stop Category 0 to IEC 60204-1).
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.3 of EN ISO 13849-2 are observed.

Remarks

- The function for stopping in an emergency is a protective measure that complements the safety functions for the safeguarding of hazard zones.



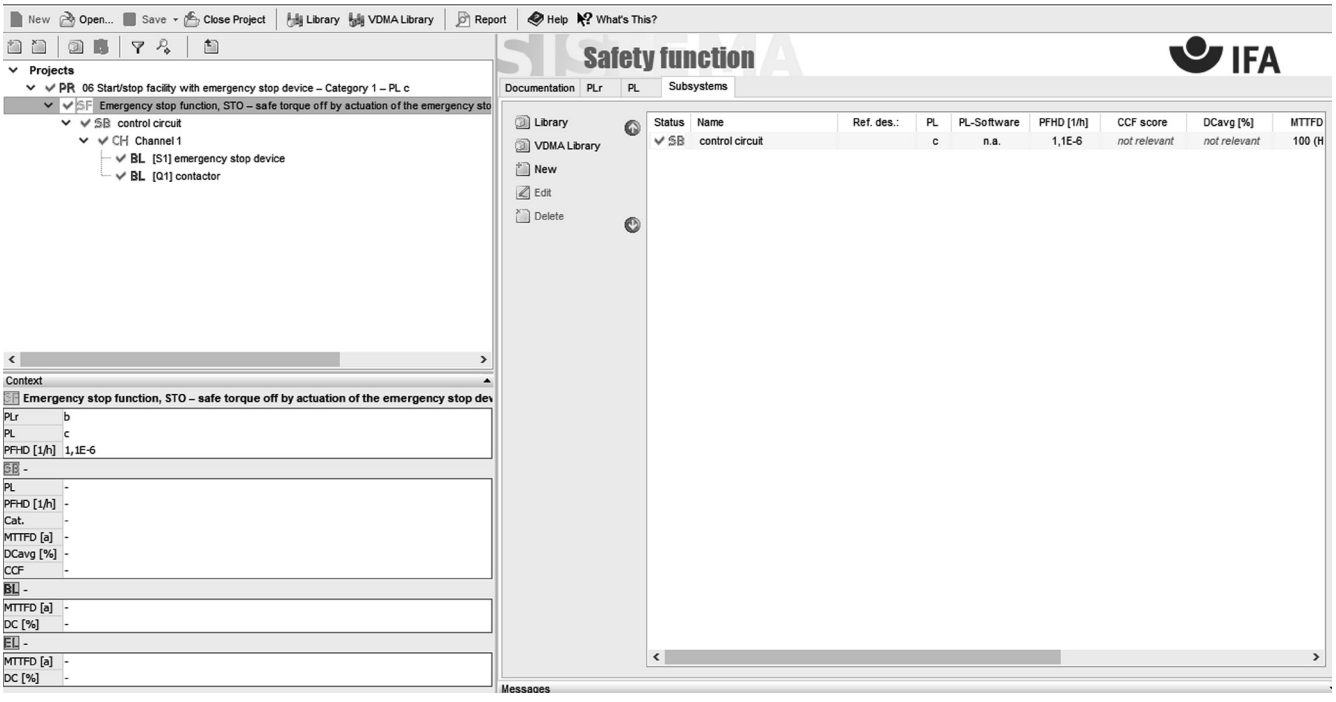
Calculation of the probability of failure

- $MTTF_D$: S1 is a standard emergency stop device according to EN ISO 13850. It is manufactured in accordance with IEC 60947-5-5. In accordance with EN ISO 13849-1, Table C.1, a B_{10D} value of 100,000 switching cycles may be applied in this case for emergency stop devices, irrespective of the load [S]. For the contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical durability of 1,300,000 switching cycles [M]. On the assumption that 50% of failures are dangerous, the B_{10D} value is produced by doubling of the B_{10} value. If the start/stop facility is assumed to be actuated twice a day on 365 working days and the emergency stop device to be actuated twelve times a year, then at a resulting n_{op} of 742 cycles per year, Q1 has an $MTTF_D$ of 35,040 years. This is also the $MTTF_D$ for the channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system satisfies Category 1 with a high $MTTF_D$ (100 years). This results in an average probability of dangerous failure of $1.1 \cdot 10^{-6}$ per hour. This satisfies PL c.

More detailed references

- EN ISO 13850: Safety of machinery – Emergency stop – Principles for design (2015).
- IEC 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (2016).

Figure 8.14:
Determining of the PL by means of SISTEMA



8.2.7 Undervoltage release by means of an emergency stop device – Category 1 – PL c (Example 7)

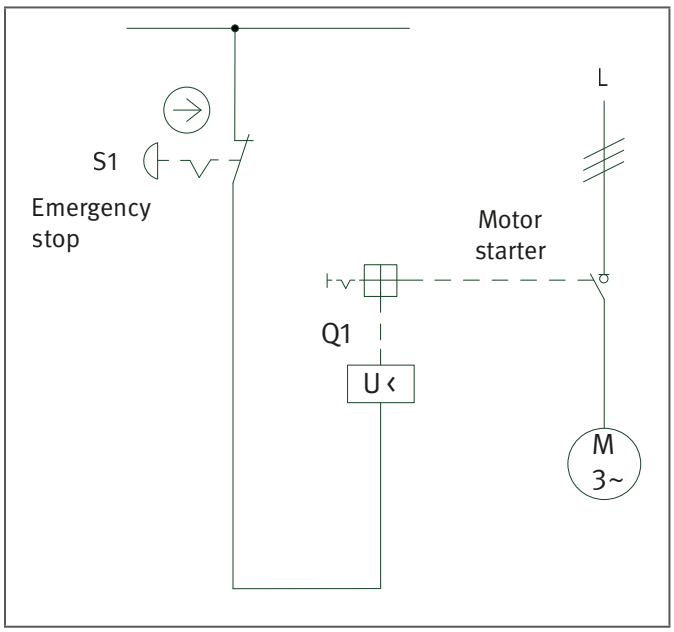


Figure 8.15:
Emergency stop device acting upon the undervoltage release of the supply disconnecting device (motor starter)

Safety function

- Emergency stop function, STO (safe torque off) by actuation of the emergency stop device acting upon the undervoltage release of a motor starter, where appropriate the supply disconnecting device.

Functional description

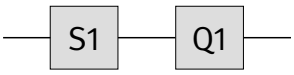
- Hazardous movements or states are interrupted upon actuation of the emergency stop device S1 by undervoltage release of the supply disconnecting device, in this case in the form of a motor starter Q1.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle of the undervoltage release is employed as the basic safety principle.
- The emergency stop device S1 is a switch with positive mode of actuation in accordance with IEC 60947-5-5, and is therefore a well-tried component in accordance with Table D.3 of EN ISO 13849-2.
- The motor starter Q1 is to be considered equivalent to a circuit breaker in accordance with Table D.3 of EN ISO 13849-2. Q1 may therefore be regarded as a well-tried component.
- The power supply to the entire machine is switched off (stop Category 0 to IEC 60204-1).

Remarks

- The function for stopping in an emergency is a protective measure that complements the safety functions for the safeguarding of hazard zones.



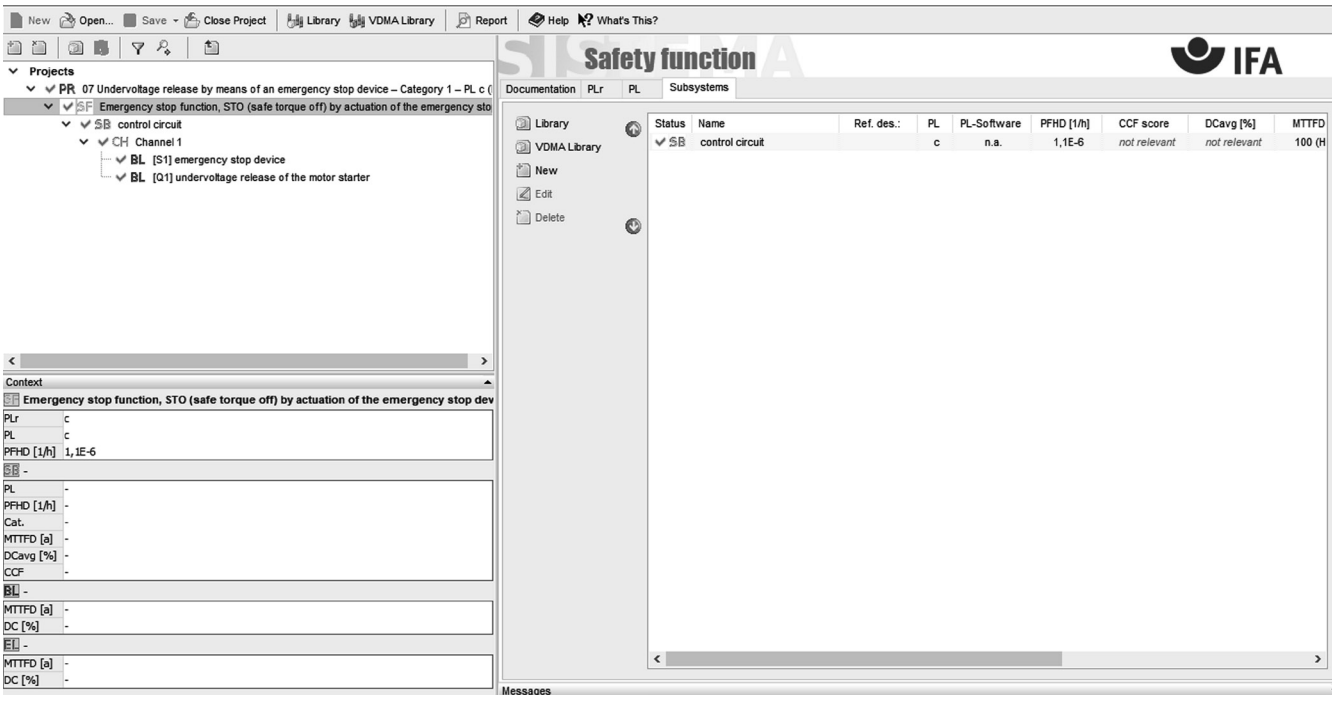
Calculation of the probability of failure

- $MTTF_D$: S1 is a standard emergency stop device according to EN ISO 13850. It is manufactured in accordance with IEC 60947-5-5. In accordance with EN ISO 13849-1, Table C.1, a B_{10D} value of 100,000 switching cycles may be applied in this case for emergency stop devices, irrespective of the load [S]. For the undervoltage release of the motor starter Q1, the B_{10} value approximates to the electrical durability of 10,000 switching cycles [M]. On the assumption that 50% of failures are dangerous, the B_{10D} value is produced by doubling of the B_{10} value. At actuation of the emergency stop device twelve times a year and a resulting n_{op} of 12 cycles per year, Q1 has an $MTTF_D$ of 16,666 years. This is also the $MTTF_D$ for the channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system satisfies Category 1 with a high $MTTF_D$ (100 years). This results in an average probability of dangerous failure of $1.1 \cdot 10^{-6}$ per hour. This satisfies PL c.

More detailed references

- EN ISO 13850: Safety of machinery – Emergency stop – Principles for design (2015).
- IEC 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (2016)

Figure 8.16:
Determining of the PL by means of SISTEMA



8.2.8 Stopping of woodworking machines – Category 1 – PL c (Example 8)

This example has been deleted, since the technology is no longer relevant.

8.2.9 Tested light barriers – Category 2 – PL c with downstream Category 1 output signal switching device (Example 9)

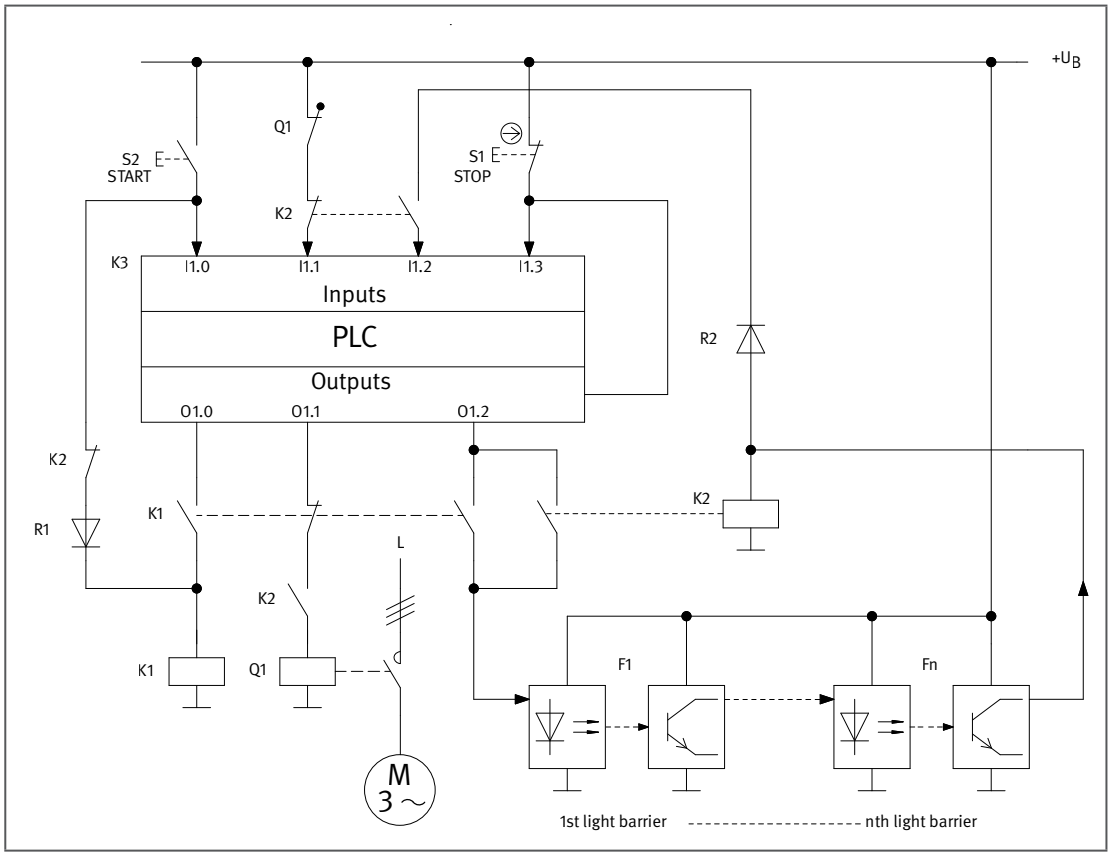


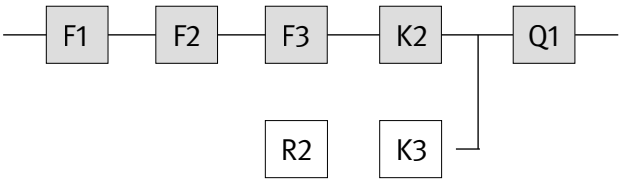
Figure 8.17: Testing of light barriers with a standard PLC

Safety function

- Safety-related stop function, initiated by a protective device: when the light beam is interrupted, a hazardous movement is halted (STO – safe torque off).

Functional description

- Interruption of a light beam of the n cascaded light barriers F1 to Fn triggers a de-energization command both by relays, by de-energization of the contactor relay K2, and via the PLC output (O1.1) of the test channel. The hazardous movement is then halted by means of the main contactor relay Q1.
- The light barriers are tested before each start of the hazardous movement following pressing of the start button S2. For this purpose, the PLC output O1.2 de-energizes the light barrier transmitter in response to a software command. The reaction of the receiver (K2 drops out again) is monitored on the PLC inputs I1.1 and I1.2. Provided the behaviour is free of faults, K2 locks in via O1.2, and the hazardous movement can be initiated by the releasing of S2. K1 is de-energized via O1.0, and the main contactor relay Q1 actuated via O1.1.
- Should a fault in one of the light barriers or in K2 be detected by the test, the outputs O1.1 and O1.2 are deactivated, and an actuating signal is no longer applied to the main contactor relay Q1.
- In the event of global failure of the PLC (output O1.0 at low potential, outputs O1.1 and O1.2 at high potential), interruption of a light beam results in de-energization of K2, independently of the PLC. In order to ensure this independence, the light barrier outputs are decoupled from the PLC by the decoupling diode R2. Under unfavourable circumstances, the light barriers can be re-activated by K2 by actuation of the start button, and the main contactor relay Q1 thus actuated. In this case, (only) the test equipment would have failed. Failure of the test equipment is detected owing to the probability of a functionally defective process under these circumstances.
- During the test, actuation of Q1 by K1 and O1.1 is blocked.



Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Special light barriers with suitable optical characteristics (aperture angle, extraneous light immunity, etc.) to IEC 61496-2 are employed.
- Several light barriers can be cascaded and monitored by only two PLC inputs and a relay or contactor relay.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L. The main contactor relay Q1 possesses a mirror contact in accordance with IEC 60947-4-1, Annex F.
- The standard components F1 to Fn and K3 are employed in accordance with the guidance in subclause 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (reduction of the requirements in the test channel owing to diversity) and the guidance in subclause 6.3.10.
- The start button S2 must be located outside the hazard zone and at a point from which the hazard zone is visible.
- The number, arrangement and height of the light beams must comply with EN ISO 13855 and IEC 62046.
- Should an arrangement for the safeguarding of hazard zones permit stepping behind the sensing field, further measures are required, such as a restart interlock. The start button S2 can be used for this purpose. To this end, the PLC K3 compares the duration for which the button is pressed with maximum and minimum values. Only if the conditions are met is a start command deemed valid.

Remarks

- The example is intended for use in applications with an infrequent demand of the safety function. This enables the requirement for the designated architecture for Category 2 to be satisfied, i.e. “testing much more frequent than the demand of the safety function” (cf. Annex G).
- Following triggering of a stop, the light barriers remain deactivated until the next start. This enables a hazard zone for example to be entered without this being “registered” by the circuit. The behaviour can be modified by corresponding adaptation of the circuit.

Calculation of the probability of failure

- By way of example, three light barriers F1 to F3 are considered for calculation of the probability of failure. Safeguarding of a second hazard zone constitutes a further safety function for which calculation is performed separately.
- For calculation of the probability of failure, the overall system is divided into two subsystems, “light barriers” and “main contactor relay” (Q1).

For the “light barriers” subsystem:

- F1, F2, F3 and K2 constitute the functional path of the Category 2 circuit structure; the PLC K3 (including decoupling diode R2) constitutes the test equipment. S2 and K1 have the function of activating testing of the light barrier, and are not involved in the calculation of the probability of failure.
- $MTTF_D$: an $MTTF_D$ of 100 years [E] is assumed for each of F1 to F3. The B_{10D} value for K2 is 20,000,000 cycles [S]. At 240 working days, 16 working hours and a cycle time of 180 seconds, n_{op} is 76,800 cycles per year. Testing as described above doubles this value, to an n_{op} of 153,600 cycles per year with an $MTTF_D$ of 1,302 years for K2.

These values yield an $MTTF_D$ of 32 years ("high") for the functional channel. An $MTTF_D$ of 50 years [E] is assumed for K3. Compared to this value, the $MTTF_D$ value of 228,311 years [S] for the decoupling diode R2 is irrelevant.

- DC_{avg}: the reasoning for the *DC* of 60% for F1 to F3 is the functional test as described. The *DC* of 99% for K2 is derived from direct monitoring in K3 with the aid of mechanically linked contact elements. The averaging formula returns a result of 61% ("low") for DC_{avg}.
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements in the "light barriers" subsystem satisfies Category 2 with a high $MTTF_D$ of the functional channel (32 years) and low DC_{avg} (61%). This results in an average probability of dangerous failure PFH_D of $1.9 \cdot 10^{-6}$ per hour.

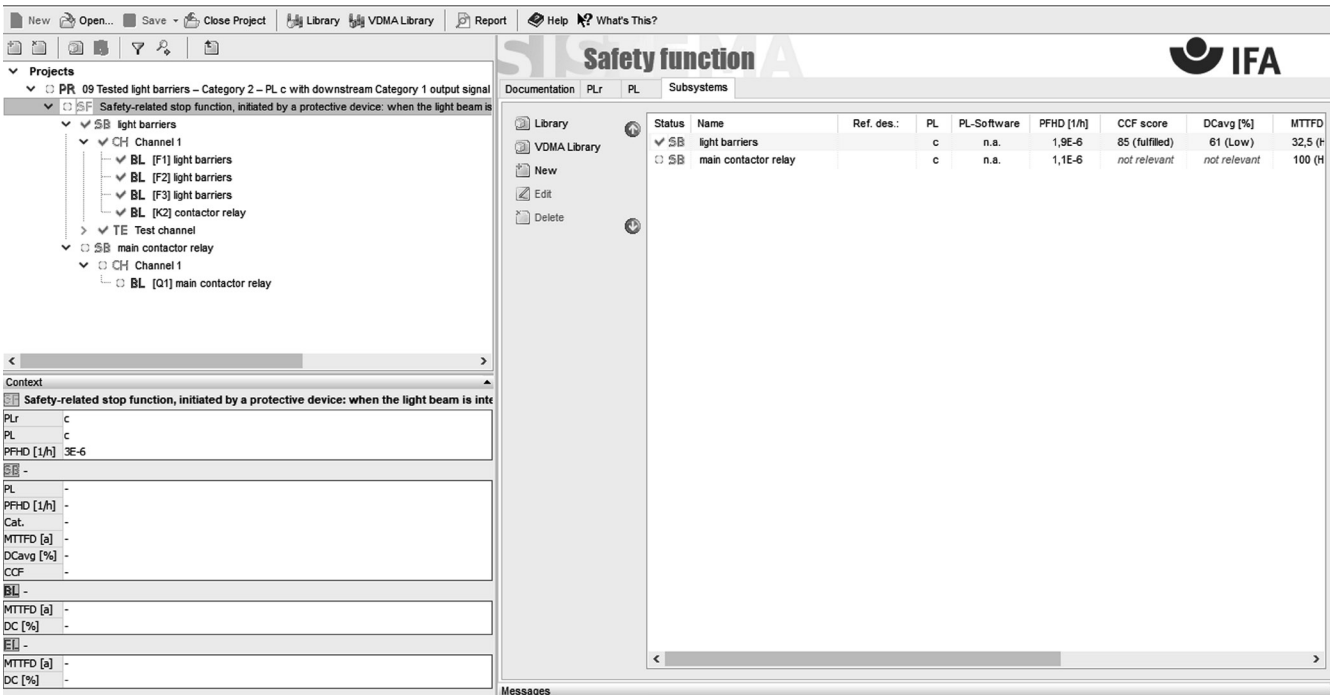
The following assumptions are made for the "main contactor relay" subsystem:

- B_{10D} = 1,300,000 cycles [S] with an n_{op} of 76,800 cycles per year. This leads to an $MTTF_D$ of 169 years, which in accordance with the standard is capped to 100 years. The structure satisfies Category 1; DC_{avg} and common cause failures are not therefore relevant. The resulting average probability of dangerous failure is $1.1 \cdot 10^{-6}$ per hour.
- Addition of the average probabilities of dangerous failure of the two subsystems results in a PFH_D of $3.0 \cdot 10^{-6}$ per hour. This satisfies PL c.
- If it is anticipated that a demand will be made upon the safety function more frequently than assumed for the Category 2 designated architecture (the ratio is lower than 100:1, i.e. more frequently than once every 5 hours), this can be allowed for accordance with Annex K, Note 1 of the standard by an additional penalty of 10% down to a ratio of 25:1. In the case with three light barriers under consideration here, the "light barriers" subsystem still attains a PFH_D of $2.1 \cdot 10^{-6}$ per hour. The average probability of dangerous failure PFH_D of $3.2 \cdot 10^{-6}$ per hour only attains PL b, however. For PL c to be attained, the number of light barriers would for example have to be reduced, or components with a higher $MTTF_D$ employed.
- In consideration of the estimation erring on the safe side as described above, an operation time (T_{10D}) of 17 years is produced for specified replacement of the wearing component Q1.

More detailed references

- IEC 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (2012) and Corrigendum 1 (2015). IEC, Geneva, Switzerland 2012/2015
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (2013). IEC, Geneva, Switzerland 2013
- IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons (2018). IEC, Geneva, Switzerland 2018
- EN ISO 13855: Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body (2010).

Figure 8.18:
Determining of the PL by means of SISTEMA

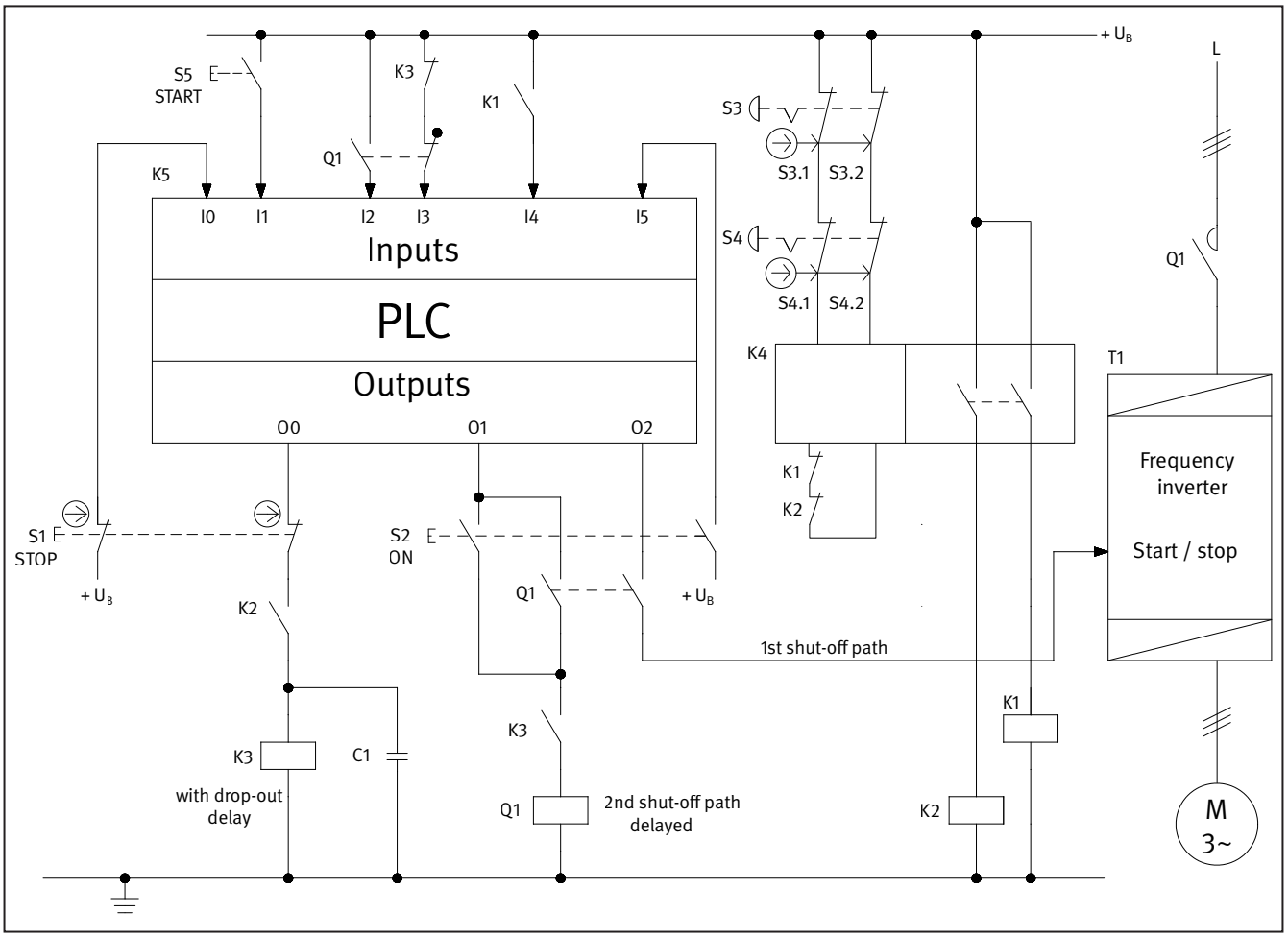


8.2.10 Tested light barriers – Category 2 – PL c with downstream Category 1 output signal switching device (Example 10)

Changes with respect to the second edition (BGIA Report 2/2008e):

The safety function was redefined and the associated safety-related block diagram adapted. The former block S3/S4 was changed to S3. PL and PFH_D values for PLC and contactors were replaced by manufacturers' values.

Figure 8.19:
Stopping of a PLC-driven frequency inverter drive following an emergency stop command

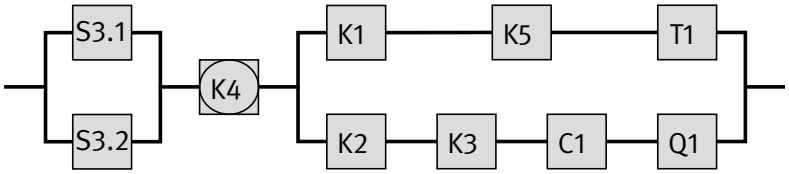


Safety function

- Actuation of the emergency-stop device S3 causes the drive to be stopped in a controlled manner (SS1-t – safe stop 1 with STO following expiry of a deceleration time).

Functional description

- The hazardous movement is stopped if either the stop button S1 or one of the emergency stop devices S3 or S4 is actuated. Only actuation by means of the emergency-stop device S3 is considered in this example. The drive is halted in an emergency in response to actuation of S3: first by deactivation of the emergency stop safety module K4, accompanied by shut-off of the contactor relays K1 and K2. Opening of the make contact K1 on the input I4 of the PLC K5 causes the starting signal on the frequency inverter (FI) T1 to be cancelled via the PLC output O2. Redundantly to the K1-K5-T1 chain, opening of the make contact K2 upstream of the contactor relay with drop-out delay K3



initiates a braking timer; upon timeout of the braking timer, the actuating signal for the mains contactor Q1 is interrupted. The timer setting is selected such that under unfavourable operating conditions, the machine movement is halted before the mains contactor Q1 has dropped out.

- Functional stopping of the drive following a stop command is initiated by opening of the two break contacts of the stop button S1. As with stopping in an emergency, the status is first queried by the PLC K5 via the input I0, and the FI is shut down by resetting of the PLC output O2. Redundantly to this process, the contactor relay K3 is shut-off – with drop-out delay provided by the capacitor C1 – and following timeout of the set braking time, the activation signal to the mains contactor Q1 is interrupted.
- In the event of failure of the PLC K5, the frequency inverter T1, the mains contactor Q1, the contactor relays K1/K2 or the contactor relay with drop-out delay K3, stopping of the drive is nevertheless assured, since two shut-off paths independent of each other are always present. Failure of the contactor relays K1 and K2 to drop out is detected – at the latest following resetting of the actuated emergency stop device – by monitoring of the mechanically linked break contacts within the emergency stop safety module K4. Failure of the contactor relay K3 to drop out is detected – at the latest before renewed start-up of the machine movement – through feedback of the mechanically linked break contact to the PLC input I3. Failure of the mains contactor Q1 to drop out is detected by the mirror contact read in on the PLC input I3. Welding of this mirror contact is detected by the mechanically linked auxiliary make contact on the PLC input I2. In the event of a fault in the capacitor C1, the measured drop-out time of the contactor relay K3 differs from the time specified in the PLC. The fault is detected and leads to the machine being shut down and to operating inhibition of the machine. Organizational measures ensure that each emergency-stop device is actuated at least once a year.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The contactor relays K1, K2 and K3 possess mechanically linked contacts in accordance with IEC 60947-5-1, Annex L.
- The pushbuttons S1, S3 and S4 possess direct opening contacts in accordance with IEC 60947-5-1, Annex K.
- The contactor Q1 possesses a mirror contact in accordance with IEC 60947-4-1, Annex F.
- The standard components K5 and T1 are employed in accordance with the guidance in subclause 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the guidance in subclause 6.3.10.
- Delayed attainment of standstill by the second shut-off path alone in the event of a fault must not involve an unacceptably high residual risk.
- The SRP/CS of the emergency stop safety module K4 satisfies all requirements for Category 3 and PL d.

Calculation of the probability of failure

Only the probability of failure of the emergency stop function is calculated.

- The emergency-stop device S3 is equipped with two break contacts S3.1 and S3.2. The manufacturer states a B_{10D} of 127,500 cycles for each of the blocks S3.1 and S3.2. With actuation annually and a resulting n_{op} of 1 cycle per year, the $MTTF_D$ of each contact is 1,275,000 years. The emergency stop safety module K4 is a tested safety component. Its probability of failure is $3.0 \cdot 10^{-7}$ per hour [M], and is added at the end of the calculation.

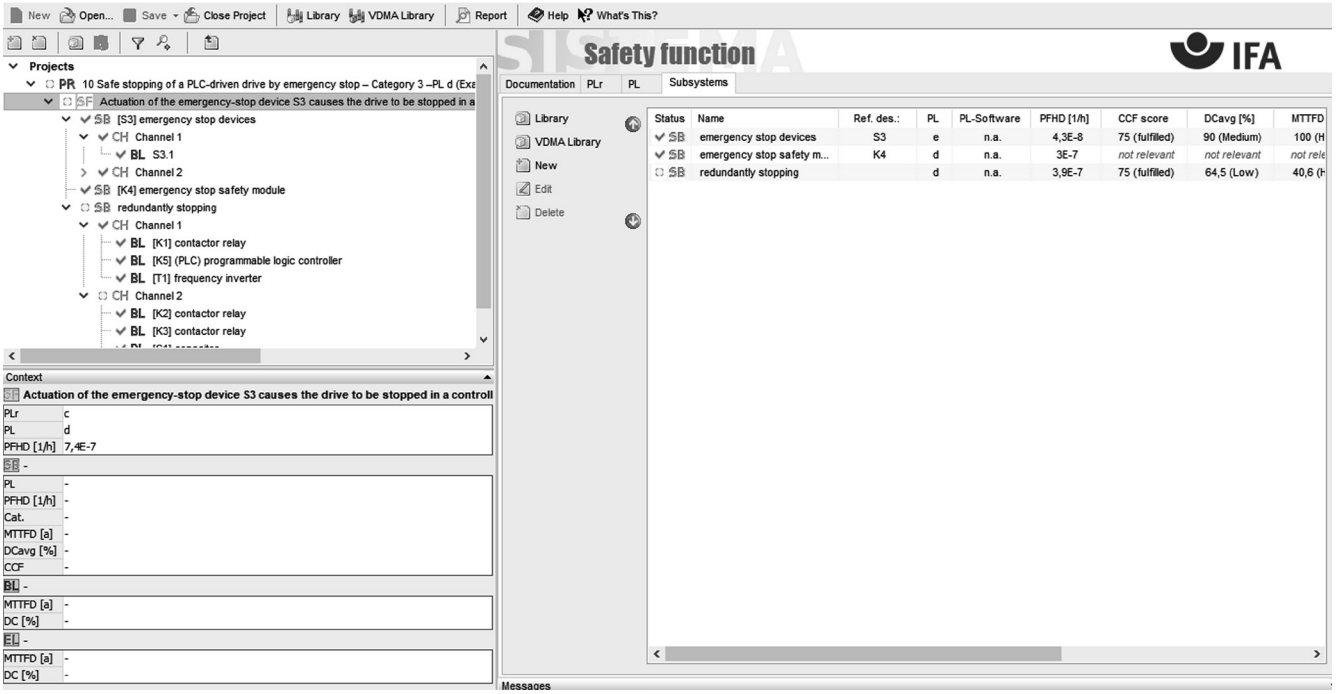
The following applies for the probability of failure of the downstream two-channel structure:

- $MTTF_D$: the PLC K5 has an $MTTF_D$ of ten years [S]. The frequency inverter has an $MTTF_D$ of 35 years [M]. The capacitor C1 is included in the calculation with an $MTTF_D$ of 45,662 years [D]. At a B_{10D} value of 5,000,000 cycles [M] and a rate of operations of daily energization on 240 working days, the result is an $MTTF_D$ of 208,333 years for K1 and K2. At a B_{10D} value of 2,000,000 cycles [M] and at 240 working days, 16 working hours and a cycle time of 3 minutes, the n_{op} is 76,800 cycles per year and the $MTTF_D$ 260 years for K3. At a B_{10D} value of 600,000 cycles [M] and at 240 working days, 16 working hours and a cycle time of 3 minutes, the n_{op} is 76,800 cycles per year and the $MTTF_D$ 7.8 years for Q1. These values produce a symmetrized $MTTF_D$ for the channel of 60 years ("high").
- DC_{avg}: an adequate test rate of the emergency-stop devices is assured (refer to the information in subclauses 6.2.14 and D.2.5.1). Fault detection of the blocks S3.1 and S3.2 is achieved by cross monitoring in K4 (*DC* = 90%). Fault detection by the process in the event of failure of actuation of the deceleration ramp leads to a *DC* of 60% for K5. For T1, the *DC* is 60%, likewise as a result of fault detection by the process. K1 and K2 exhibit a *DC* of 99% owing to the integral fault detection in K4. For K3, the *DC* is 99% owing to fault detection by K5. For C1, the *DC* is 60% owing to testing in the PLC of the timing element with the FI shut-off by way of the drop-out time of the contactor relay K3. For Q1, the *DC* is then 99% owing to direct monitoring in K5. The averaging formula for the DC_{avg} yields a result of 64% ("low").
- Adequate measures against common cause failure (75 points): separation (15), diversity (20), FMEA (5) and environmental conditions (25 + 10)
- The two-channel combination of the control elements satisfies Category 3. This yields an average probability of dangerous failure PFH_D of $3.9 \cdot 10^{-7}$ per hour. This satisfies PL d. Addition of the probability of dangerous failure of K4 and S3 yields an overall probability of failure of $7.4 \cdot 10^{-7}$ per hour. This also then satisfies PL d.
- The wearing contactor Q1 should be replaced after approximately 7.8 years (T_{10D}).

More detailed references

- *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld, R.*: Safe drive controls with frequency inverters. IFA Report 4/2018. 3rd ed. Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV). Berlin, Germany 2019 (will be published in Summer 2019). www.dguv.de/ifa, Webcode: e635980
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (2016)

Figure 8.20:
Determining of the PL by means of SISTEMA



8.2.11 Tested pneumatic valve (subsystem) – Category 2 – PL d (Example 11)

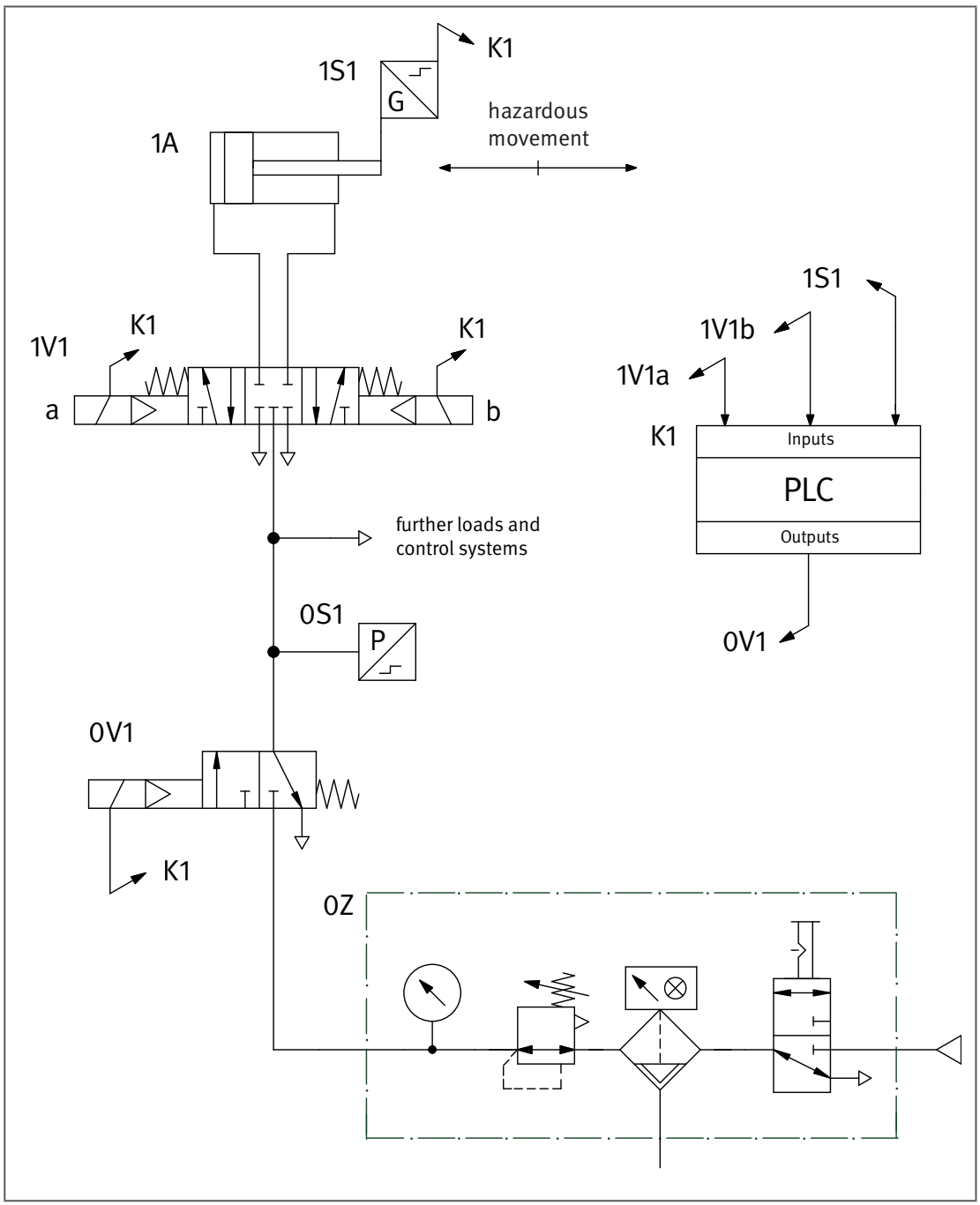
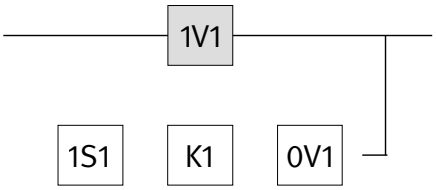


Figure 8.21: Pneumatic valve with electronic testing for the control of hazardous movements

Safety functions

- Safety-related stop function: stopping of a hazardous movement and prevention of unexpected starting from the rest position, implemented by SSC and in the event of detected faults (failure detection) by SDE
- Only the pneumatic part of the control system is shown here, in the form of a subsystem. Further SRP/CS (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.



Functional description

- Hazardous movements are controlled by a directional control valve 1V1.
- Failure of the directional control valve 1V1 between functional tests may result in loss of the safety function. The failure is dependent upon the reliability of the directional control valve.
- Testing of the safety function is forced via the PLC K1 by means of a displacement measurement system 1S1. Testing takes place at suitable intervals and in response to a demand of the safety function. Detection of failure of 1V1 leads to the exhaust valve 0V1 being switched off.
- Interruption of the hazardous movement by means of the exhaust valve 0V1 generally results in a longer overrun. The distance from the hazard zone must be selected in consideration of the longer overrun.
- The test function must not be impaired by failure of the directional control valve. Failure of the test function must not lead to failure of the directional control valve.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V1 is a directional control valve with closed centre position, sufficient overlap and spring-centred central position.
- The safety-oriented switching position is attained by cancellation of the control signal.
- Testing may for example take the form of checking of the time/distance characteristic (displacement measurement system 1S1) of the hazardous movements in conjunction with the switching position of the directional control valve, with evaluation in a PLC (K1).
- K1 must not be used for the electrical drive of 1V1.
- In order to prevent a systematic failure, the higher-level de-energization function (acting upon exhaust valve 0V1 in this example) is checked at suitable intervals, e.g. daily.
- For use in applications with infrequent operator intervention in the hazard zone. This enables the requirement of the designated architecture for Category 2 to be satisfied. The requirement is for testing to be performed immediately when a demand is made upon the safety function, and for the total time for detection of the failure and placing of the machine in a non-hazardous state, for example in consideration of the overrun, which depends upon factors including the depressurization and switching times of the valves (depressurization in this case is at a higher level via the valve 0V1), to be shorter than the time to attainment of the hazard (see also EN ISO 13855 and cf. subclause 6.2.14).
- The standard component K1 is employed in accordance with the information in subclause 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the information in subclause 6.3.

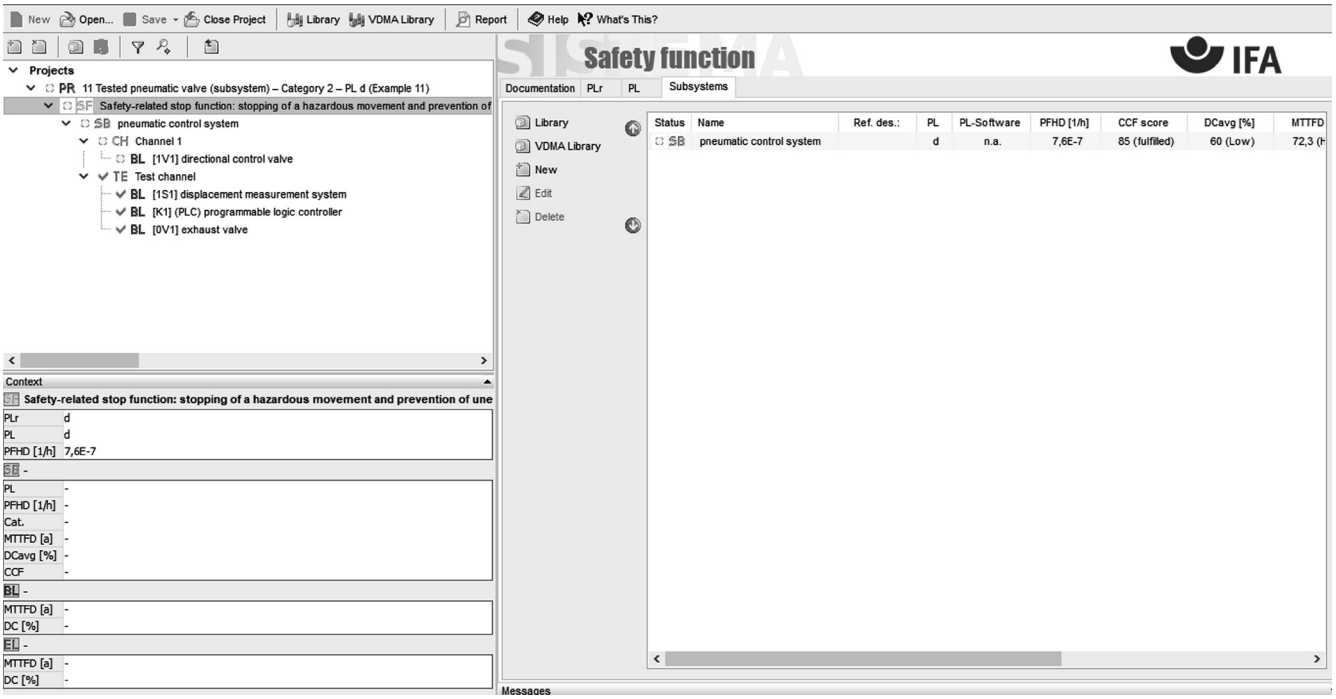
Calculation of the probability of failure

- $MTTF_D$ of the functional channel: a B_{10D} value of 20,000,000 switching cycles [S] is assumed for the directional control valve 1V1. At 240 working days, 16 working hours per day and a cycle time of 5 seconds, n_{op} is 2,764,800 switching cycles per year and the $MTTF_D$ is 72.3 years. This is also the $MTTF_D$ value for the functional channel.
- $MTTF_D$ of the test channel: an $MTTF_D$ value of 150 years [E] is assumed for the displacement measurement system 1S1. An $MTTF_D$ value of 50 years [E] is assumed for the PLC K1. A B_{10D} value of 20,000,000 cycles [S] applies for the exhaust valve 0V1. At actuation once daily on 240 working days, the $MTTF_D$ value for 0V1 is 833,333 years. The $MTTF_D$ of the test channel is thus 37.5 years.
- DC_{avg}: the *DC* of 60% for 1V1 is based upon comparison of the distance/time characteristic of the hazardous movement in conjunction with the switching status of the directional control valve. This is also the DC_{avg} ("low").
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements satisfies Category 2 with a high $MTTF_D$ (72.3 years) and low DC_{avg} (60%). This results in an average probability of dangerous failure of $7.6 \cdot 10^{-7}$ per hour. This satisfies PL d. The addition of further SRP/CS in the form of subsystems for completion of the safety function may under certain circumstances result in a lower PL. The wearing element 1V1 should be replaced approximately every seven years (T_{10D}).

More detailed reference

- VDMA technical rule 24584: Safety functions of regulated and unregulated (fluid) mechanical systems (08.16)

Figure 8.22:
Determining of the PL by means of SISTEMA



8.2.12 Tested hydraulic valve (subsystem) – Category 2 – PL d (Example 12)

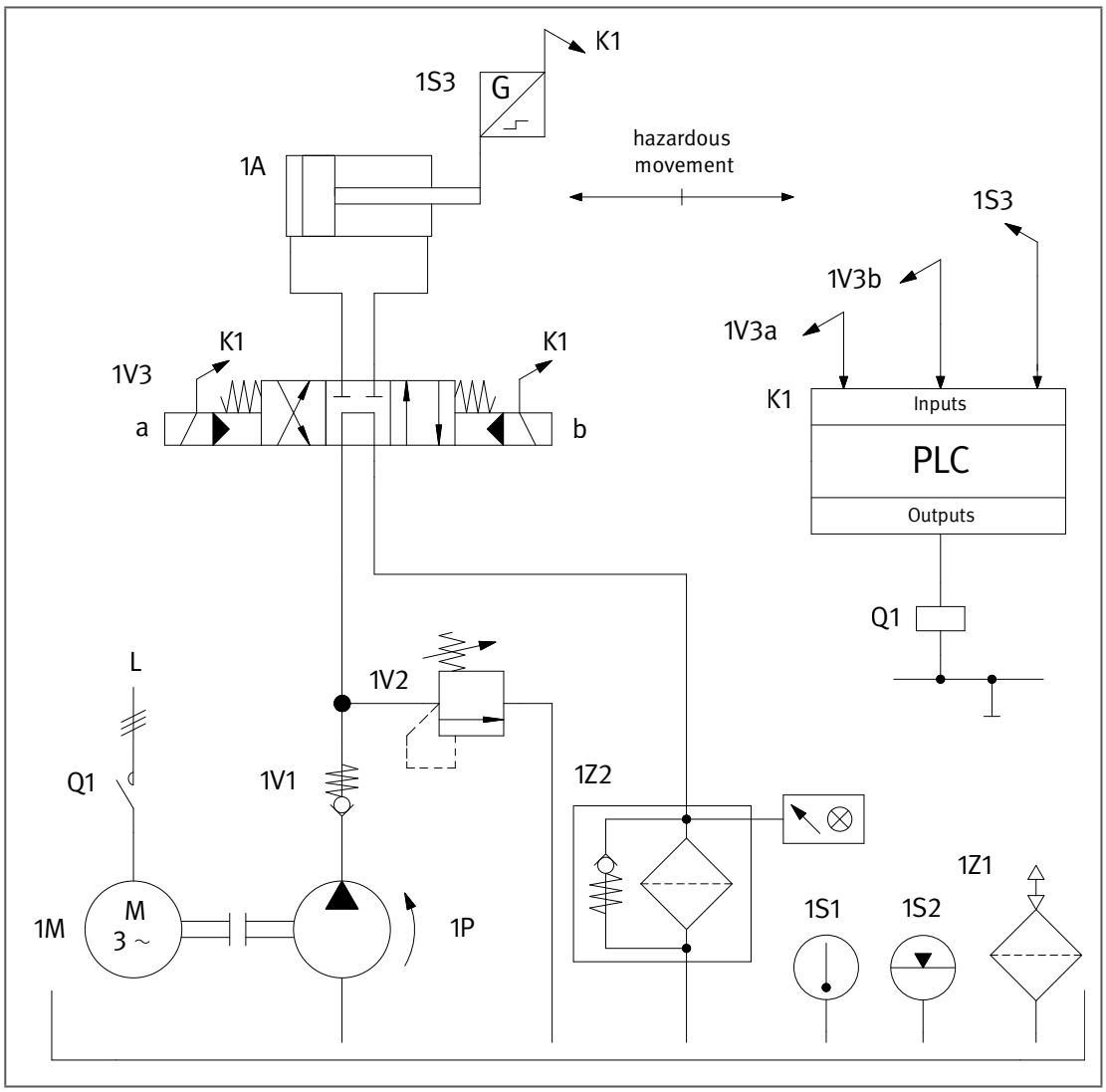


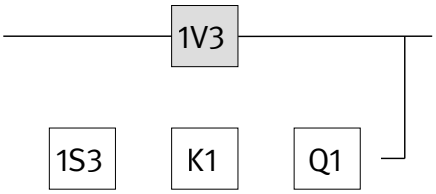
Figure 8.23: Hydraulic valve with electronic testing for the control of hazardous movements

Safety functions

- Safety-related stop function: stopping of a hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control system is shown here, in the form of a subsystem. Further safety-related control components (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled by the directional control valve 1V3.
- Failure of the directional control valve 1V3 between functional tests may result in loss of the safety function. The probability of failure is dependent upon the reliability of the directional control valve.
- Testing of the safety function is forced via the PLC K1 by means of a displacement measurement system 1S3. Testing takes place at suitable intervals and in response to a demand of the safety function. Detection of a failure of 1V3 leads to the hydraulic pump 1M/1P being switched off by the contactor Q1.



- Interruption of the hazardous movement by the hydraulic pump generally results in a longer overrun. The distance from the hazard zone must be selected in consideration of the longer overrun.
- The test function must not be impaired by failure of the directional control valve. Failure of the test function must not lead to failure of the directional control valve.

Design features

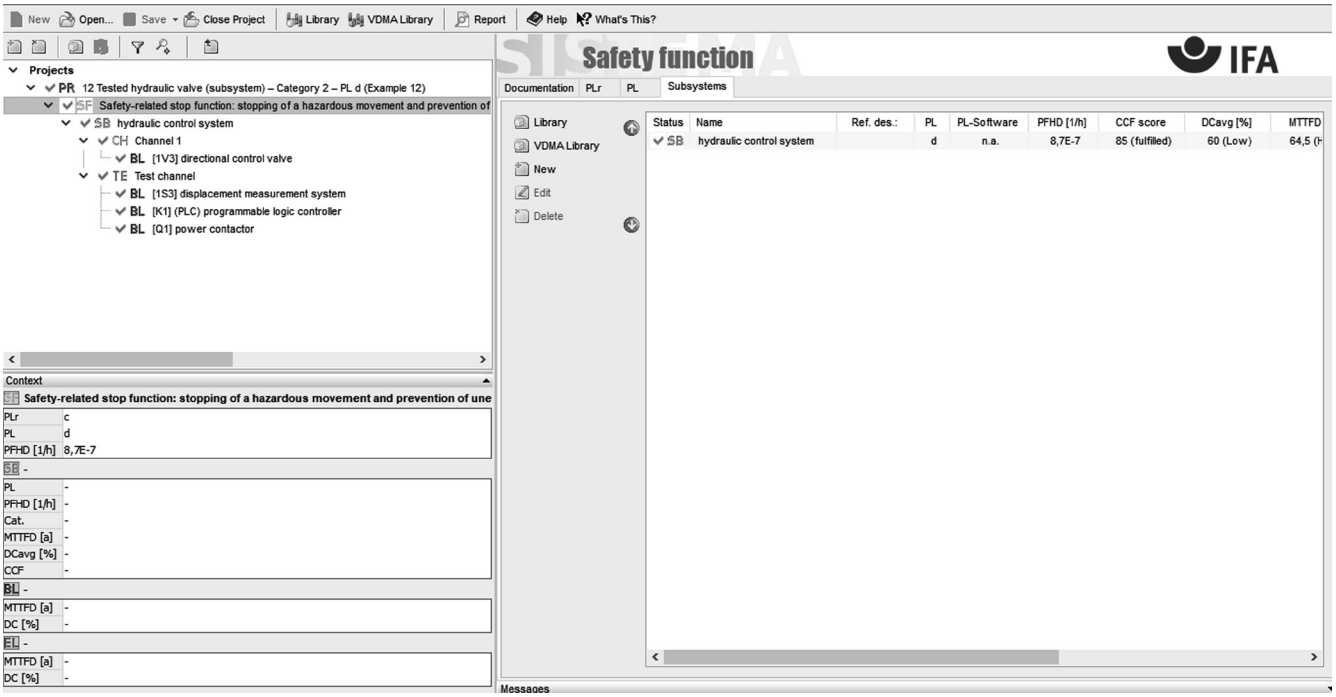
- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V3 is a directional control valve with closed centre position, sufficient overlap and spring-centred central position.
- The safety-oriented switching position is attained by cancellation of the control signal.
- Testing may for example take the form of checking of the distance/time characteristic (displacement measurement system 1S3) of the hazardous movements in conjunction with the switching position of the directional control valve, with evaluation in a PLC (K1). K1 must not be used for the electrical drive of 1V3.
- In order to prevent a systematic failure, the higher-level de-energization function (acting upon the hydraulic pump in this example) is checked at suitable intervals, e.g. daily.
- For use in applications with infrequent operator intervention in the hazard zone. This enables the requirement of the designated architecture for Category 2 to be satisfied. The requirement is for testing to be performed immediately upon a demand being made upon the safety function, and for the total time for detection of the failure and placing of the machine in a non-hazardous state, for example in consideration of the overrun, to be shorter than the time to attainment of the hazard (see also EN ISO 13855 and cf. subclause 6.2.14)
- The standard component K1 is employed in accordance with the information in subclause 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the information in subclause 6.3.

Calculation of the probability of failure

- $MTTF_D$ of the functional channel: an $MTTF_D$ of 150 years is assumed for the directional control valve 1V3 [M]. This is also the $MTTF_D$ value for the functional channel, which is first capped to 100 years.
- $MTTF_D$ of the test channel: an $MTTF_D$ value of 91 years [M] is assumed for the displacement measurement system 1S3. An $MTTF_D$ value of 50 years [E] is assumed for the PLC K1. A B_{10D} value of 1,300,000 cycles [S] applies for the contactor Q1. At actuation once daily on 240 working days, the $MTTF_D$ value for Q1 is 54,166 years. The $MTTF_D$ of the test channel is thus 32.3 years. The $MTTF_D$ of the functional channel must therefore be reduced to 64.5 years in accordance with the underlying analysis model.
- DC_{avg}: the DC of 60% for 1V3 is based upon the comparison of the distance/time characteristic of the hazardous movement in conjunction with the switching status of the directional control valve. This is also the DC_{avg} (“low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)

- The combination of the control elements satisfies Category 2 with a high $MTTF_D$ (75 years) and low DC_{avg} (60%). This results in an average probability of dangerous failure of $8.7 \cdot 10^{-7}$ per hour. This satisfies PL d. The addition of further SRP/CS in the form of subsystems for completion of the safety function may under certain circumstances result in a lower PL.

Figure 8.24:
Determining of the PL by means of SISTEMA



8.2.13 No-load sensing system for studio hoists – Category 2 – PL d (Example 13)

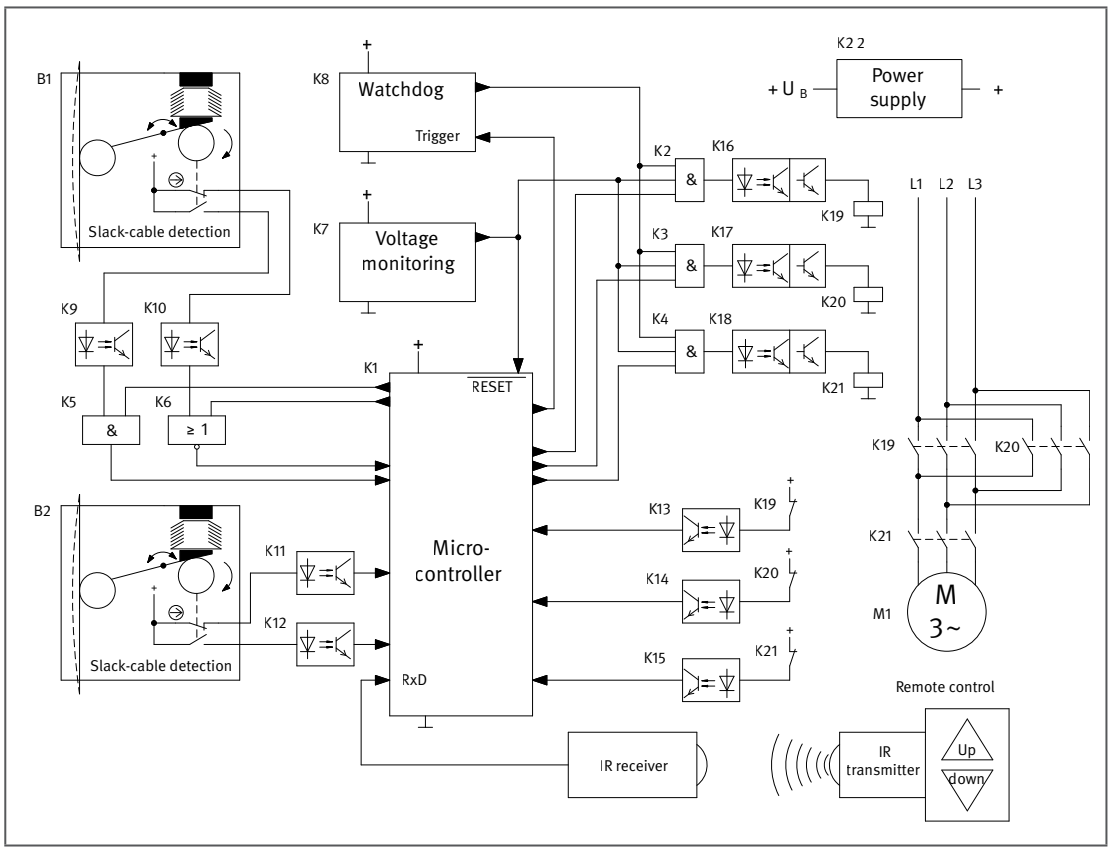


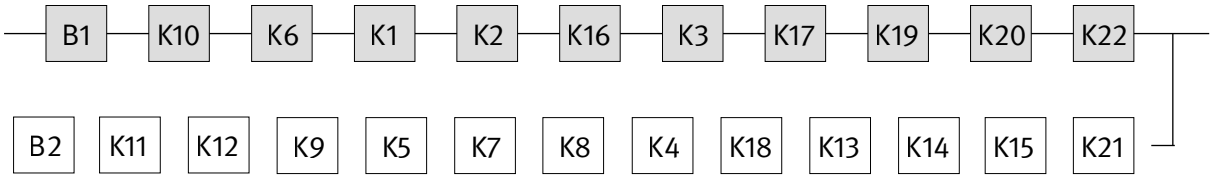
Figure 8.25: Combined electromechanical and programmable electronic control system for the prevention of no-load states on studio hoists

Safety function

- No-load/slack-cable detection: should a slack cable or suspension element be detected on a studio hoist, the downward movement is stopped (STO – safe torque off).

Functional description

- Studio hoists driven by electric motors are widely used in studio and stage applications. During downward movement, the cable may become slack should the load stick or tilt or come to rest on other objects. In such cases, a risk exists for example of the obstruction suddenly giving way, the load slipping, and danger consequently arising for persons in the hazard zone.
- Upward and downward movements of the studio hoist can for example be controlled by means of an infrared remote control. This function is not evaluated here; it must, however, always be implemented with consideration for safety.
- In order for the studio hoist to be prevented from falling in the event of breakage of one suspension element, the load is borne by two suspension elements. A slack-cable switch B1/B2 with a break-contact element/make-contact element combination is fitted to each suspension element.
- The microcontroller K1 evaluates the switching states of the slack-cable switches B1 and B2. Via logic gates K2/K3 and optocoupled transistor amplifiers K16/K17, K1 also controls the contactor relays K19 and K20 for the upward and downward movements of the studio hoist.
- The switching states of the contacts of the slack-cable switches B1 and B2 are evaluated by the microcontroller K1 and tested for plausibility. For testing of the inputs used on the microcontroller, forced dynamics is employed on the signals from the slack-cable switch B1. This involves the microcontroller forcing a temporary signal change via the logic gates K5 and K6, in order to ascertain whether the inputs are still able to transmit the signal change. Forced dynamics of the signals of one slack-cable switch is sufficient.



- Self-tests of the integrated units such as the ALU, RAM and ROM are performed in the microcontroller K1. The voltage monitor K7 monitors the supply voltage generated by means of K22. Faults in the microcontroller are detected by temporal monitoring of the program sequence in the watchdog K8. The components K19 to K21 for control of the studio hoist's upward and and downward movements are monitored by means of readback – decoupled by optocouplers K13 to K15 – in the microcontroller. Should a fault be detected, the studio hoist is shut off at a higher level by the component detecting the fault via the contactor relay K21, actuated by logic gate K4 and decoupled by optocoupler K18. If the watchdog K8 is not retriggered in time by the microcontroller K1, the movement of the studio hoist is stopped from K8 via all logic gates K2 to K4.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits as described in the initial paragraphs of Chapter 8 are implemented.
- A slack cable is detected redundantly for both suspension elements via the two slack-cable switches B1 and B2. These switches contain position switches with direct opening action in accordance with IEC 60947-5-1, Annex K.
- A stable arrangement is assured for the operating mechanism of the slack-cable switches.
- K19 to K21 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.
- The software (SRESW) for K1 is programmed in accordance with the requirements for PL d and the information in subclause 6.3.

Remarks

- DIN 56950-2, subclause 5.2.1 requires two suspension elements in order to prevent a studio hoist and its load from falling.
- Visual inspections and maintenance of the suspension elements must be performed at suitable intervals.
- Parts of the circuit structure as shown are not explicitly designed to prevent possible hazards resulting from unexpected movement of the studio hoist.
- As the calculation of the probability of failure shows, the circuit structure used attains PL d for the safety function under consideration here. Use of the risk graph to determine the required Performance Level PL_r with the parameters S2, F1 and P1 in accordance with DIN 56950-2, subclause A.1.2.3.3 results in a PL_r of c, provided the studio hoist is operated under supervision and only by skilled personnel. Should this not be the case, a PL_r of d is required.

Calculation of the probability of failure

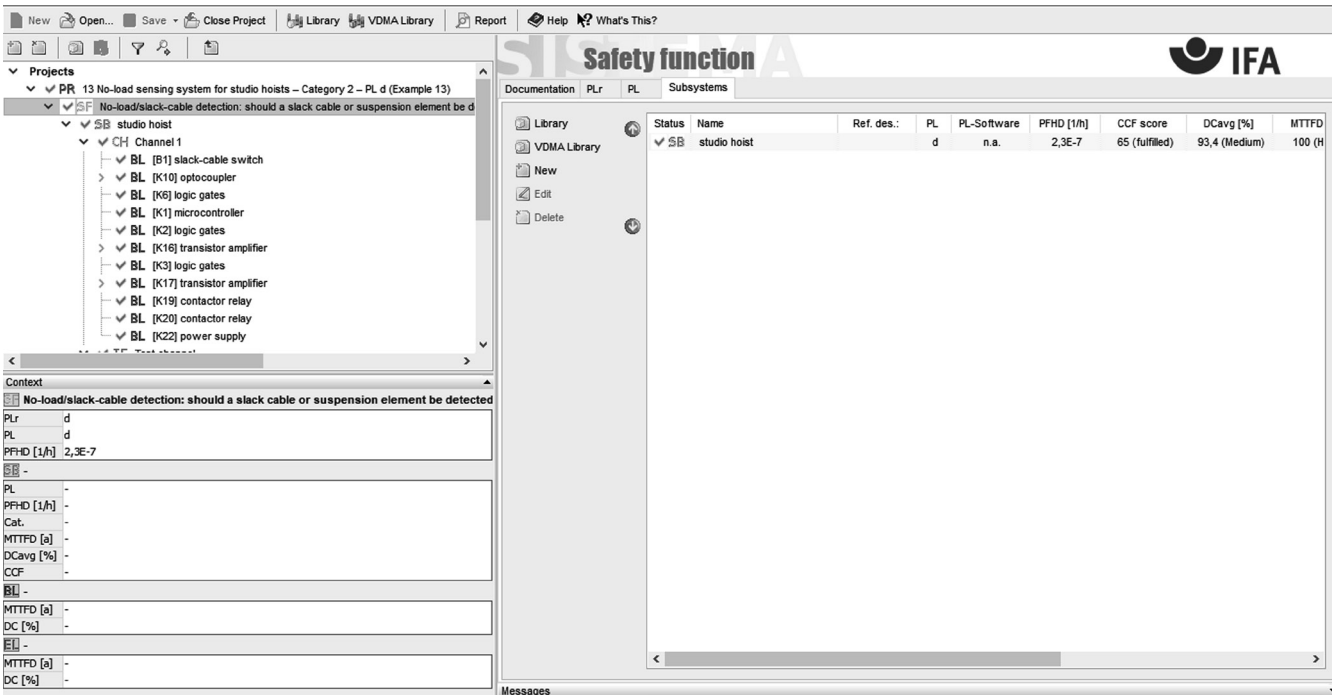
- Components are grouped into blocks in Figure 8.25 in the interests of clarity. K9 to K15 each contain one optocoupler and two resistances. K16 to K18 additionally each contain a transistor for driving the downstream contactor relays.
- For application of the simplified procedure for estimation of the achieved PL, the components in the circuit are assigned to the blocks of the designated architecture for Category 2 as follows:
  I: B1
  L: K10, K6, K1, K2, K16, K3, K17, K22
  O: K19, K20
  TE: B2, K11, K12, K9, K5, K7, K8, K4, K18, K13, K14, K15
  OTE: K21

- $MTTF_D$: the $MTTF_D$ values required for the calculation were sourced primarily from EN ISO 13849-1 [S], and from SN 29500-2 and SN 29500-14 [D]. The following values are substituted for B1 and B2: B_{10D}: 100,000 cycles [E]; n_{op}: 10 cycles per year. For the contactor relays K19 to K21: B_{10D}: 400,000 cycles [S]; n_{op}: 10 cycles per day on 365 working days. An $MTTF_D$ of 1,141 years [D] is substituted for the microcontroller K1. The following $MTTF_D$ values are substituted for the electronic components [D]: 4,566 years for the watchdog K8, 5,707 years for the optocouplers K9 to K18, 22,831 years for the logic gates K2 to K6, 38,052 years for the voltage monitor K7, 45,662 years for transistors and 228,310 years for resistors. An $MTTF_D$ of 228 years [E] is assumed for the power supply K22. Summation of the failure rates for all components of the functional channel (blocks I, L and O) produces an $MTTF_D$ value of 128 years. This value is capped to 100 years ("high") in accordance with the requirements of the standard.
- The $MTTF_D$ of the test channel is produced by summation of the failure rates of all components of blocks TE and OTE. The resulting value of 389 years is greater than or equal to half of the $MTTF_D$ of the functional channel.
- DC_{avg}: the DC is 60% for B1, K10 and K6 owing to cross monitoring of B1 and B2 in K1 with a low demand rate upon the safety function. The DC is 60% for K1 owing to temporal monitoring of program sequence and self-tests of simple effectiveness. The DC is 99% for K2, K3, K16, K17, K19 and K20 owing to direct monitoring by means of mechanically linked contact elements. For K22, the DC is 99%. The averaging formula returns a result of 93% ("medium") for DC_{avg}.
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection (15) and environmental conditions (25 + 10)
- The combination of the control elements satisfies Category 2 with a high $MTTF_D$ of the functional channel (100 years) and medium DC_{avg} (93%). This results in an average probability of dangerous failure PFH_D of $2.3 \cdot 10^{-7}$ per hour. This satisfies PL d.

More detailed references

- DIN 56950-2: Entertainment technology – Machinery installations – Part 2: Safety requirements for studio hoists (09.14). Beuth, Berlin, Germany 2014
- DGUV Information 215-310: Sicherheit bei Veranstaltungen und Produktionen – Leitfaden für Theater, Film, Hörfunk, Fernsehen, Konzerte, Shows, Events, Messen und Ausstellungen (formerly BGI 810). Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin, Germany 2016
  http://publikationen.dguv.de/dguv/pdf/10002/215-310.pdf
- SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Published by: Siemens AG, Corporate Technology, Technology & Innovation Management, Munich, Germany 2004-2014

Figure 8.26:
Determining of the PL by means of SISTEMA



8.2.14 Pneumatic valve control (subsystem) – Category 3 – PL d (Example 14)

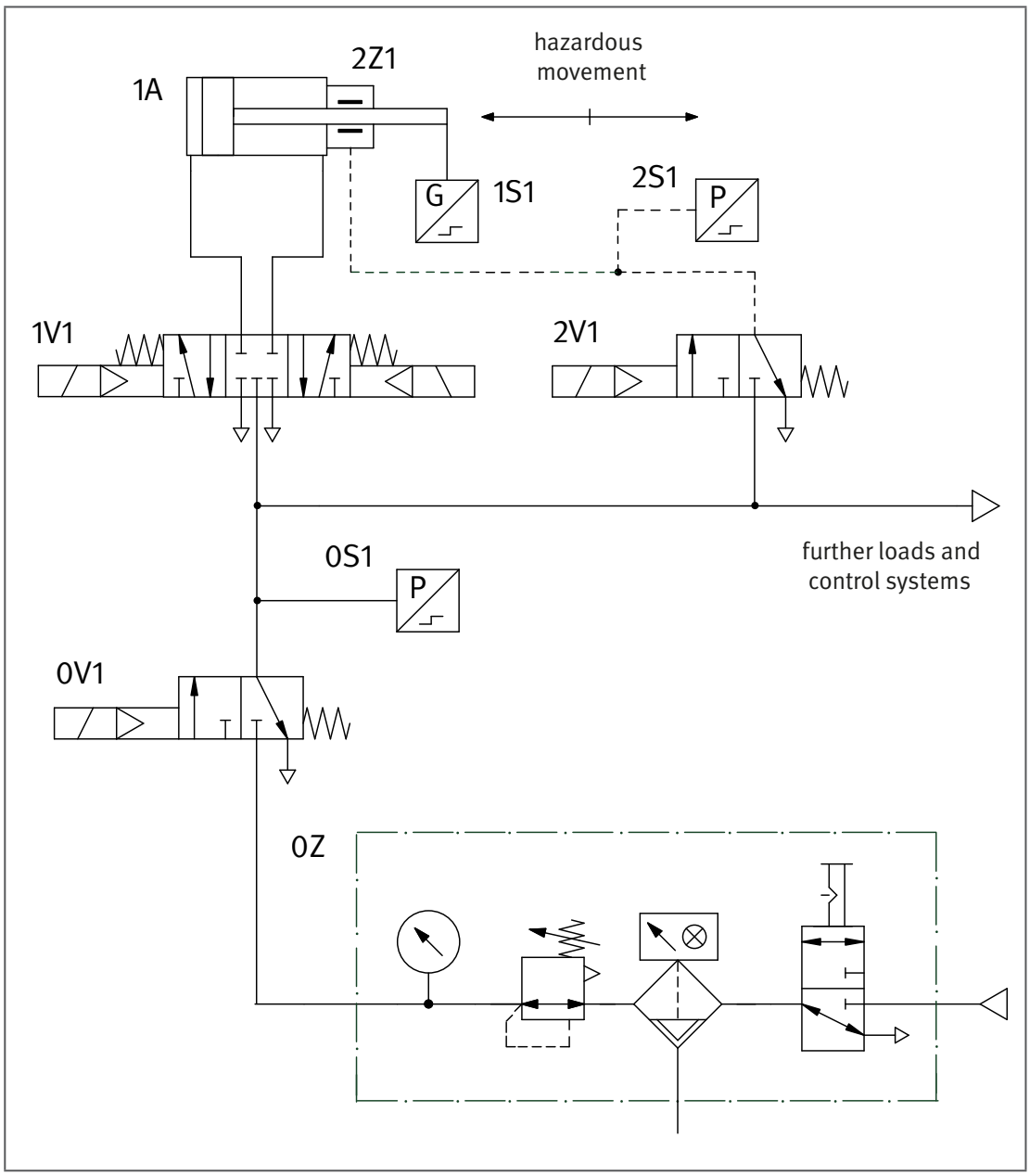


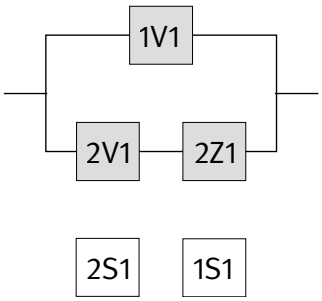
Figure 8.27: Tested pneumatic valves for redundant control of hazardous movements

Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position, implemented by safety sub-functions SSC and SBC
- Only the pneumatic part of the control system is shown here, in the form of a subsystem. Further SRP/CS (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled/stopped redundantly by a directional control valve 1V1 and a brake 2Z1 on the piston rod respectively. The brake 2Z1 is actuated by a control valve 2V1.
- Failure of one of these valves or of the brake alone does not result in loss of the safety function.
- The directional control valve and the brake are actuated cyclically in the process.



- The functioning of the control valve 2V1 is monitored by means of a pressure switch 2S1. Certain faults on the unmonitored directional control valve 1V1 and the unmonitored brake 2Z1 are detected in the work process. In addition, the overrun (distance/time characteristic) during the braking process (dynamic) and/or at start-up of the machine (static) is monitored with the aid of a displacement measurement system 1S1 on the piston rod. An accumulation of undetected faults may lead to loss of the safety function.
- Testing of the safety function is implemented at suitable intervals, for example at least every eight working hours.
- The test function must not be impaired by failure of the brake. Failure of the test function must not lead to failure of the brake.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The directional control valve 1V1 features a closed centre position with sufficient overlap and spring-centred central position.
- The safety-oriented switching position is assumed from any position by cancellation of the control signal.
- Signals from the pressure monitor 2S1 and the displacement measurement system 1S1 are processed for example in the upstream electrical logic (not shown).

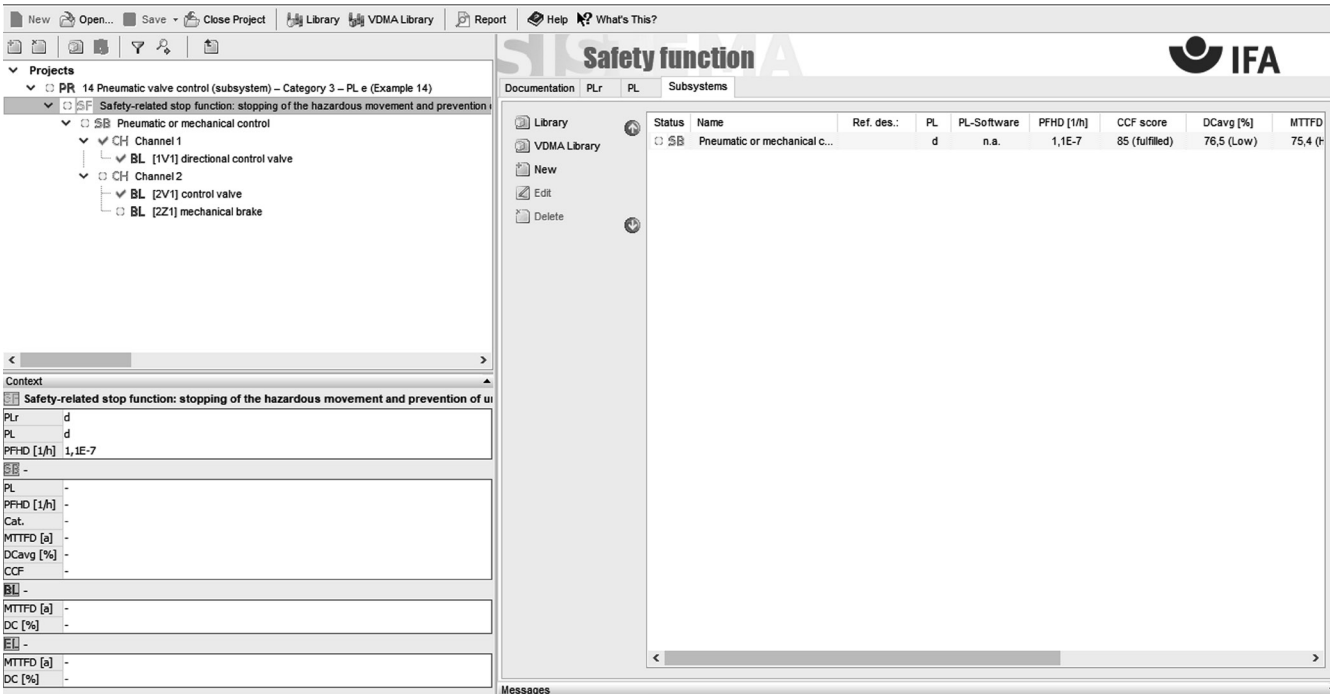
Calculation of the probability of failure

- $MTTF_D$: B_{10D} values of 20,000,000 cycles [S] are assumed for the valves 1V1 and 2V1. At 240 working days, 16 working hours and a cycle time of 15 seconds, n_{op} is 921,600 cycles per year. The $MTTF_D$ for 1V1 and 2V1 is thus 217 years. A B_{10D} value of 5,000,000 switching cycles [M] is substituted for the mechanical brake on the piston rod 2Z1. This results in an $MTTF_D$ of 54 years for the mechanical brake. Overall, the resulting symmetrized $MTTF_D$ value per channel is 75 years (“high”).
- DC_{avg}: pressure monitoring of the control signal for the brake results in a DC of 99% for the control valve 2V1. The DC for the directional control valve 1V1 is 60% owing to fault detection through the process. Start-up testing of the mechanical brake yields a DC of 75% for 2Z1. Averaging thus produces a DC_{avg} of 76.5% (“low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements satisfies Category 3 with a high $MTTF_D$ per channel (75 years) and low DC_{avg} (76.5%). This results in an average probability of dangerous failure of $1.1 \cdot 10^{-7}$ per hour. This satisfies PL d. The addition of further SRP/CS in the form of subsystems for completion of the safety function may under certain circumstances result in a lower PL.
- The wearing brake 2Z1 should be replaced at intervals of approximately five years (T_{10D}).

More detailed reference

- VDMA technical rule 24584: Safety functions of regulated and unregulated (fluid) mechanical systems (08.16)

Figure 8.28:
Determining of the PL by means of SISTEMA



8.2.15 Protective device and hydraulics controlled by PLC – Category 3 – PL d (Example 15)

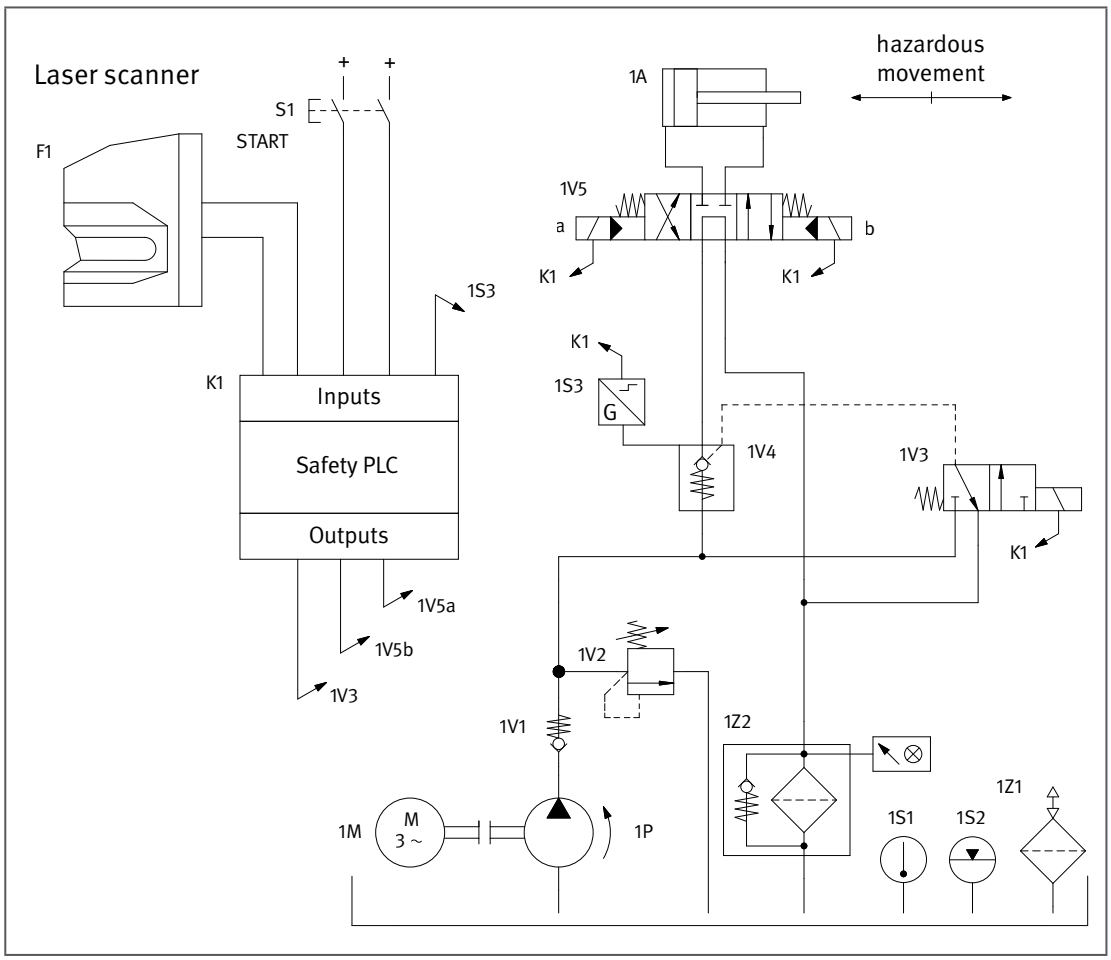


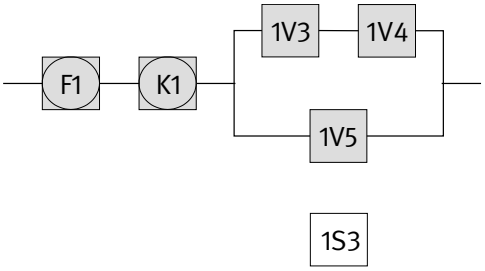
Figure 8.29: Detection zone monitoring by laser scanner with electrohydraulic deactivation of the hazardous movement

Safety function

- Safety-related stop function, initiated by a protective device: penetration of the laser scanner's detection zone results in stopping of the hazardous movement.

Functional description

- The laser scanner F1 monitors, with its detection zone, the area in which movement of the cylinder 1A may present a danger to the operator. The output signal of the laser scanner is read in on two channels by the safety PLC K1. Following any violation of the detection zone, the next movement must be enabled by actuation of a start button S1 evaluated in K1 (restart interlock). K1 controls the movement of 1A with the aid of the hydraulic part of the control system.
- The hydraulic part of the control system comprises a two-channel arrangement. The first channel comprises directional control valve 1V3, which acts upon the pilot-operated non-return valve 1V4. In the closed position, 1V4 blocks movements of 1A. The second channel consists of the directional control valve 1V5, which in its closed centre position also prevents movement of 1A.
- 1V5 is actuated cyclically in the process. 1V3 and 1V4 close only in the event of violation of the detection zone (demand of the safety function), but at least once per shift.
- Direct position monitoring 1S3 is implemented on 1V4 and evaluated in K1 as a fault detection measure. Faults in 1V5 can be detected via the process owing to the function. An accumulation of undetected faults in the hydraulic part of the control system may lead to loss of the safety function.



Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Faults in the conductors to F1 and K1 must not be hazardous in their effects. For this purpose, faults are detected as they arise, and the safe state is initiated. Alternatively, fault exclusion to EN ISO 13849-2, Table D.4 must be possible for conductor short circuits.
- The laser scanner F1 and safety PLC K1 are tested safety components for use in PL d that satisfy Category 3 and the relevant product standards.
- The directional control valve 1V5 features a closed centre position with sufficient overlap and spring-centred central position. The position of 1V4 is monitored electrically, since 1V4 is not switched cyclically.
- The software (SRASW) is programmed in accordance with the requirements for PL d and the information in sub-clause 6.3.
- It is assumed that each output of the safety PLC is driven by both processing channels of the PLC. Should this not be the case, the outputs that drive 1V3 and 1V4 are driven by one channel of the PLC, the output that drives 1V5 by the other.

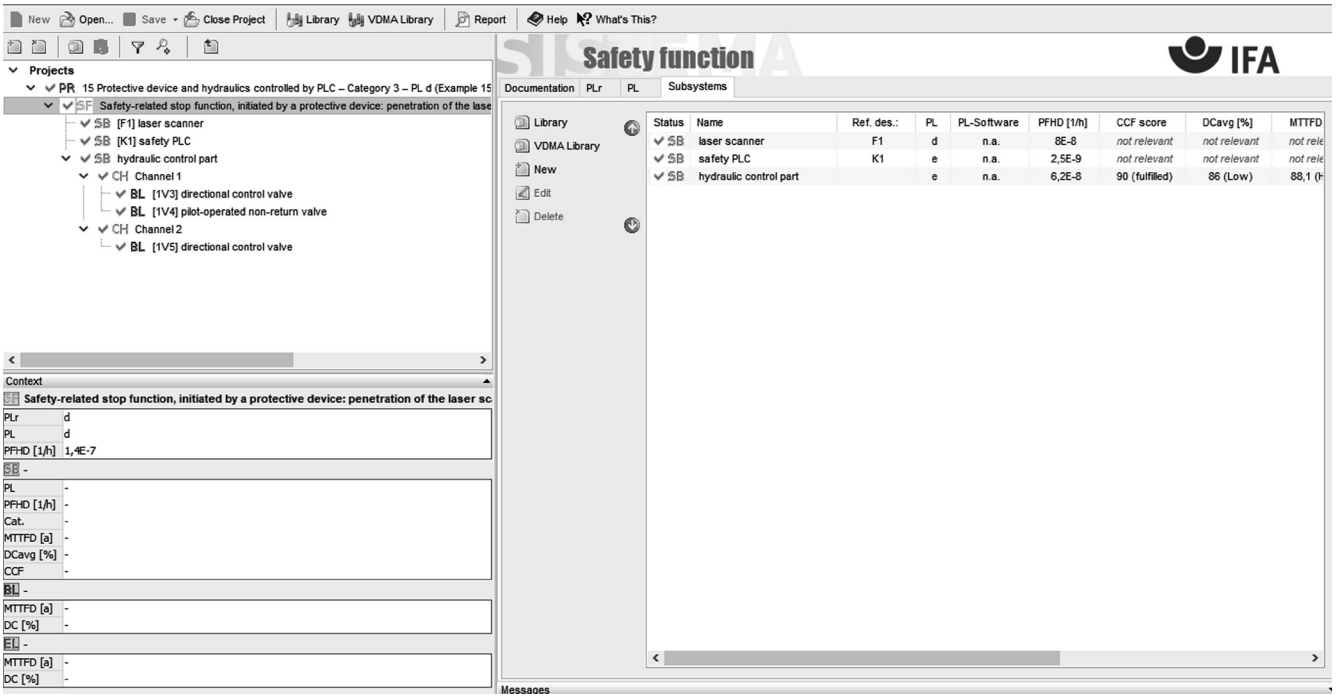
Calculation of the probability of failure

- Since the laser scanner F1 and the safety PLC K1 are available for purchase as safety components, their probabilities of failure are added at the end of the calculation (F1: $PFH_D = 8.0 \cdot 10^{-8}$ per hour [M], K1: $PFH_D = 2.5 \cdot 10^{-9}$ per hour [M]). For the hydraulic part of the control system, the probability of failure is calculated as shown below.
- $MTTF_D$: values of 150 years [M] are assumed for the valves 1V3 to 1V5. Overall, this results in a symmetrized $MTTF_D$ value of 88 years (“high”) for the two channels.
- DC_{avg}: a *DC* of 99% for 1V4 is produced by direct monitoring in K1 with the aid of the position monitor 1S3. Owing to the close coupling of 1V3 and 1V4, this results in 1V3 being monitored indirectly at the same time with a *DC* of 99%. The *DC* of 60% for 1V5 is based upon fault detection in the process with cyclical actuation. Averaging thus produces a DC_{avg} of 86% (“low”).
- Adequate measures against common cause failure (90 points): separation (15), diversity (20), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements in the hydraulic part satisfies Category 3 with a high $MTTF_D$ per channel (88 years) and low DC_{avg} (86%). This results in an average probability of dangerous failure of $6.2 \cdot 10^{-8}$ per hour for the hydraulic system.
- Altogether, the average probability of dangerous failure PFH_D is $(8.0 + 0.25 + 6.2) \cdot 10^{-8}$ per hour = $1.4 \cdot 10^{-7}$ per hour. This satisfies PL d.

More detailed reference

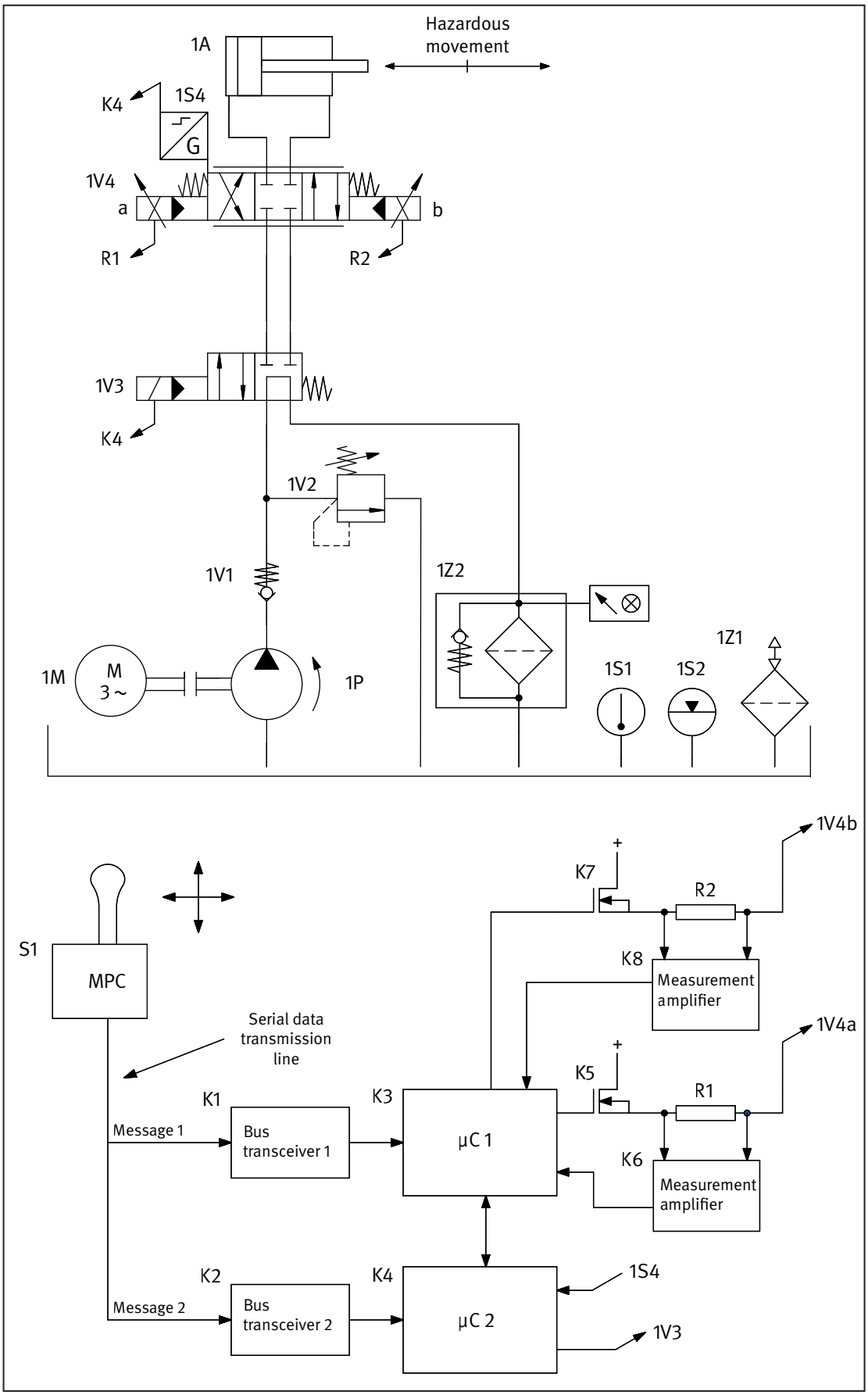
- *Bömer, T.*: Hinweise zum praktischen Einsatz von Laserscannern (code 310 243). In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2nd ed. Suppl. XII/99. Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin, Germany. Erich Schmidt, Berlin, Germany 2003 – loose-leaf ed. www.ifa-handbuchdigital.de/310243

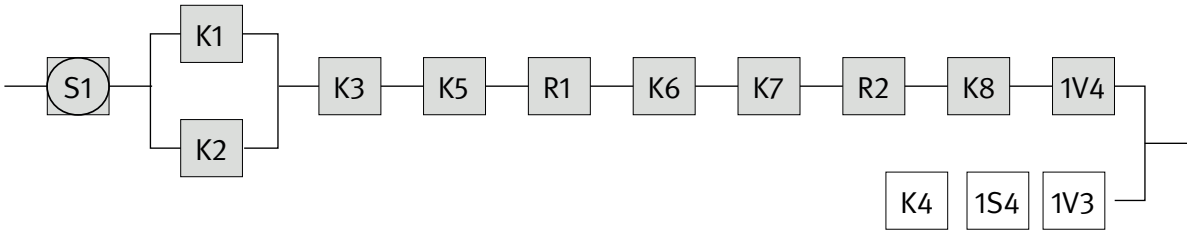
Figure 8.30:
Determining of the PL by means of SISTEMA



8.2.16 Earth-moving machine control system with bus system – Category 2/3 – PL d (Example 16)

Figure 8.31:
Control of hazardous movements of an earth-moving machine





Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position of tools on earth-moving machinery.
- Further safety-related functions, such as that for preventing an incorrect direction of movement being selected for tools on the earth-moving machine, are not considered in this example.

Functional description

- The multi-purpose control (MPC) S1 converts the operator‘s manual movement of it into electronic messages. It sends these messages cyclically over a serial data communications line (bus system) to the logic control. This generates control signals for the hydraulics, which in turn executes the working movements of the earth-moving machine desired by the operator.
- The message 1 sent by the MPC S1 reaches the microcontroller K3 via the bus transceiver K1. From message 1 and in accordance with the algorithms stored in the software, K3 generates the analog signals required for actuation of the proportional valve 1V4. The resistances R1/R2 and the measuring amplifiers K6/K8 have the function of controlling the output currents for the proportional valve. The microcontroller K4 receives a redundant message 2 from S1 via the bus transceiver K2. Within the response time/process safety time, K4 checks the correct displacement of the proportional valve 1V4, as signalled by the position measuring system 1S4 integrated into 1V4, for plausibility against the desired position determined from message 2. Should faults be detected, K4 switches off the hydraulic pressure at a higher level by means of the directional control valve 1V3, and places the system in the safe state.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The MPC is a safety component suitable for use in PL d and satisfies the requirements for Category 3.
- In accordance with the functional description, processing of the control information and actuation of the valves are effected within a Category 2 structure. Within this structure, K4 and 1S4 form the test channel with 1V3 as the shut-off element of the test channel.
- Owing to the continual monitoring of 1V4 by K4 through 1S4, failure of 1V4 can be detected as soon as a demand is made upon the safety function. 1V3 must execute the safe response within the response time in order for the structure of the control to satisfy Category 2. Abrupt switching of 1V3 at a higher level must not give rise to hazards.
- The proportional valve 1V4 and the directional control valve 1V3 have a closed position/closed centre position, spring centred central position, and sufficient overlap.
- The software (SRESW) for K3 and K4 is programmed in accordance with the requirements for PL d and the information in subclause 6.3.

- Data transfer from the MPC to the logic control is safe in accordance with GS-ET-26/IEC 61784-3. The data communications protocol employed contains redundant messages with comparison between K3 and K4, and measures for detection of the following transmission errors: repetition, loss, insertion, incorrect sequence, corruption, delay and masquerade (see also subclause 6.2.18). The residual error rate Λ is lower than $1 \cdot 10^{-8}$ per hour and thus contributes, as specified in the assessment standards, less than 1% towards the maximum permissible probability of failure of the safety function. Modelling is in Category 4; the resulting component in the calculation of the overall probability of failure is negligible.

Remarks

- An emergency motion function of the earth-moving machine, which is not shown here, may be required; if so, it must be implemented at a higher level.

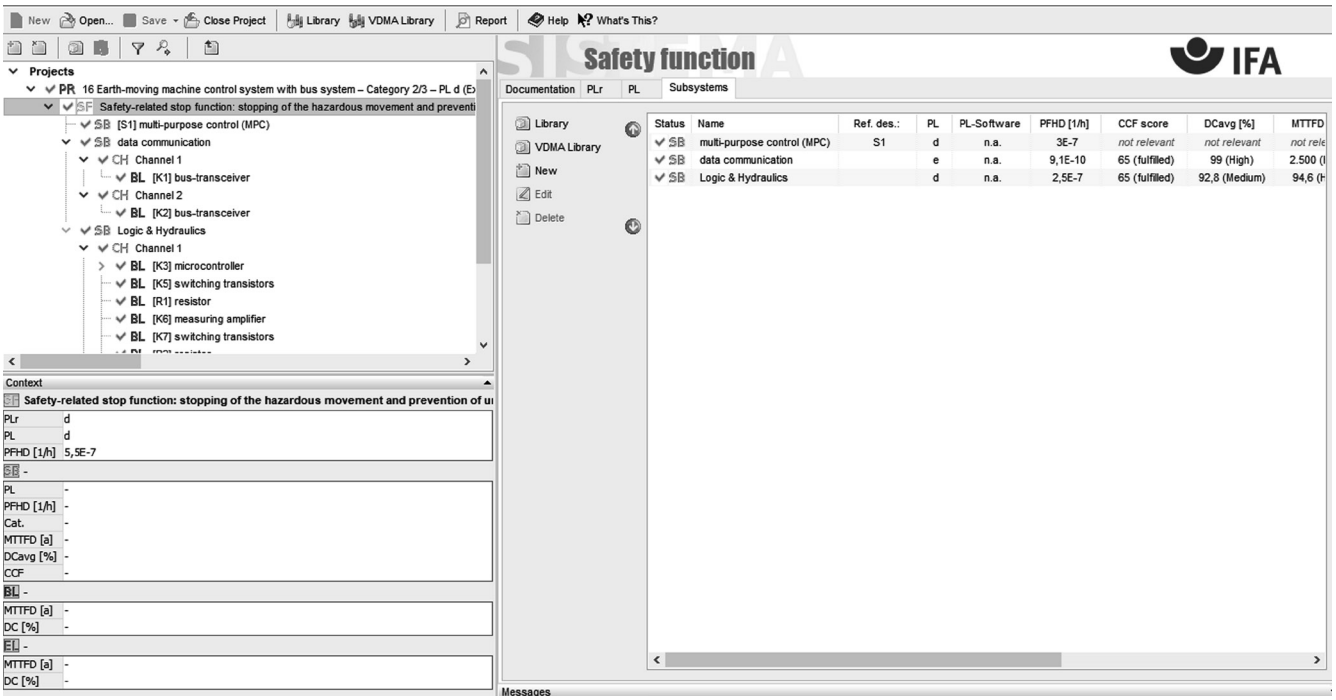
Calculation of the probability of failure

- The multi-purpose control S1 is a commercial safety component. The associated probability of failure is added at the end of the calculation ($PFH_D = 3.0 \cdot 10^{-7}$ per hour [E]). For the remaining part of the control system, the probability of failure is calculated below.
- $MTTF_D$ of data communication: an $MTTF_D$ of 11,416 years [D] is assumed for the bus transceivers K1 and K2. This is capped in Category 4 to the maximum value of 2,500 years.
- DC_{avg} of data communication: DC = 99% for K1 and K2 by cross monitoring of the messages in the microcontrollers K3 and K4.
- The calculated probability of failure of data communication is a PFH_D of $9.1 \cdot 10^{-10}$ per hour.
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection (15) and environmental conditions (25 + 10). This analysis also applies to the downstream parts of the control system.
- $MTTF_D$ of the functional channel of the logic and hydraulic control system: in accordance with SN 29500-2, an $MTTF_D$ of 878 years [D] is considered for the microcontroller K3, including its peripherals. The following values are substituted for the further electrical components [D]: 45,662 years for the switching transistors K5 and K7, 228,311 years for the resistances R1 and R2, and 1,142 years for the measuring amplifiers K6 and K8. An $MTTF_D$ of 150 years [S] is assumed for the proportional valve 1V4. The $MTTF_D$ value of the functional channel is thus 104 years.
- $MTTF_D$ of the test channel of the logic and hydraulic control: in accordance with SN 29500-2, an $MTTF_D$ of 878 years [D] is considered for the microcontroller K4, including its peripherals. An $MTTF_D$ of 75 years [E] is assumed for the position measuring system 1S4. An $MTTF_D$ of 150 years [S] is assumed for the directional control valve 1V3. The $MTTF_D$ value of the test channel is thus 47 years. Use of the simplified procedure described in the standard for estimation of the quantifiable aspects of the PL is conditional upon the $MTTF_D$ of the test channel being greater than half the $MTTF_D$ of the functional channel. The $MTTF_D$ value of the functional channel is therefore reduced to 94 years.
- DC_{avg} of the functional channel of the logic and hydraulic control: the DC for K3 is 60% owing to cross monitoring with K4 and self-tests of simple effectiveness by means of software; the DC for the remaining electrical components is 90% owing to fault detection in K4 by means of the position measuring system 1S4. The DC for 1V4 is 99% owing to direct monitoring of the position via 1S4 in K4. The averaging formula for DC_{avg} produces a result of 93% (“medium”).
- The logic and hydraulic control satisfies Category 2 with a high $MTTF_D$ of each channel (94 years) and medium DC_{avg} (93%). This results in an average probability of dangerous failure PFH_D of $2.5 \cdot 10^{-7}$ per hour.
- The average probability of dangerous failure of the safety function is produced by addition of the proportions for the MPC, the data communication and the logic and hydraulic control, yielding a PFH_D of $5.5 \cdot 10^{-7}$ per hour. This satisfies PL d.

More detailed references

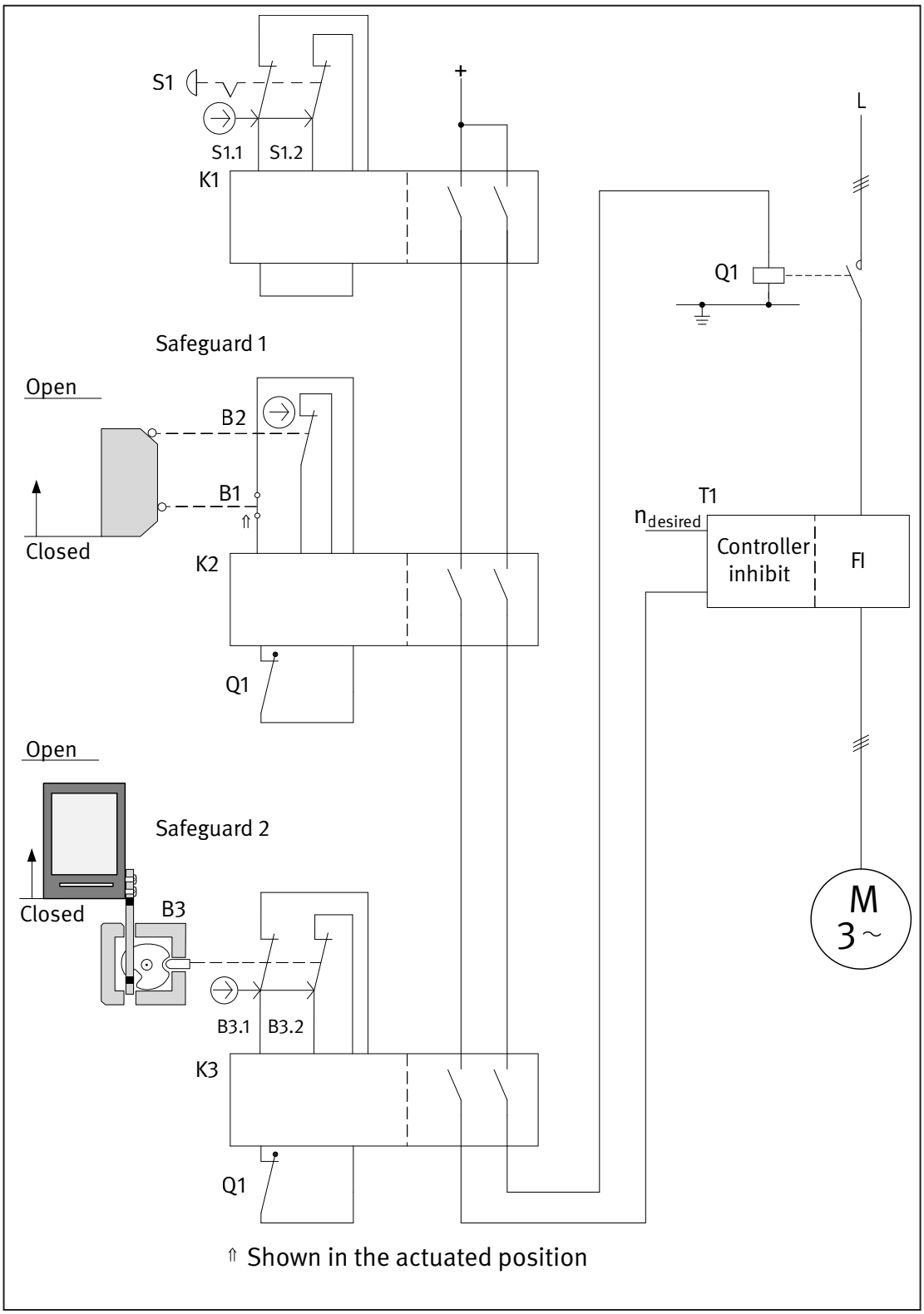
- ISO 15998: Earth-moving machinery – Machine control systems (MCS) using electronic components – Performance criteria and tests (04.08). ISO, Geneva, Switzerland 2008
- IEC 61784-3: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions (2016). IEC, Geneva, Switzerland 2016
- Grundsätze für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“ (GS-ET-26) (03.14). Published by: Fachbereich Energie Textil Elektro Medienerzeugnisse, Cologne, Germany 2014. www.dguv.de, Webcode: d14884
- SN 29500: Failure rates of components – Expected values. Published by: Siemens AG, Corporate Technology, Technology & Innovation Management, Munich, Germany 2004-2014

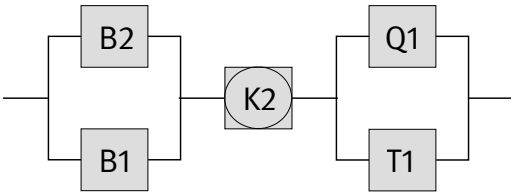
Figure 8.32:
Determining of the PL by means of SISTEMA



8.2.17 Cascading of guards by means of safety modules – Category 3 – PL d (Example 17)

Figure 8.33:
Cascading of guards by means of safety modules (emergency stop function, STO)





Safety functions

- Safety-related stop function, initiated by a guard: opening of the moveable guard initiates the safety function STO (safe torque off):
  Guard 1 with type 1 position switches (loading)
  Guard 2 with type 2 position switch (unloading)
- Emergency stop function, STO – safe torque off by actuation of the emergency stop device

Functional description

- Actuation of the emergency stop device S1 possessing two direct opening contacts causes hazardous movements or states to be de-energized redundantly via the safety module K1, by interruption of the control voltage of the contactor Q1 and selection of the controller inhibit of the frequency inverter T1.
- In addition, a hazard zone is guarded by two moveable guards (e.g. one each for loading and unloading). Opening of guard 1 is detected by two position switches B1/B2 employing a break contact/make contact combination, and evaluated in a central safety module K2. The latter can interrupt or prevent hazardous movements or states in the same way as K1. Guard 2 is monitored by a type 2 position switch with the contacts B3.1 and B3.2 and a safety module K3, also acting upon Q1 and T1.
- The safety function is retained in the event of a component failure.
- The majority of component failures are detected and lead to operating inhibition. The position switches B1 and B2 on guard 1 are monitored for plausibility in the associated safety module. The safety module also employs internal diagnostics measures.
- The electrical contacts B3.1 and B3.2 are monitored for plausibility in the associated safety module K3. This also employs internal diagnostics measures.
- Faults in the contactor Q1 are detected by means of mirror contacts and their readback in K2 and K3. Additional readback in K1 is not necessary, since a demand for the emergency stop function is much less frequent. A part of the faults in T1 are detected by the process. A small number of faults are not detected by the controller.
- Organizational measures ensure that the emergency-stop device is actuated at least once a year.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the guards is assured for actuation of the position switches.
- The emergency stop device S1 with the direct opening contacts S1.1 and S1.2 satisfies EN ISO 13850.
- The contacts of the position switches B2 and B3 have direct opening action in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the position switches B1, B2 and B3 are laid separately or with protection.
- The contactor Q1 possesses mirror contacts in accordance with IEC 60947-4-1, Annex F.

- The safety modules K1, K2 and K3 satisfy all requirements for Category 4 and PL e.
- The frequency inverter T1 has no integral safety function.

Remarks

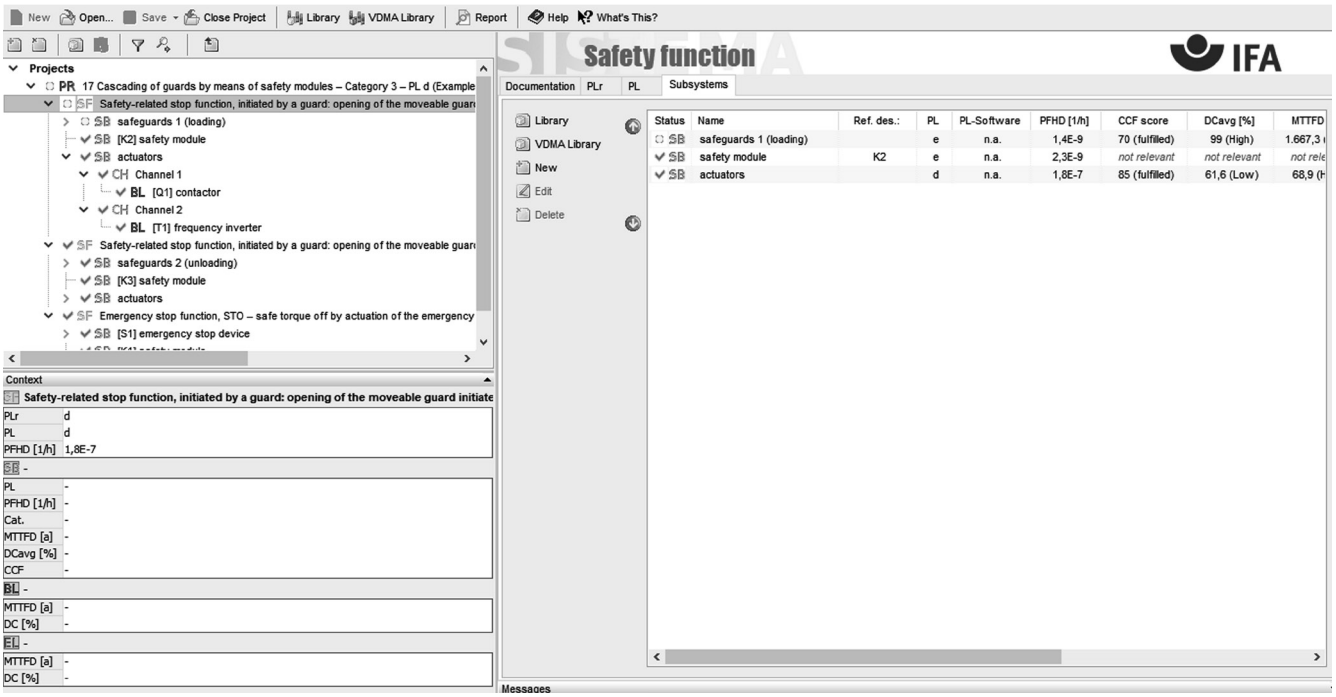
- The emergency stop function is a complementary protective measure to EN ISO 12100 [3].

Calculation of the probability of failure

- Each of the three safety functions can be presented in three subsystems. The safety-related block diagram shows the safety-related stop function by way of example for one of the safeguards, since only one guard is opened at any given time. A comparable safety function with a virtually identical calculation of the probability of failure applies to the second guard. Reasoning must be provided for fault exclusion for breakage of the actuator of the position switch B3.
  The probability of failure of the subsystems is calculated as follows.
- S1 is a standard emergency stop device to EN ISO 13850. A B_{10D} value of 100,000 switching cycles for each contact can be substituted for emergency stop devices, irrespective of the load [S]. Three actuations per year is assumed for n_{op}. In consideration of the total switching operations of Q1 caused by actuation of the safeguards, this value is not applied during further analysis of the two safety functions.
- $MTTF_D$ (guard 1, loading): switch B1 is a position switch with make contact. The B_{10D} is $1 \cdot 10^5$ switching cycles [M]. For the position switch B2 with direct opening action and roller actuation, the B_{10D} is $20 \cdot 10^6$ switching cycles [M]. At 220 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} is 21,120 cycles per year for these components, and the $MTTF_D$ is 47.3 years for B1 and 9,469 years for B2.
  For the contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical durability of 1,000,000 switching cycles [M]. If 50% of failures are assumed to be dangerous, the B_{10D} value is produced by doubling of the B_{10} value. Since Q1 is involved in both safety-related stop functions, double the value assumed above for n_{op} yields an $MTTF_D$ of 473 years. The $MTTF_D$ for the frequency inverter T1 is 20 years [M]. Altogether, the symmetrized $MTTF_D$ value per channel in the subsystem Q1/T1 is 68.9 years (“high”). The position switch B1 exhibits a limited operation time of 4.7 years. Its replacement in good time is recommended.
- $MTTF_D$ (guard 2, unloading): for the position switch B3 with separate actuator and the direct opening contacts B3.1 and B3.2, a B_{10D} value of 4,000,000 cycles [M] is stated for each contact. At 220 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} for these components is 21,120 cycles per year, and the $MTTF_D$ 1,893 years. For the contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to the electrical durability of 1,000,000 switching cycles [M]. Since 50% of failures are assumed to be dangerous, the B_{10D} value is produced by doubling of the B_{10} value. Since the contactor Q1 is involved in both safety-related stop functions (loading and unloading), doubling the value assumed for n_{op} yields an $MTTF_D$ of 473 years. The $MTTF_D$ for the frequency inverter T1 is 20 years [M]. Altogether, the symmetrized $MTTF_D$ value per channel in the subsystem Q1/T1 is 68 years (“high”).
- DC_{avg}: the DC of 99% for B1 and B2/B3 is based upon plausibility monitoring in K2/K3. This corresponds to the DC_{avg} for the subsystem. The DC of 99% for the contactor Q1 is derived from readback of the contact position in the safety modules. Fault detection by the process yields a DC of 60% for the frequency inverter T1. Averaging thus results in a DC_{avg} of 62% (“low”) for the subsystem Q1/T1. An adequate test rate of the emergency-stop device is assured (refer to the information in subclauses 6.2.14 and D.2.5.1).
- Adequate measures against common cause failure in the subsystems S1.1/S1.2, B2/B1, B3.1/B3.2 and Q1/T2 (65, 70 or 85 points): separation (15), protection against overvoltage etc. (15) and environmental conditions (25 + 10), well-tried components in B2/B1 (5), diversity in Q1/T1 (20)
- The subsystems B1/B2 and B3.1/B3.2 correspond to Category 4 with a high $MTTF_D$ and high DC_{avg} (99%). This results in an average probability of dangerous failure of $3.3 \cdot 10^{-8}$ per hour and $2.5 \cdot 10^{-8}$ per hour. The subsystem Q1/T1 satisfies Category 3 with a high $MTTF_D$ (68.9 years) and low DC_{avg} (62%). This results in an average probability of dangerous failure of $1.8 \cdot 10^{-7}$ per hour for the safety function of “position monitoring of interlocking devices (guard 1, loading)”.

- For the safety function of “position monitoring of interlocking devices (guard 2, unloading)”, the average probability of dangerous failure is $2.1 \cdot 10^{-7}$ per hour. This corresponds in both cases to PL d.
- The average probability of dangerous failure for the emergency stop function is $2.0 \cdot 10^{-7}$ per hour. This satisfies PL d.

Figure 8.34:
Determining of the PL by means of SISTEMA



8.2.18 Position monitoring of movable guards – Category 3 – PL d (Example 18)

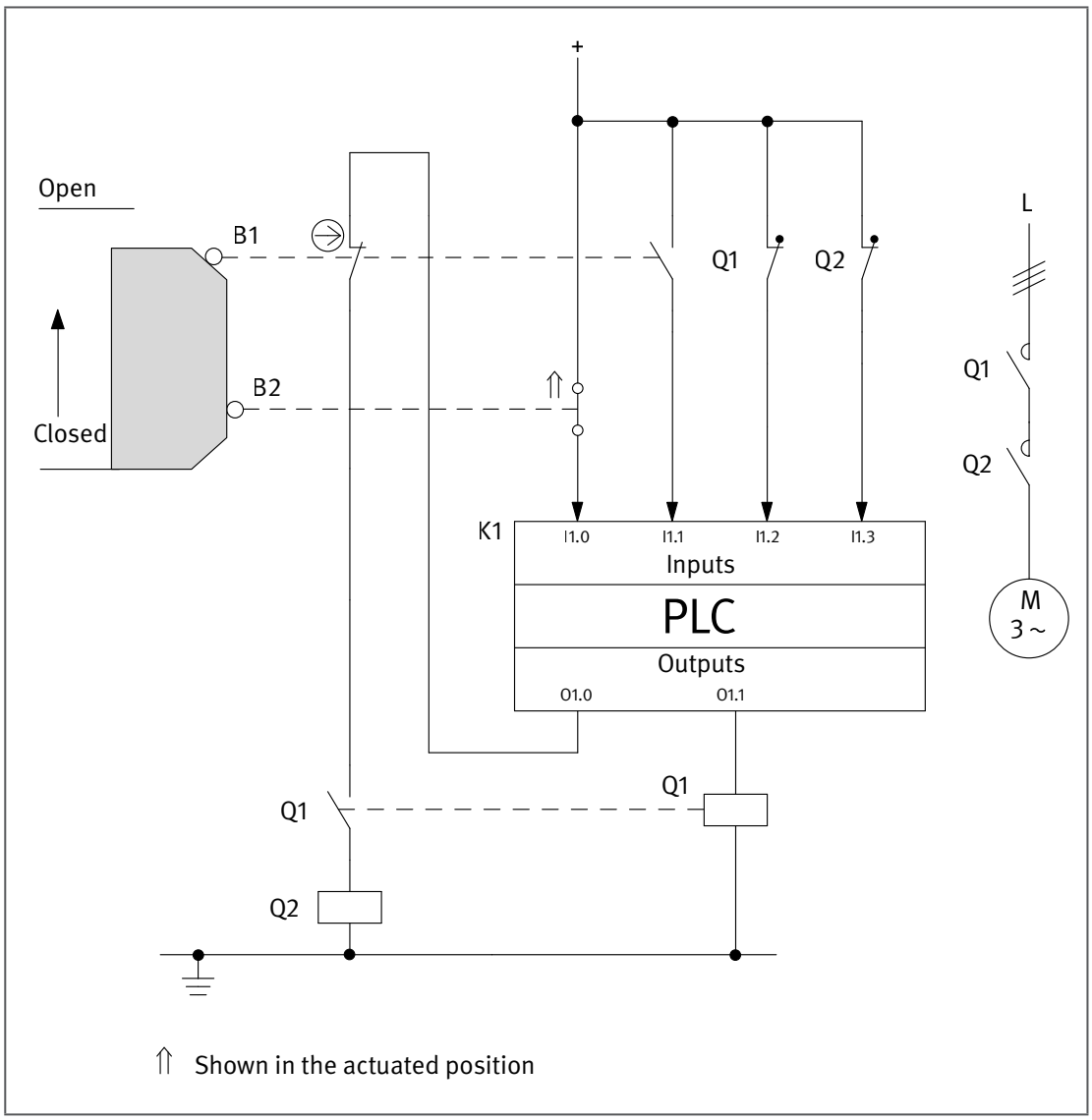


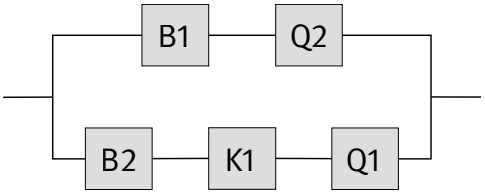
Figure 8.35: Redundant position monitoring of a movable guard in diversified technology (electromechanical and programmable electronic)

Safety function

- Safety-related stop function, initiated by a guard: opening of the movable guard (safety guard) initiates the safety function STO (safe torque off).

Functional description

- Opening of the movable guard (e.g. safety guard) is detected by two position switches B1 and B2 employing a break contact/make contact combination. The position switch B1 with direct opening contact actuates a contactor Q2, which interrupts/prevents hazardous movements or states when it drops out. The position switch B2 with make contact is read in by a standard PLC K1, which can bring about the same de-energization response by actuation of a second contactor Q1.
- The safety function is retained in the event of a component failure.
- The switching position of B1 is also read into the PLC K1 by means of a make contact, and is compared for plausibility with the switching position of B2. The switching position of the contactors Q1 and Q2 is likewise monitored in K1 by mirror contacts. Component failures in B1, B2, Q1 and Q2 are detected by K1 and lead to operating inhibition owing to the dropping-out of Q1 and Q2. Faults in the PLC K1 are detected only by the function (fault detection by the process).



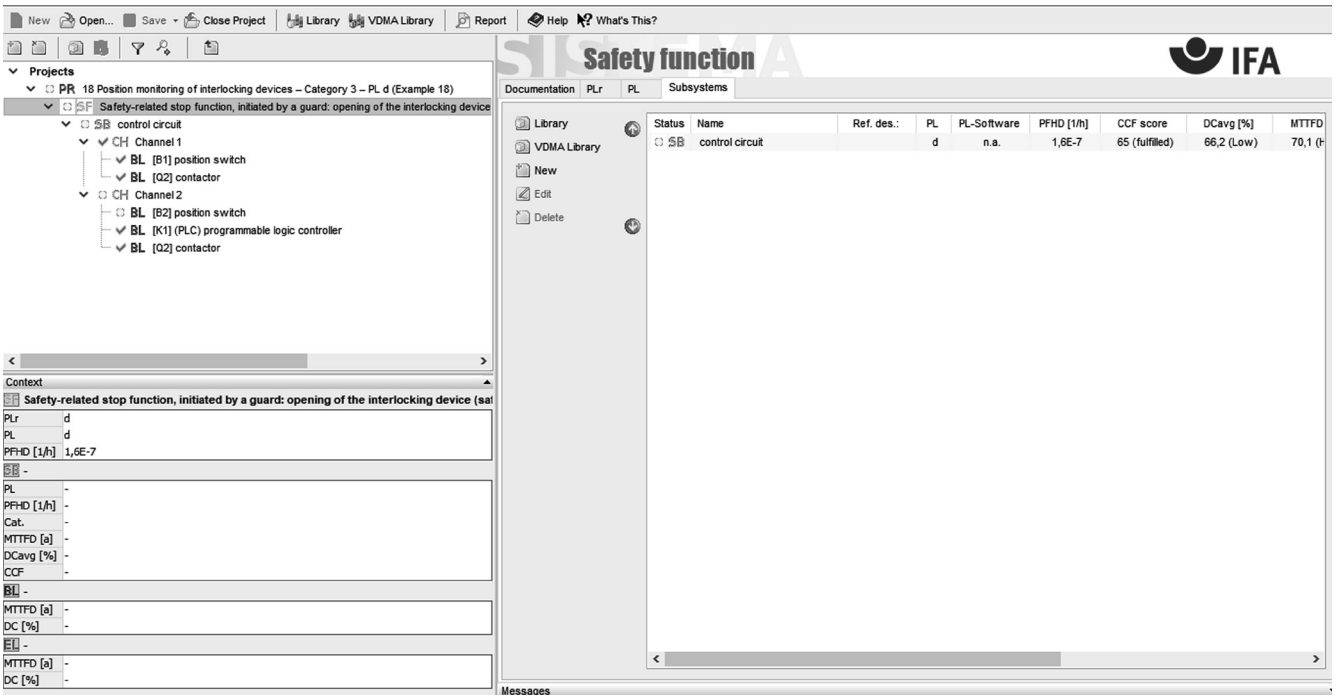
Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the guard is assured for actuation of the position switch.
- B1 is a position switch with a dirct opening contact in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the position switches are laid separately or with protection.
- Faults in the actuating and operating mechanism are detected by the use of two position switches differing in the principle of their operation (break and make contacts).
- Q1 and Q2 possess mirror contacts in accordance with IEC 60947-4-1, Annex F. The PLC K1 satisfies the normative requirements described in subclause 6.3.

Calculation of the probability of failure

- $MTTF_D$: the position switch B1 with roller actuation exhibits a B_{10D} of $20 \cdot 10^6$ switching cycles [M]. For position switch B2 (make contact), the B_{10D} is 100,000 switching cycles [M]. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} for these components is 5,840 cycles per year and the $MTTF_D$ is 34,246.6 years for B1 and 171 years for B2. For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical durability of 1,300,000 switching cycles [M]. On the assumption that 50% of failures are dangerous, the B_{10D} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_D$ of 4,452 years for Q1 and Q2. An *MTTF* value of 15 years [M] is substituted for the PLC, doubling of which results in an $MTTF_D$ value of 30 years. The combination of B1 and Q2 results in an $MTTF_D$ of 3,940 years for the first channel; B2, K1 and Q2 contribute to an $MTTF_D$ of 25.4 years in the second channel. Altogether, the $MTTF_D$ value symmetrized over both channels is 70 years per channel (“high”). The position switch B2 exhibits a limited operation time of 17.1 years. Its replacement in good time is recommended.
- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the two switching states in the PLC K1. The *DC* of 99% for the contactors Q1 and Q2 is derived from readback via mirror contacts, also in K1. Owing to the possibility of fault detection by the process, a *DC* of 60% is assumed for K1. Averaging thus produces a DC_{avg} of 66.2% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements satisfies Category 3 with a high $MTTF_D$ (70 years) and low DC_{avg} (66.2%). This results in an average probability of dangerous failure of $1.6 \cdot 10^{-7}$ per hour. This satisfies PL d.

Figure 8.36:
Determining of the PL by means of SISTEMA

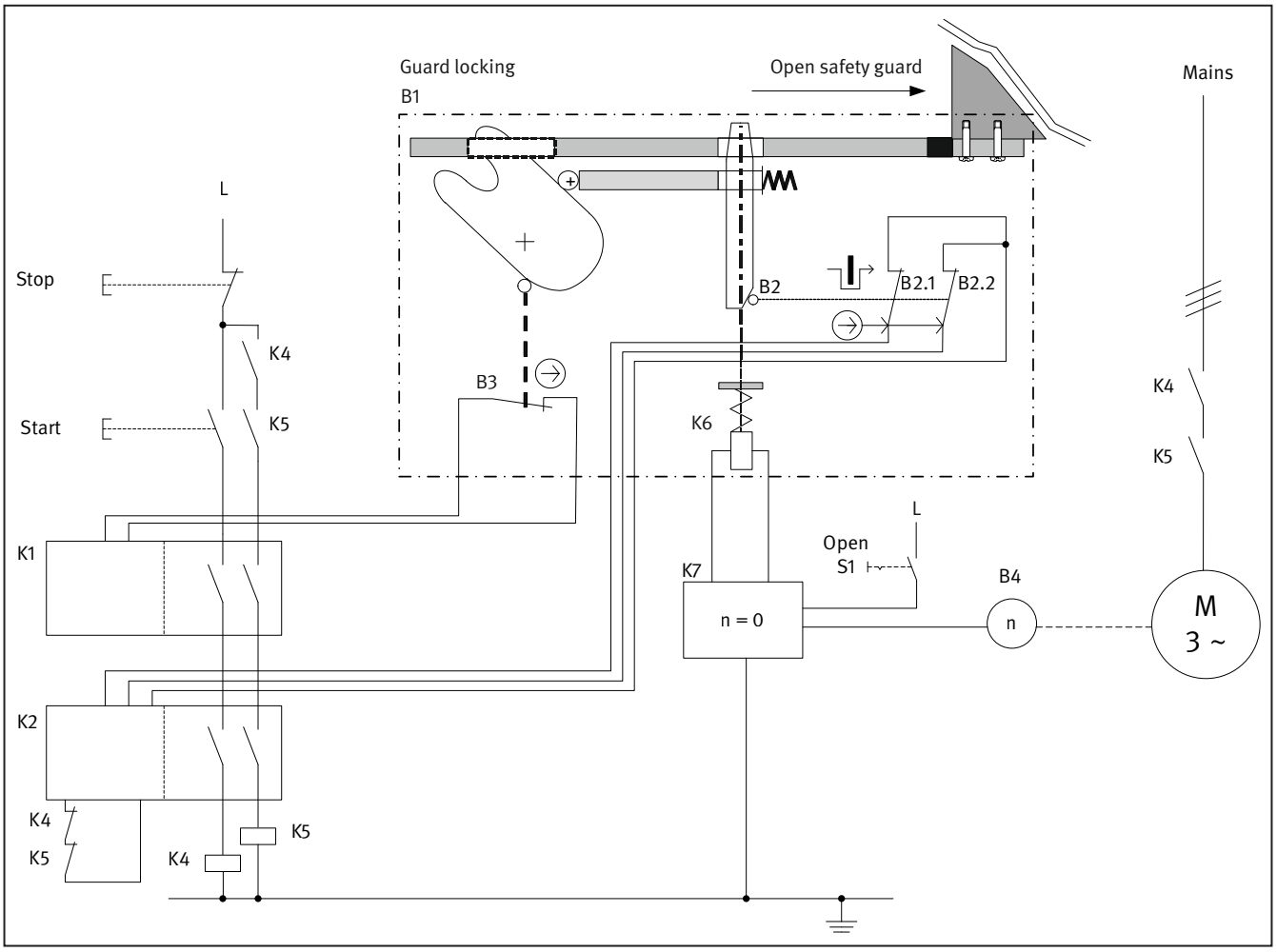


8.2.19 Interlocking device with guard locking – Category 3 – PL d (Example 19)

Changes with respect to the second edition (BGIA Report 2/2008e):

The example was comprehensively revised.

Figure 8.37:
Position monitoring of an interlocking device by means of guard locking

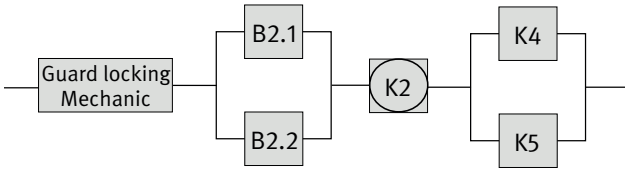


Safety functions

- Guard locking (PL d): access to a hazardous movement is prevented by means of a guard door with guard locking.
- Release of guard locking: opening of the safety guard is possible only once the motor has come to a halt.

Functional description

- Access to a hazardous movement is prevented by a guard door with guard locking until the moving part has come to rest (guard locking safety function). The door is held closed by a spring-actuated pin (the locking element) of a solenoid that prevents the actuator being withdrawn from the switch head until the locking solenoid is actuated.
- According to the manufacturer, the guard locking has a fail-safe locking element.



- When the guard door is open, unexpected start-up of the motor is prevented in two channels by the interlock safety function (not shown).
- The pin of the locking element acts directly upon the direct opening contacts B2.1 and B2.2, which are connected to a safety module K2.
- The hazardous movement can be started only when the guard door is closed and guard locking activated, since the enabling circuits of K1 and K2 are connected in series.
- Actuation of the stop button causes the contactor relays K4 and K5 to drop out. Once the motor has reached a standstill, guard locking can be opened by actuation of the latching switch S1 (safety function: release of guard locking). The stationary state of the motor is detected by two-channel monitoring B4, K7.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- B1 is an electromechanical guard locking device with fail-safe locking element.

  Fault exclusion can be assumed for the mechanical components of the guard locking device, including mechanical failure of the locking element and the actuator, when the following conditions are met:

  – Use in accordance with the operating manual, in particular the installation instructions and technical data (e.g. actuating radius, actuating velocity)
  – Prevention of working loose
  – The static forces on the guard locking device are lower than the locking force stated on the data sheet
  – No dynamic forces arise, since current flows through the unlocking solenoid only when the guard door is closed; refer in this context also to DGUV Informative publication 203-079 concerning the selection and fitting of interlocking devices
  – The device is not used as a mechanical stop
  – The actuator is mounted such that it cannot be removed
  – Regular maintenance is performed
  – Positive coupling following fitting
  – Adequate mechanical strength of all mounting and functional elements
  – Dropping of the door does not lead to the actuator being used outside the range specified by the manufacturer
  – Damage that could be caused by foreseeable external influences (such as the ingress of dirt or dust; mechanical shock) is prevented by the form of mounting or need not be anticipated under the given conditions of use
- B2.1 and B2.2 are switching elements of the guard locking device with direct opening contacts in accordance with IEC 60947-5-1, Annex K. The manufacturer states a B_{10D} value for the purposes of calculation.
- B3 is a direct opening contact in accordance with IEC 60947-5-1, Annex K, and has the purpose of monitoring the door position.
- K4 and K5 possess mechanically linked contacts to IEC 60947-5-1, Annex L.
- The safety modules K1 and K2 detect cross-circuits and shorts to earth, and satisfy the requirements of Category 4, PL d of EN ISO 13849-1.
- The stationary state monitor consists of the sin/cos encoder B4 and the standstill monitor K7. Both satisfy the requirements of Category 4 and PL e.

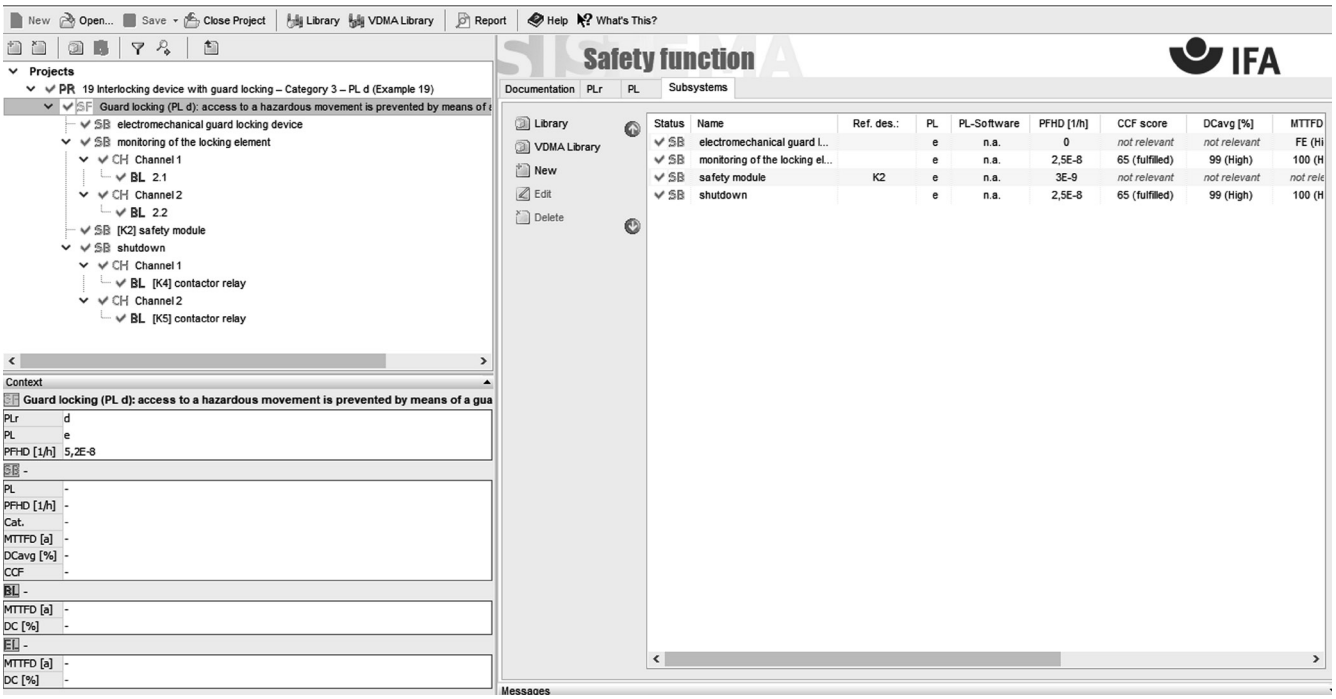
Calculation of the probability of failure

- Fault exclusion can be assumed for the mechanism of the guard locking device B1.
  Note: On guard locking devices with fail-safe locking element, fault exclusion is possible only in accordance with the manufacturer‘s information.
- The manufacturer states a B_{10D} value of 3,000,000 cycles [M] each for the switching elements B2.1 and B2.2. At actuation once every 10 minutes, n_{op} is 17,520 cycles per year and the $MTTF_D$ is 1,712 years.
- The contactor relays K4 and K5 have a B_{10D} value of 1,000,000 cycles [M]. At actuation once every 10 minutes, n_{op} is 17,520 cycles per year and the $MTTF_D$ is 570 years.
- The manufacturer states a PFH_D of $3.0 \cdot 10^{-9}$ per hour [M] for the safety module K2.
- DC_{avg}: the *DC* of 99% for the contacts B2.1 and B2.2 is attributable to direct monitoring in K2. The *DC* of 99% for K4 and K5 is attributable to direct monitoring in K2 by means of mechanically linked contacts. Averaging results in a DC_{avg} of 99% (“high”).
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- For the safety function “access to a hazardous movement is prevented by means of a guard door with guard locking”, the average probability of dangerous failure PFH_D is $5.2 \cdot 10^{-8}$ per hour. This satisfies PL e. However, since the position switch (B2) for monitoring of the locking element and the associated actuating mechanism is present only once, the PL is limited to d.
- For the safety function “release of guard locking: opening of the guard is possible only once the motor has come to a halt”, the probability of failure is determined only by the sin/cos encoder B4 and the standstill monitor K7. According to the manufacturer‘s information, the PFH_D for the sin/cos encoder B4 is $1.2 \cdot 10^{-8}$ per hour. A PFH_D of $2.0 \cdot 10^{-8}$ per hour is stated for the standstill monitor K7 [M]. The *PFH* of this safety function is $3.2 \cdot 10^{-8}$ per hour.

More detailed reference

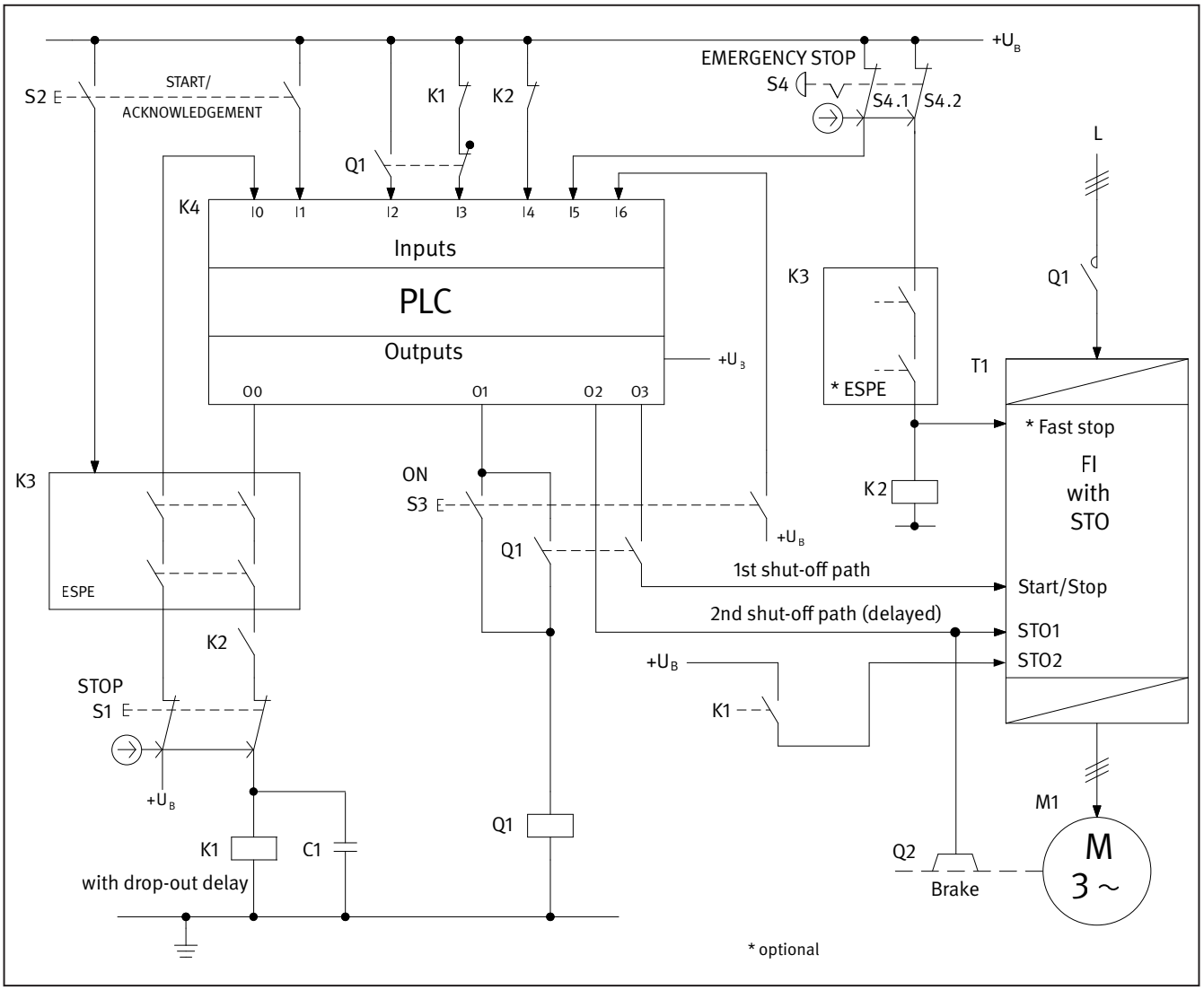
- DGUV Informative publication 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen 203-079 (12/2015). Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin, Germany 2015. http://publikationen.dguv.de/dguv/pdf/10002/203-079.pdf
- Principles of testing and certification for interlocking devices with solenoid guard-locking. GS-ET-19E (2015). www.bgetem.de, Webcode: 12700341

Figure 8.38:
Determining of the PL by means of SISTEMA



8.2.20 Safe stopping of a PLC-driven drive – Category 3 – PL d (Example 20)

Figure 8.39:
Safe stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command or following tripping of a protective device (in this case, an ESPE)

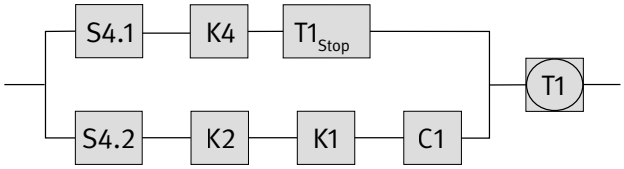


Safety function

- Safety-related stop function: following a stop command, an emergency stop command or tripping of a protective device, the drive is halted (SS1-t – safe stop 1, STO is activated with a time delay).

Functional description

- The hazardous movement is interrupted redundantly if either the stop button S1 or the protective device K3 – shown in the circuit diagram as electro-sensitive protective equipment (ESPE) – is activated. The drive is halted in an emergency following actuation of the emergency stop device S4. In all three cases, stopping is initiated via the output O3 of the PLC K4 by deactivation of the “Start/Stop” input on the frequency inverter (FI) T1. Redundantly to this process, the input “STO2” on T1 is deactivated by de-energization of the contactor relay K1 (with the use of the capacitor C1 for drop-out delay). A further shut-off path exists on the “STO1” input on T1 via the output O2 of the PLC K4: this also causes the brake Q2 to be applied. The first shut-off path is thus implemented directly by the PLC K4; conversely, the second shut-off path employs relay technology and delayed drop-out. The timer settings for O2 in the PLC program and for K1 are selected such that the machine movement is halted even under unfavourable operating conditions.



- Should a “fast stop” input with a particularly short deceleration phase be available on the FI, an ESPE may be connected to it if desired, as shown on the circuit diagram. This option is not considered further below.
- In the event of failure of the PLC K4, the “Start/Stop”, “STO1” or “STO2” frequency inverter inputs, the contactor relay K1 with drop-out delay or the contactor relay K2, stopping of the drive is nevertheless assured, since two mutually independent shut-off paths are always present. Failure of the contactor relays K1 or K2 to drop out is detected – at the latest before renewed start-up of the machine movement – by the feedback of the mechanically linked break-contact elements to the PLC inputs I3 and I4.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Owing to the use of an FI with STO, the contactor Q1 is no longer absolutely essential for de-energization of the supply voltage. The FI must be suitable for ramping up and braking.
- For comparison of command disconnection on the “STO1/STO2” inputs on the FI, a duration of sufficient length is selected to allow for variation in the drop-out delay of K1.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contacts of the stop button S1 and of the emergency stop device S4 are direct opening contacts in accordance with IEC 60947-5-1, Annex K.
- The standard component K4 is employed in accordance with the information in subclause 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL c (downgraded owing to diversity) and the guidance in subclause 6.3.10.
- If the brake Q2 is provided for functional reasons only, i.e. it is not involved in performance of the safety function, it is disregarded in the calculation of the probability of failure, as in this example. A condition for this procedure is that coasting down of the drive in the event of a failure of the stop function, in which case de-energization is effected by means of STO alone, must not be associated with an unacceptably high residual risk. The involvement of a brake in performance of the safety function in conjunction with the use of an FI is described in Example 23 (revolving door control).
- The ESPE K3, for example in the form of a light curtain, satisfies the requirements for Type 4 to IEC 61496-1 and IEC 61496-2, and for PL e.

Calculation of the probability of failure

- The probability of failure PFH_D of safe stopping initiated by the emergency stop device S4 or by the ESPE is calculated. The “fast stop” function of the FI and the facility for de-energization of the power supply to the FI via Q1 are not considered in the calculation of the probability of failure of the safety function.
- The FI T1 with STO is available for purchase as a safety component; its probability of failure is added at the end of the calculation ($1.5 \cdot 10^{-8}$ per hour [M]). The stop function of the FI is modelled in the first channel of the block diagram (T1stop). The FI with STO would in fact be modelled in the second channel of the block diagram; a model with a turnkey safety component including PFH_D in a single channel is however not covered by the standard. The FI T1 and its STO function are therefore considered as a single subsystem. This estimation therefore errs on the safe side.

Safe stop initiated by the emergency stop device S4:

- $MTTF_D$: the following $MTTF_D$ values are estimated: 50 years for K4 and 100 years for the stop function T1stop of the FI [E]. At a B_{10D} value of 100,000 cycles [S] each and an n_{op} of 12 cycles per year, the $MTTF_D$ for S4.1 and S4.2 is 83,333 years. At a B_{10D} value of 400,000 cycles [S] and at 240 working days, 8 working hours and a cycle time of 6 minutes, the n_{op} for K1 is 19,200 cycles per year and the $MTTF_D$ 208 years. At a B_{10D} value of 400,000 cycles [S] and actuation once daily on 240 working days, the $MTTF_D$ for K2 is 16,667 years. The capacitor C1 is considered in the calculation with an $MTTF_D$ of 45,662 years [D]. These values yield a symmetrized $MTTF_D$ of each channel of 72 years ("high").
- DC_{avg}: fault detection by the process results in a *DC* of 60% for T1stop, and in combination with internal self-tests in a *DC* of 60% for K4. Testing of the timing element with the FI de-energized results in a *DC* of 99% for K1. Testing of the timing element with the FI de-energized in combination with fault detection by comparison in the FI at a demand of the safety function results in a *DC* of 90% for C1. For S4.1, S4.2 and K2, *DC* is 99% owing to plausibility testing in K4. An adequate test rate of the emergency-stop device is assured (refer to the information in subclauses 6.2.14 and D.2.5.1). The averaging formula for DC_{avg} returns a result of 65% ("low").
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements satisfies Category 3 with a high $MTTF_D$ of each channel (72 years) and a low DC_{avg} (65%). Together with the FI T1, this results in an average probability of dangerous failure PFH_D of $1.7 \cdot 10^{-7}$ per hour. This satisfies PL d.

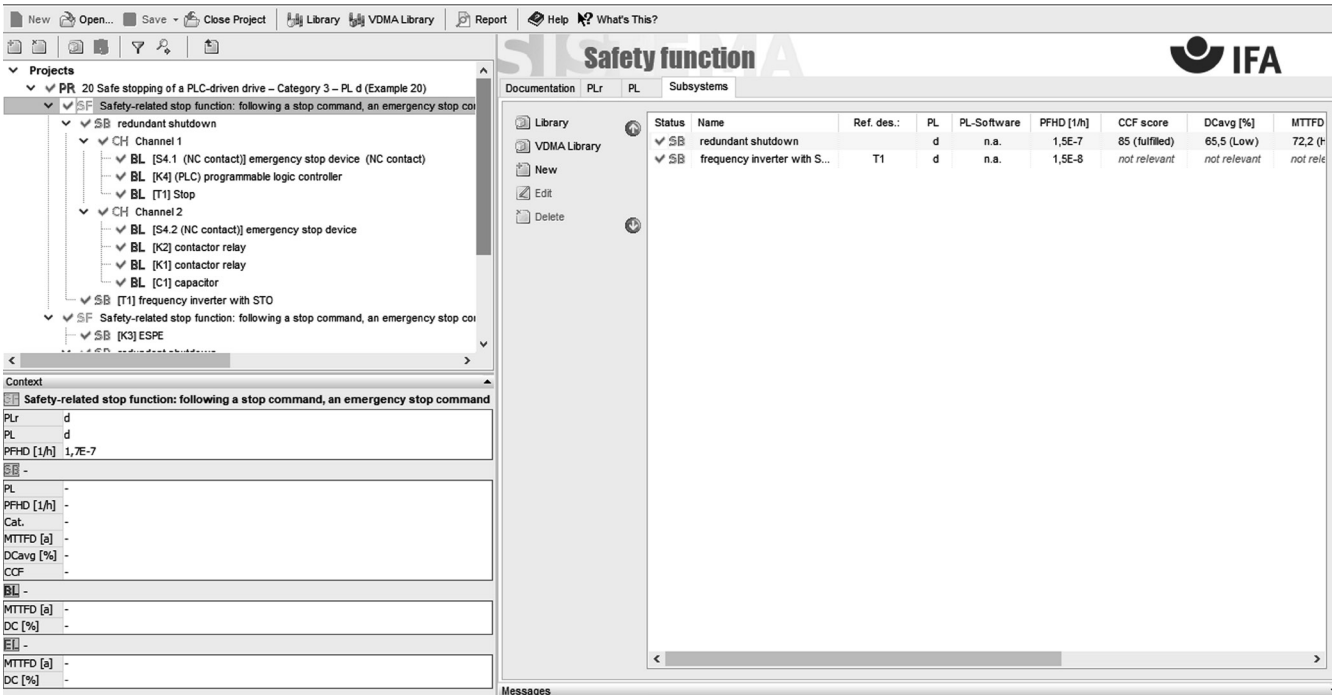
Safe stop initiated by the ESPE K3:

- The ESPE K3 is available as a commercial safety component. Its probability of failure PFH_D is $3.0 \cdot 10^{-8}$ per hour [M], and is added at the end of the calculation.
- The probability of failure of the "PLC/electromechanical" two-channel structure is calculated using the same $MTTF_D$ and *DC* values as above. The component K2 however is not involved in performance of this safety function. The results are: an $MTTF_D$ for each channel of 72 years ("high") and a DC_{avg} of 65% ("low"). For Category 3, this yields an average probability of dangerous failure PFH_D of $1.5 \cdot 10^{-7}$ per hour. The overall probability of failure is determined by addition, resulting in a PFH_D of $2.0 \cdot 10^{-7}$ per hour. This also satisfies PL d.

More detailed references

- *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld, R.*: Safe drive controls with frequency inverters. IFA Report 4/2018e. 3rd ed. Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin, Germany 2019 (will be published in Summer 2019). www.dguv.de/ifa, Webcode: e635980
- IEC 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (2012) and Corrigendum 1 (2015). IEC, Geneva, Switzerland 2012/2015
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (2013). IEC, Geneva, Switzerland 2013
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (2016). IEC, Geneva, Switzerland 2016

Figure 8.40:
Determining of the PL by means of SISTEMA



8.2.21 Safely limited speed – Category 3 – PL d (Example 21)

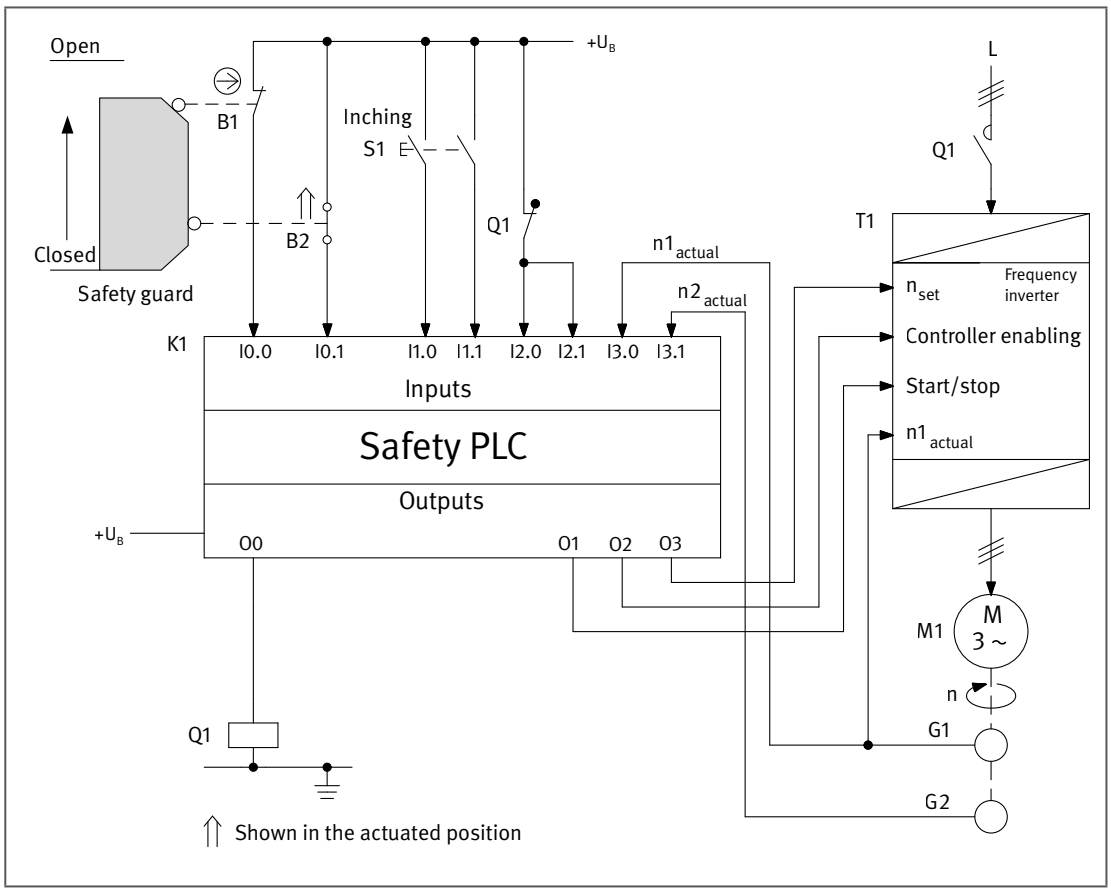


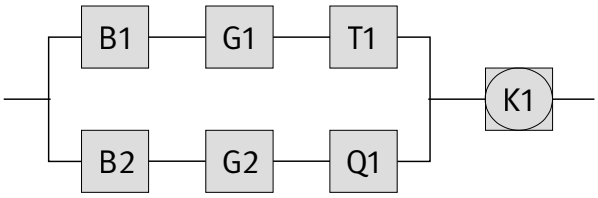
Figure 8.41: Safely limited speed with the safety guard open, with desired/actual value comparison and defined speed limit value within a safety PLC

Safety function

- Safely limited speed (SLS): when the safety guard is open, exceeding of a permissible speed is prevented.

Functional description

- This example shows implementation of the SLS safety function with a frequency inverter without integrated safety function. The SLS safety function is used for example for inching mode during servicing tasks.
- A hazardous movement is safely prevented or interrupted when the safety guard is open. Opening of the safety guard is detected by two position switches B1 and B2 employing a break-contact/make-contact element combination. When the pushbutton S1 is actuated, a movement at a safely limited speed (inching mode) is initiated by means of the safety PLC K1. The two processing channels within the PLC each process a set limit value. The actual value of the limited speed on the inputs I3.0 and I3.1 of K1 is monitored by two separate rotary encoders G1 and G2. Each channel of the PLC performs the desired/actual speed comparison independently. Should the speed not be reduced successfully to the limited value by means of T1, K1 can initiate a halt by blocking the start/stop signal and servo enable on the frequency inverter. The power supply to T1 is also interrupted by the mains contactor relay Q1 after a programmed timeout.
- The two-channel safety PLC K1 performs internal fault detection. Should one processing channel fail, the remaining (i.e. functioning) processing channel reduces the speed of the frequency inverter T1 and de-energizes the mains contactor relay Q1. A failure of the frequency inverter that could for example lead to unexpected start-up, continued running or an increase in the speed is detected by separate monitoring of the speed by the rotary encoders G1 and G2 in the two processing channels. Failure of the mains contactor relay Q1 to drop out is detected by the break-contact element connected to both processing channels (inputs I2.0 and I2.1 of K1), and leads both to blocking of the start/stop signal and of servo enable on the inverter by both processing channels.



Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the safeguard is assured for actuation of the position switch.
- The position switch B1 features direct opening action in accordance with IEC 60947-5-1, Annex K. The position switch B2 also complies with IEC 60947-5-1.
- The contactor Q1 possesses a mirror contact in accordance with IEC 60947-4-1, Annex F.
- The supply conductors to the position switches are laid either separately or with protection against mechanical damage.
- For the “safely limited speed” safety function, a fault exclusion is assumed for the fault condition of encoder shaft breakage (G1/G2). Details of the possibility of a fault exclusion can be found for example in IEC 61800-5-2, Table D.8, and GS-IFA-M21.
- The standard components G1 and G2 (where relevant for the rotary encoders) and T1 are employed in accordance with the information in subclause 6.3.10.
- The safety component K1 satisfies all requirements for Category 3 and PL d. The software (SRASW) is programmed in accordance with the requirements for PL d and the information in subclause 6.3.10.
- It is assumed that each output of the safety PLC is actuated by both processing channels of the PLC and that the analog output 03 is monitored by two channels.

Calculation of the probability of failure

- The SRP/CS is divided into the two subsystems sensor/actuator and PLC. For the PLC subsystem, a tested safety PLC suitable for PL d is employed. This PLC‘s probability of failure of $1.5 \cdot 10^{-7}$ per hour [E] is added at the end of the calculation for the sensor/actuator subsystem. For the composition of the block diagram, refer also to Figure 6.14 and the relevant information in the associated text. The probability of failure for the sensor/actuator subsystem is calculated below.
- $MTTF_D$: at 240 working days, 8 working hours and a cycle time of one hour, n_{op} is 1,920 cycles per year. A B_{10D} value of 20,000,000 cycles [S] is assumed for the position switch B1 owing to its direct opening action; the associated $MTTF_D$ value is 104,166.7 years. Owing to the defined control current (low load; the mechanical durability of the contacts is the determining factor), a B_{10D} value of 100,000 cycles [E] is assumed for the make-contact element, which is opened by spring force (see also Table D.2), and therefore an $MTTF_D$ of 520 years. The contactor Q1, with a B_{10D} value of 400,000 cycles, switches operationally only once daily, equating to an n_{op} of 240 cycles per year and an $MTTF_D$ of 16,667 years. The following manufacturer‘s values are available: an $MTTF_D$ of 100 years for T1 and an $MTTF_D$ of 190 years for G1/G2 [M]. These values yield a symmetrized $MTTF_D$ of each channel of 84 years (“high”).
- DC_{avg}: a DC of 99% is assumed for each of the components used. For the position switches and the rotary encoders, this value is based upon cross monitoring of input signals in K1. For the frequency inverter T1, the speed is monitored in the safety PLC via the two rotary encoders, and fault detection is provided by the process; the main contactor relay Q1 is monitored directly by the PLC. These values yield a DC_{avg} of 99% (“high”).

- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)

- The sensor/actuator subsystem satisfies Category 3 with a high $MTTF_D$ of each channel (84 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure PFH_D of $3.0 \cdot 10^{-8}$ per hour. This satisfies PL e. A PL_r of d is thus surpassed, which with the required two-channel design of the hardware with few components, the use of B_{10D} values in accordance with the standard, a *DC* of "high" and a "moderate" rate of operations will virtually always be the case.

- The overall probability of failure is determined by addition of the probability of dangerous failure of K1 ($1.5 \cdot 10^{-7}$ per hour) and is $PFH_D = 1.8 \cdot 10^{-7}$ per hour. This satisfies PL d.

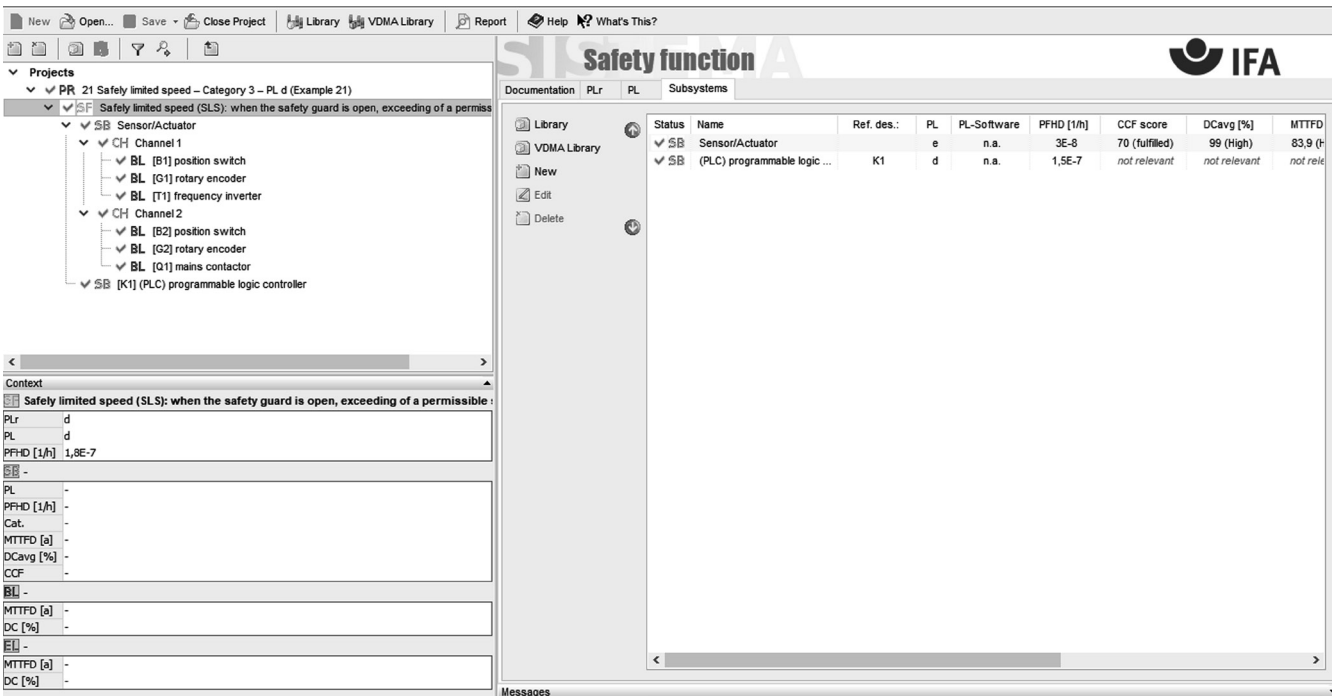
More detailed references

- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (2016). IEC, Geneva, Switzerland 2016

- Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit (GS-IFA-M21). Published by: Institut für Arbeitsschutz der DGUV, Prüf- und Zertifizierungsstelle im DGUV Test, Sankt Augustin, Germany 2015. www.dguv.de, Webcode: d11973

- EN 1010-1: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (2004) + A1 (2010)

Figure 8.42
Determining of the PL by means of SISTEMA



8.2.22 Muting of a protective device – Category 3 – PL d (Example 22)

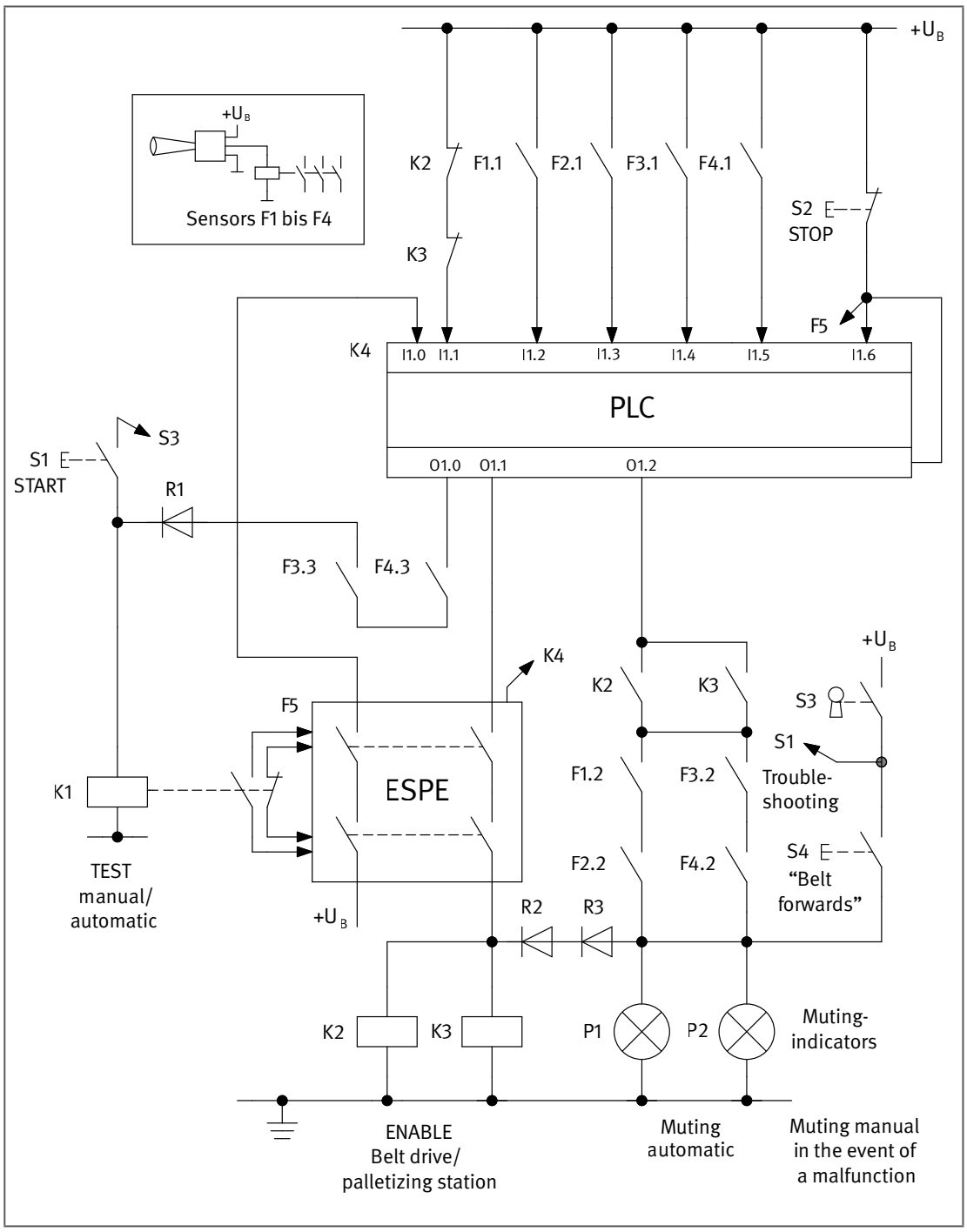
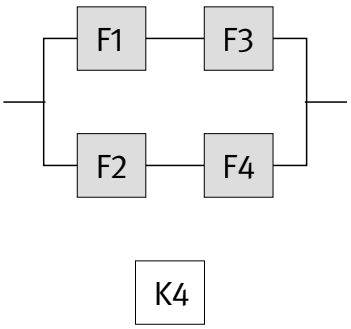


Figure 8.43: Muting of a protective device at the discharge point from a palletizer station controlled by a PLC

Safety function

- Muting function: temporary muting (bypassing) of a protective device as a function of the process. Further safety functions, such as safeguarding of access to the palletizer station or the start/restart interlock, are not dealt with in detail below.



Functional description

- A triple-beam light barrier (ESPE) F5 of Type 4 to IEC 61496 safeguards the access to the discharge point of the palletizer station. The light barrier embodies the additional functions of start interlock and restart interlock, which are implemented by means of two antivalent inputs. Disabling of the start interlock of the light barrier is coupled to the start command for the belt drive, i.e. energization of the palletizer station, and is initiated by picking-up and subsequent dropping-out of the contactor relay K1 in response to actuation and release of the start button S1. A condition for a valid start command is that the contactor relays K2 and K3 have dropped out (queried via input I1.1) and that the start interlock has been cancelled (queried via input I1.0). Output O1.1 is set as a result.
- Four infrared light sensors F1 to F4 (for arrangement, refer also to Figure 8.44) are incorporated for control of the muting process. Via the inputs I1.2 to I1.5, the PLC monitors the actuation sequence of the four infrared light sensors via the sensor‘s contacts F1.1 to F4.1, in consideration of two programmed time settings. The muting function is implemented only in the output circuit of the PLC (output O1.2), independently of the output circuit of the light barrier F5. The muting contacts F1.2 and F2.2/F3.2 and F4.2, connected in series, are connected by OR logic via the diodes R2 and R3 respectively with the “enabling” function implemented by the contactor relays K2 and K3.

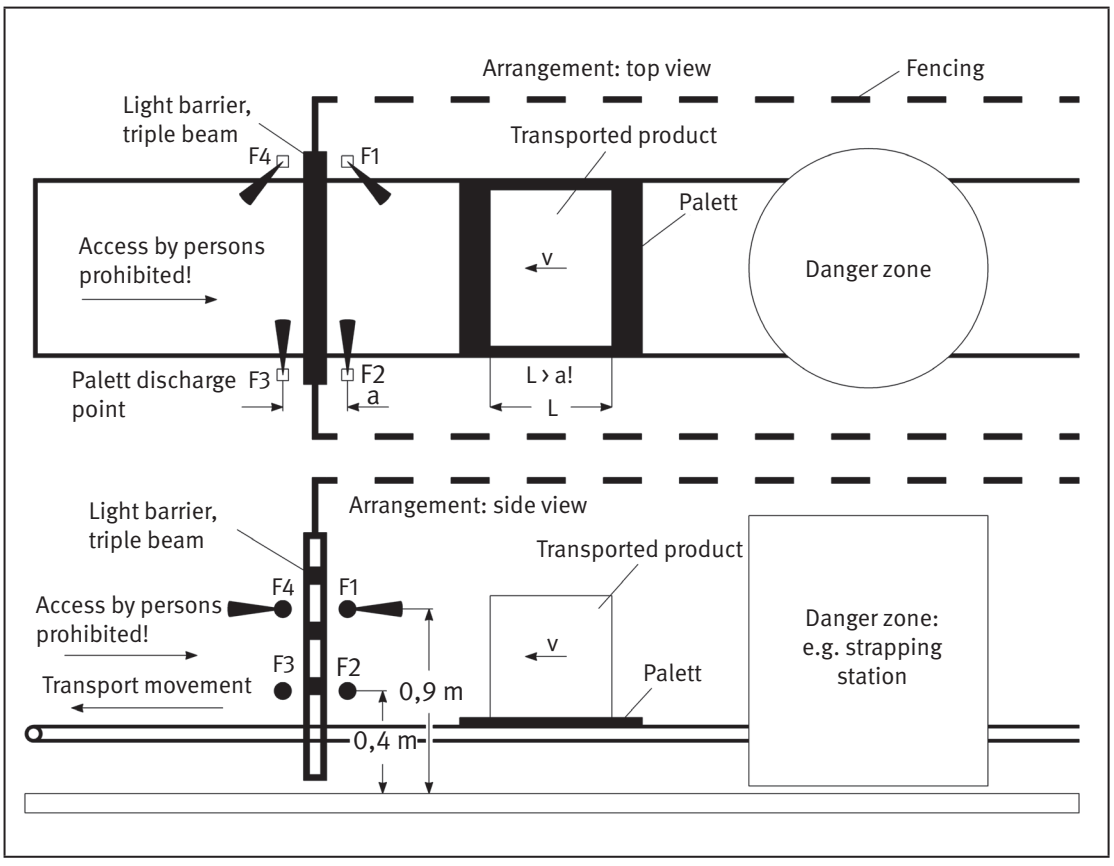


Figure 8.44: Palletizer station with automatic control – principle of safeguarding of the pallet discharge point by means of a light barrier, and arrangement of the muting sensors F1 to F4

- R2 and R3 cause the muting function to be displayed correctly, and isolate the activated enabling output from the muting displays P1/P2 when the muting function is not active. Faults in R2 or R3 cannot lead to unexpected muting (i.e. dangerous failure of the muting function).
- Should the voltage break down and be restored, or the light barrier F5 be interrupted and the muting function not be active, the contactor relays K2 and K3 are de-energized. The absence of latching-in under these circumstances prevents them from picking up again should the muting circuits be closed again. The installation can be restarted only by disabling of the restart interlock, i.e. by deliberate actuation and release of the start button S1.
- For starting or restarting as intended, for example following a fault on the installation, the key switch S3 must be actuated. In the event of an outage, the operator can eject a pallet from the detection zone of the light barrier and the muting sensors by means of the hold-to-run button S4.
  For smooth progress of the pallets through the discharge opening, two time settings in the PLC program must be matched to the velocity of the transport movement:
  – The time setting T1 determines the maximum period within which – following activation of the sensor F1 – the sensor F2 must be activated and the muting function thus initiated by the transported product.
  – Time setting T2 begins with renewed clearing of the sensor F2. T2 must be selected such that when the detection zone of the light barriers becomes clear again, K1 is energized and de-energized again before sensor F3 is deactivated by the transported product and the muting function thereby terminated.
- Failure of the contactor relays K2 and K3 to drop out is detected at the latest before the belt drive/the palletizer station start up again, owing to the feedback of the mechanically linked break contacts to the PLC input I1.1. Failure of K1 is detected at the next discharge of a pallet.
- Unintended start-up of the belt drive/palletizer station by themselves in the event of the loss and subsequent restoration of power or a failure of the standard PLC is prevented by the function of the start-up and restart interlock. The PLC can disable the restart interlock only immediately after the pallet has passed the light barrier, i.e. whilst sensors F3 and F4 are still activated.
- The failure of individual muting sensors is either detected directly by the PLC program (owing to monitoring for proper completion of activation and deactivation), or becomes evident by operating inhibition during transport of the pallet.
- Failure of the hold-to-run button S4, which is used only for the clearing of faults (manual muting), is detected directly by the operator.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The contactor relays K1 to K3 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The supply conductors to the light barrier F5 and the hold-to-run button S4 are laid such that short-circuits between individual conductors (including to the supply voltage) can be excluded.
- The control components S1 to S4 are located at a point outside the hazard zone and from where the hazard zone can be viewed.
- The muting state is displayed by two lights clearly visible to the operator at the access point to the hazard zone.
- The muting sensors F1 to F4 are standard components and are engineered with electronic hardware without software.

Remarks

- Example enabling arrangement for automated material discharge on safeguards of access points to palletization and depalletization equipment, transfer stations, strapping or wrapping machines. The same principle can be used for access points for material infeed.

- When muting sensors are used that employ microcontrollers and software that have not been subjected to a safety analysis by the manufacturer (i.e. the requirements imposed upon safety-related embedded software are not met), components featuring diverse technology must be employed in the two channels in the intended PL of d.
- In accordance with EN 415-4, it can be assumed that the unobserved access of persons through feed or discharge openings is prevented sufficiently reliably when requirements including the following are met:
  – Use of a two-beam or three-beam light barrier in consideration of the necessary installation height (with the access point open/an empty pallet present in it), or
  – Muting of the protective function of the light barrier by the loaded pallet with clearances to the side of less than 0.2 m, and muting activated by the pallet load only immediately prior to interruption of the light beams (without greater timing intervals and geometrical gaps).

Calculation of the probability of failure

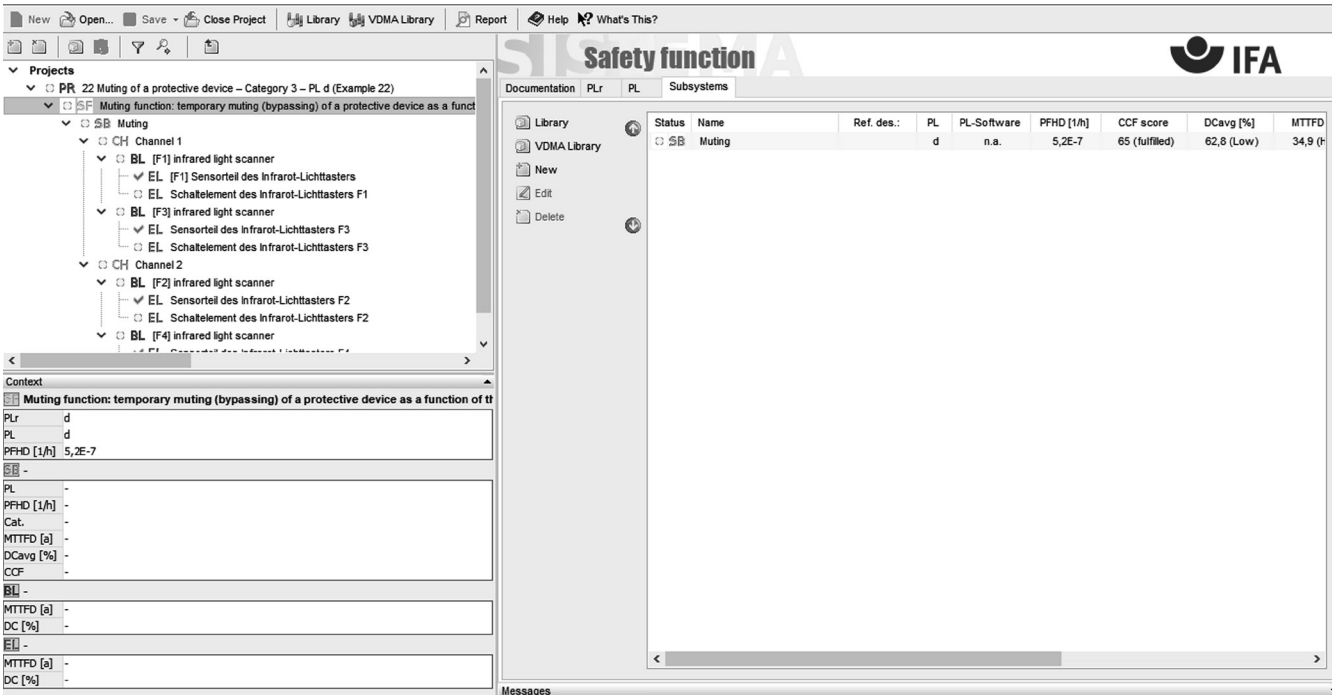
In the calculation below, a *DC* of 0% is assumed for the output relays of the muting sensors F1 to F4, since the contacts employed for muting are not subject to automatic fault detection. For this reason, periodic manual inspection that can be achieved by simple means is specified.

- $MTTF_D$: an $MTTF_D$ of 100 years [E] is assumed for the sensor part of each of the muting sensors F1 to F4. A B_{10D} value of 2,000,000 cycles [E] applies for the output relays of F1 to F4. At 300 working days, 16 working hours and a cycle time of 200 seconds, n_{op} is 86,400 cycles per year and the $MTTF_D$ 232 years for these elements. An $MTTF_D$ of 35 years (“high”) is produced for the channel.
- DC_{avg}: a *DC* of 90% is attained for the sensor part of the muting sensors F1 to F4 by way of the PLC monitoring. The *DC* for the output relays is estimated erring on the safe side at 0%. The resulting DC_{avg} value is 63% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements satisfies Category 3 with a high $MTTF_D$ of each channel (35 years) and a low DC_{avg} (63%). This results in an average probability of dangerous failure PFH_D of $5.2 \cdot 10^{-7}$ per hour. This satisfies PL d.

More detailed references

- EN 415-4: Safety of packaging machines – Part 4: Palletisers and depalletisers (06.97) +AC (2002)
- IEC 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (2012) and Corrigendum 1 (2015). IEC, Geneva, Switzerland 2012/2015
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (2013). IEC, Geneva, Switzerland 2013
- IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons (2018). IEC, Geneva, Switzerland 2018
- EN ISO 13855: Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body (2010). ISO, Geneva, Switzerland 2010

Figure 8.45:
Determining of the PL by means of SISTEMA



8.2.23 Revolving door control – Category 3 – PL d (Example 23)

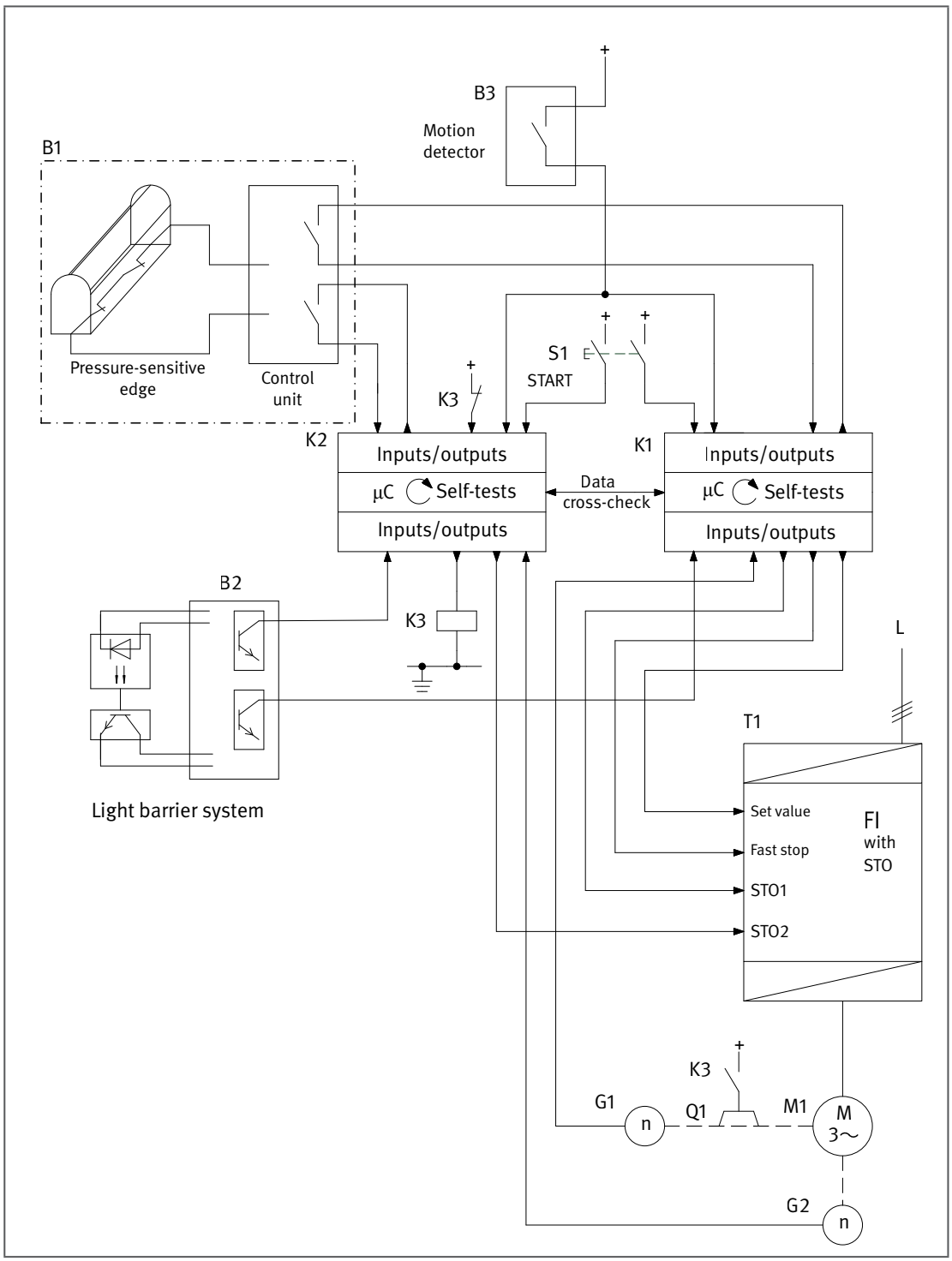
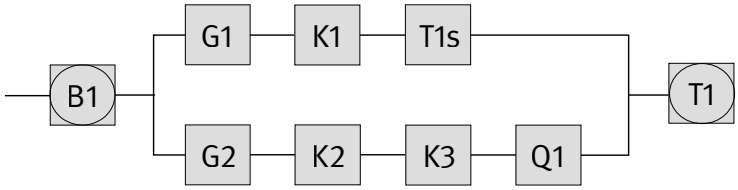


Figure 8.46: Revolving door control employing microcontrollers

Safety functions

- Safety-related stop function: when the pressure-sensitive edge is actuated, the revolving movement of the door is halted (SS1-r – safe stop 1 with ramp monitoring). This safety function is shown in the safety-related block diagram.
- Safely limited speed (SLS): when a person or object is detected by the light barrier, the speed of the revolving door is reduced and safely limited.



Functional description

- The revolving movement of the door is initiated only once the control system has been switched on by the pushbutton S1. In normal operation, the command for the revolving movement is issued by the motion detector B3 located on the door. The frequency inverter T1 is actuated jointly by the two microcontrollers K1 and K2. Each microcontroller (µC) contains a central processing unit (CPU) in the form of a microprocessor, and working memory (RAM) and read-only memory (ROM). K1 controls the functions of setpoint assignment, STO1, and fast stop (T1s). K2 actuates STO2, and the brake Q1 can be released by means of the contactor relay K3. The rotary encoders G1 and G2 signal the motor speed to K1 and K2 respectively. The redundant speed monitoring is required for both safety functions (ramp monitoring and SLS), and is also used for monitoring of the frequency inverter T1.
- Faults in the pressure-sensitive edge or light barrier are detected in the associated control units. The same applies to faults in the control units themselves, which are detected by internal monitoring. Faults in the components of the microcontrollers are detected by the performance of self-tests and by data comparison. When detected, faults are controlled via K1 and/or K2, leading to the door‘s movement being halted by T1 and/or Q1. The wings of the door can be opened manually in order for trapped persons to be freed.
- Owing to redundant processing channels, a single fault does not result in loss of the safety functions. The combination of undetected faults may lead to loss of the safety functions.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The pressure-sensitive edge serves as a safeguard against crush, shear and entrapment points. The pressure-sensitive edge and the control unit are treated as a single unit (B1). The subsystem B1 satisfies the requirements of EN ISO 13856-2 in Category 3 and of EN ISO 13849-1 for PL d. Faults in the signal generator of the pressure-sensitive edge or in the supply conductors must be excluded or be detected via the control unit (pressure-sensitive edges operating on either the break-contact or make-contact principle may be employed). Following actuation and subsequent release of pressure upon a pressure-sensitive edge, the rotary movement begins again with a time delay. The pressure-sensitive edge possesses an adequate deformation path and an adequate range of action.
- The light barrier has the function of leading, non-contact safeguarding of hazard zones. The light barrier system B2 satisfies the requirements for Type 4 to IEC 61496-1 and IEC 61496-2 and for PL e to EN ISO 13849-1. The reduced, safely limited revolving speed that is assumed following detection of a person or an object by the light barrier is increased again to the normal speed following a preset timeout. The supply conductors to the transmitter and receiver are laid separately or with protection.
- During start-up of the door‘s revolving movement for the first time, start-up tests are performed. The tests include, for example, tests of the microcontroller blocks (microprocessor, random-access and read-only memory), input and output tests, and checking of driving of the motor by the frequency inverter (including testing of the fast stop function and of STO1/STO2). A brake test is also performed, in which the frequency inverter is required to act against the applied brake.
- During comparison of data between the two controllers, desired values and intermediate results are exchanged, with inclusion of the cyclical self-tests.
- Owing to the use of a frequency inverter with STO, a contactor is no longer required for disconnection of the supply voltage. The frequency inverter is suitable for driving and braking.

- K3 possesses mechanically linked contact elements to IEC 60947-5-1, Annex L. The switching position of the break-contact element is monitored by the microcontroller K2 for the purpose of fault detection.
- It is assumed in the example that closed-loop control provided by the frequency inverter T1 is sufficient for braking of the revolving door. Once a standstill has been reached, STO is activated in order to prevent unexpected start-up. The braking time and braking distance are monitored by the controller (ramp monitoring). The brake Q1 in the second channel is required so that, should T1 no longer be able to perform the fast stop T1s following the occurrence of a fault, no danger can arise owing to an unexpected movement. Q1 operates on the closed-circuit current principle.
- The software (SRESW) in K1 and K2 is programmed in accordance with the requirements for PL d as per subclause 6.3.
- The standard components G1 and G2 (where relevant for the rotary encoders) and T1 are employed in accordance with the information in subclause 6.3.10.
- For the safety functions under analysis, a fault exclusion is assumed for the fault condition of encoder shaft breakage (G1/G2). For details of the possibility of a fault exclusion, refer for example to IEC 61800-5-2, Table D.8/ GS-IFA-M21.

Remarks

- The circuit example can be employed for implementation of the “safety-related stop function” and “safely limited speed” safety functions in a control system for three-wing and four-wing revolving doors with break-out function (the door wings can be folded manually in an emergency) for use in public and commercial buildings.
- Regular manual inspection of the pressure-sensitive edge is required. Firstly, its serviceability must be checked; secondly, the pressure-sensitive edge must be inspected visually in order for any damage to be detected in good time.

Calculation of the probability of failure

Detailed calculation of the probability of failure is performed for the safety function “safety-related stop function (SS1-r)”, which is also shown in the block diagram:

- Since the pressure-sensitive edge with the associated control unit is available commercially as a safety component, its probability of failure is added at the end of the calculation ($3.0 \cdot 10^{-7}$ per hour [E]).
- The frequency inverter T1 with STO is also available for purchase as a safety component; its probability of failure is added at the end of the calculation ($1.5 \cdot 10^{-8}$ per hour [M]). The fast stop function T1s is modelled in the first channel of the block diagram.
- $MTTF_D$: the safety-related components of K1 and K2 and their peripherals are considered, following application of the parts count method, by a value of 878 years [E]. A value of 190 years [M] is substituted in the formula for G1 and G2. A value of 100 years [M] is applied for T1s. A B_{10D} value of 400,000 cycles [S] is substituted for K3. At one actuation per day, n_{op} is 365 cycles per year, and the $MTTF_D$ is 10,959 years. A B_{10D} value of 1,000,000 cycles [M] is substituted for Q1, resulting in an $MTTF_D$ of 27,397 years. The brake Q1 is required only in the event of a fault, and is not subject to operational wear. Overall, the symmetrized $MTTF_D$ value for the two channels is 82 years (“high”).
- DC_{avg}: owing to internal self-tests and comparison, the *DC* for K1 and K2 is 60%. Internal self-tests are performed on the microcontroller components. Ramp monitoring yields a *DC* of 99% for the block T1s. Owing to the comparison performed by way of K1 and K2, G1 and G2 are rated with a *DC* of 99%. With direct monitoring of a read-back mechanically linked contact element, K3 is rated accordingly with a *DC* of 99%. Owing to performance of the static start-up test, a *DC* of 30% is substituted for Q1. Averaging thus yields a DC_{avg} of 95% (“medium”).
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements satisfies Category 3 with a high $MTTF_D$ of each channel (82 years) and medium DC_{avg} (95%). This yields an average probability of dangerous failure PFH_D of $4.3 \cdot 10^{-8}$ per hour. Together with the sensor unit B1 (consisting of a pressure-sensitive edge and control unit) and the frequency inverter T1, the overall average probability of dangerous failure of the control for this safety function is $3.6 \cdot 10^{-7}$ per hour. This satisfies PL d.

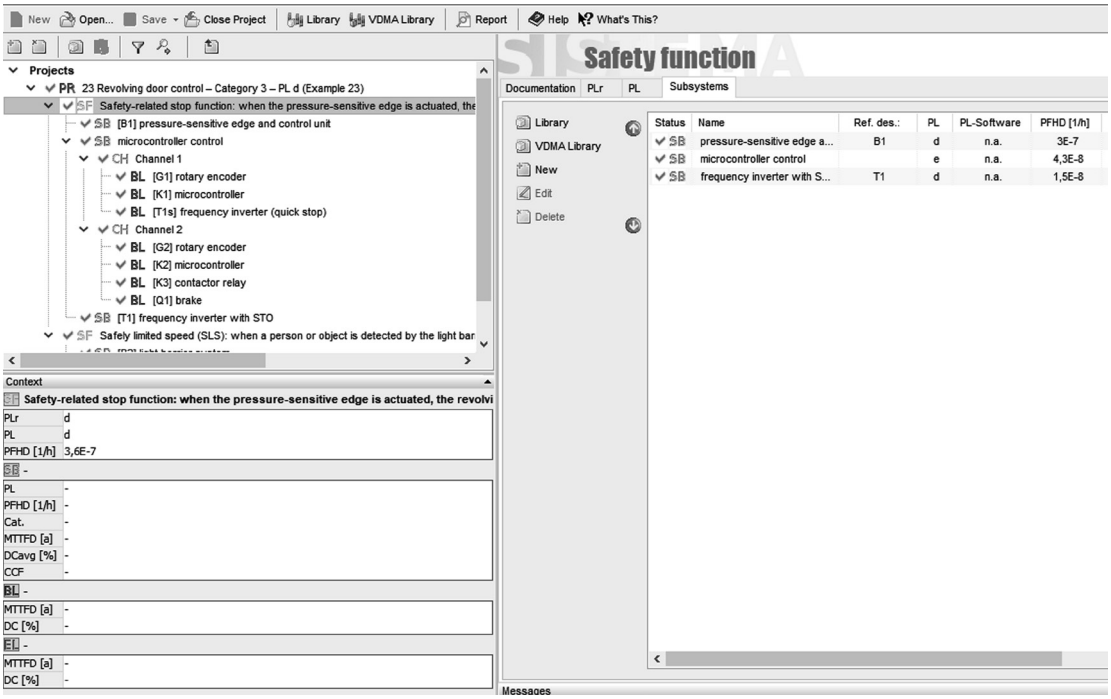
Calculation of the probability of failure for the “safely limited speed (SLS)” safety function

- For this analysis, the sensor unit B1 in the first example analysis is replaced by the light barrier system B2 with a probability of failure of $1.5 \cdot 10^{-9}$ per hour [E]. Addition yields an average probability of dangerous failure of the control system for this safety function of $6.0 \cdot 10^{-8}$ per hour. The implementation of the safety function SLS satisfies PL d.

More detailed references

- EN ISO 13856-2: Safety of machinery – Pressure-sensitive protective devices – Part 2: General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars (2013)
- DIN 18650-1: Powered pedestrian doors – Part 1: Product requirements and test methods (06.10). Beuth, Berlin, Germany 2010
- IEC 60947-4-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2009) + A1 (2012). IEC, Geneva, Switzerland 2009/2012
- IEC 61496-1 (2012) + Cor. (2015): Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests 2012) + Corrigendum (2015). IEC, Geneva, Switzerland 2012/2015
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (2013). IEC, Geneva, Switzerland 2013
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (2016). IEC, Geneva, Switzerland 2016
- Grundsätze für die Prüfung und Zertifizierung von Winkel- und Wegmesssystemen für die Funktionale Sicherheit (GS-IFA-M21). Published by: Institut für Arbeitsschutz der DGUV (IFA), Prüf- und Zertifizierungsstelle im DGUV Test, Sankt Augustin, Germany 2015. www.dguv.de, Webcode; d11973

Figure 8.47:
Determining of the PL by means of SISTEMA

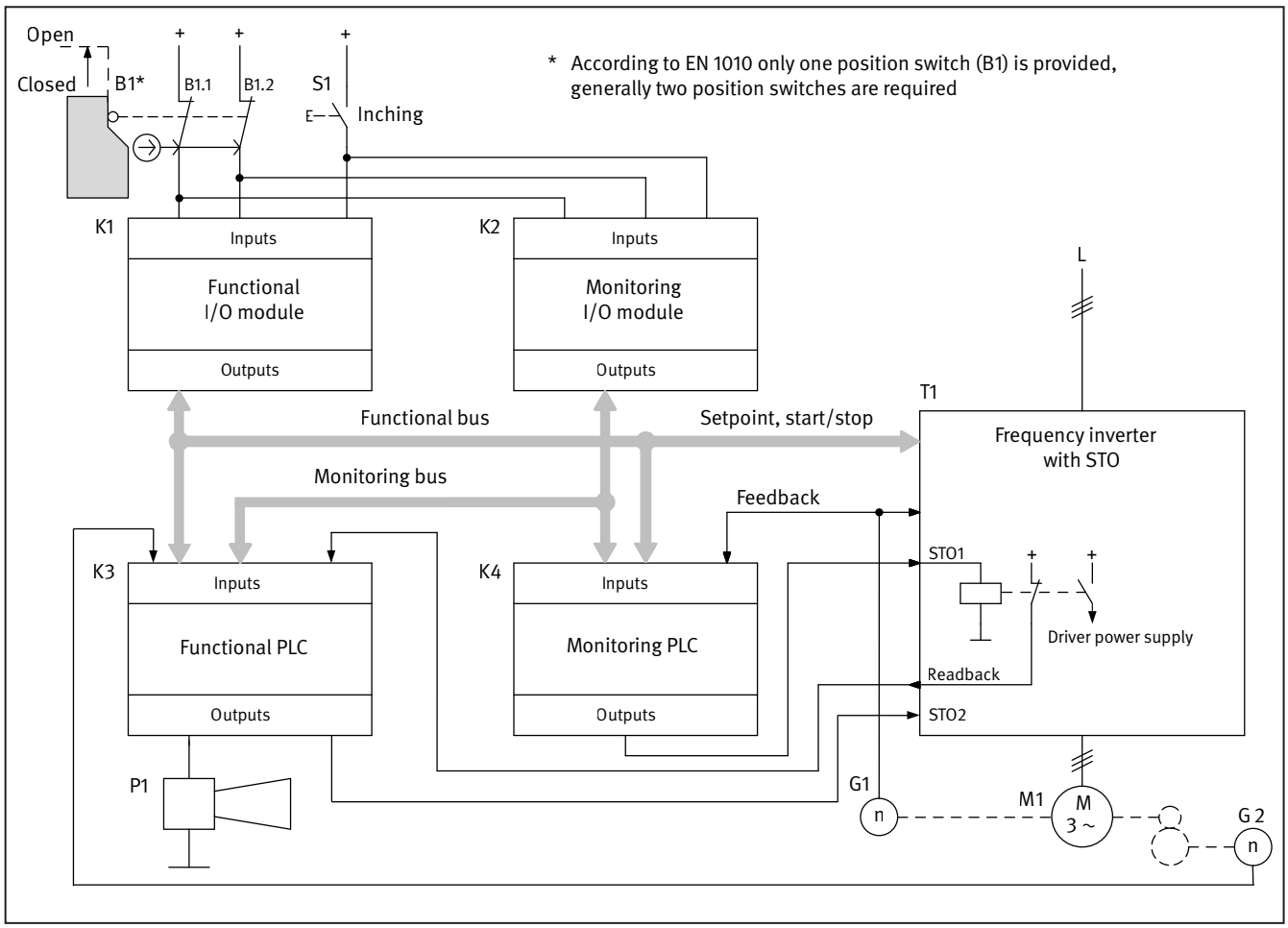


8.2.24 Inching mode with safely limited speed on a printing press – Category 3 – PL d/c (example 24)

Changes with respect to the second edition (BGIA Report 2/2008e):

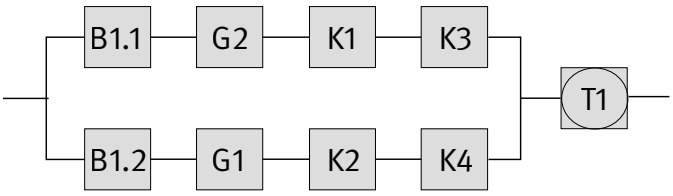
- B1 was replaced by a variant with two direct opening contacts (instead of a break/make contact combination).
- A second encoder G2 on the machine shaft was added to the existing encoder G1 on the motor shaft.
- The frequency inverter T1 was replaced by a variant with integral STO safety function.
- The Category 3 subsystem B1 was grouped with the downstream Category 3 subsystem comprising G1, G2 and K1 to K4.

Figure 8.48:
Inching mode with safely limited speed on a printing press with two-channel microprocessor control



Safety functions

- Safety-related stop function, initiated by a safeguard: the drive is to stop when the guard door is opened (SS1-r – safe stop 1, monitoring of the deceleration ramp, and STO following standstill).
- Safely limited speed (SLS): when the guard door is open, machine movements may occur only at limited speed.
- Inching mode: when the guard door is open, movements are possible only whilst an inching button is pressed.



Functional description

- The remote I/O module K1 registers the states of the position switch with personnel safety function B1 fitted to the safeguard and of the inching button S1, and makes these states available on the functional bus. This information is interpreted by the functional PLC K3 and results in the stop function on the frequency inverter T1 being initiated when the guard door is opened. A signal for the fastest possible stop is transmitted over the functional bus for this purpose. The I/O module K2 and the monitoring PLC K4, which communicate over a dedicated monitoring bus, operate redundantly to K1 and K3. The deceleration ramp is monitored in the functional PLC K3 through the encoder G2 and in the monitoring PLC K4 through the encoder G1. Once a standstill has been reached, or in the event of detection of a fault during stopping, the integral STO safety function is initiated by K3 and K4 via the two STO inputs STO1 and STO2 of T1.
- The open state of the safeguard is detected in K3 and K4 via B1, K1 and K2 as described above. K3 and K4 then monitor the specified limited speed (SLS) redundantly of each other through G2 and G1. If this speed is exceeded, K3 and K4 initiate SS1-r independently of each other, as described above.
- With B1 actuated, only inching mode by means of S1 with safely limited speed is permissible. Releasing of S1 is detected redundantly in K1 to K4 and leads, as described above for the safety-related stop function and SLS, to safe stop 1 of the drive (SS1-r).
- In accordance with EN 1010-1, a single position switch B1 is sufficient. The majority of faults in S1 are detected and controlled by a special actuating procedure, which forces a signal change: when S1 is pressed for the first time, an acoustic warning (signal generator P1) is output; only when S1 is released and pressed again does the drive start up, with delay.
- Faults in K1 and K2 are detected by a status comparison in K4. K4 also monitors K3 by monitoring the input and output information. Some faults in K3 also become evident through faults in the process. Self-tests (e.g. temporal program sequence monitoring by an internal watchdog) are performed in K4; in addition, K3 uses K4 for regular selection of STO1, and monitors the feedback signal from T1.
- Together with the sin/cos encoder G1, the frequency inverter T1 forms a closed-loop control system in which faults (printing errors, paper tears) are revealed by the production process, which is highly synchronous. The encoder signals from G1 on the motor shaft are also read into K4 and monitored in T1 for plausibility of the sin/cos information ($\sin^2 + \cos^2 = 1$). Redundantly to this, the signals from a diversely engineered encoder G2 on the machine shaft are also interpreted. Although the two encoders are not located on the same shaft, their values, read into K4/K3 and converted into paper speeds, can be compared in K4, thereby providing fault detection for G1 and G2. Fault detection for STO1 in T1 is implemented by provision of a feedback signal that is interpreted in K3. Correct execution of STO2 is monitored by internal test measures in T1; in the event of a fault, these measures initiate stopping.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The break contacts of B1 satisfy IEC 60947-5-1, Annex K, and B1 complies with DGUV Information 203-079 governing the selection and fitting of interlocking devices. Measures are implemented to prevent displacement and reasonably foreseeable misuse (see EN ISO 14119). A stable arrangement of the safeguard is assured for actuation of the position switch.

- S1 satisfies IEC 60947-5-1; short-circuiting between adjacent contacts that are isolated from each other can therefore be excluded. Despite the warning at start-up and forced dynamics, S1 may stick during inching mode. An additional requirement is therefore that an emergency stop device be installed within the operator‘s reach.
- The conditions for fault exclusion for conductor short circuits in accordance with EN ISO 13849-2, Table D.4 must be observed for the connecting lines to S1. Faults in the connecting lines to B1 are detected by monitoring in K4.
- The programmable components K1 to K4 satisfy the normative requirements in accordance with subclause 6.3.
- G1 is integrated into the closed-loop control circuit (acquisition of the commutation). The encoder G2, which is engineered with diversity, has the purpose of fault detection.
- The standard components G1 and G2 are employed in accordance with the information in subclause 6.3.10.
- T1 possesses an integrated STO safety function, which satisfies all requirements for Category 3 and PL d. The required fault detection is attained by provision and external monitoring of a feedback signal for STO1 and by internal monitoring measures for STO2.
- The bus systems (functional bus, monitoring bus) are employed in accordance with the information in subclause 6.2.18.

Remarks

- This example describes the safeguarding of entrapment points on rotary printing press. For non-cyclical operator intervention in the hazard zone, i.e. less frequently than one intervention per hour, EN 1010-1 requires only one position switch for monitoring of the guard position. The fault-tolerance criterion for Category 3 generally requires the use of two position switches for similar machine control systems.
- For inching mode subject to the condition that safely limited speed is already guaranteed, the possibility of avoiding the hazard can be assumed under certain conditions. For risk assessment, refer also to Example 4 in Annex A.

Calculation of the probability of failure

- The three safety functions differ only on the sensor level. B1, G1 and S1 are therefore described separately.
- The two contacts with direct opening action of B1 are integrated into the downstream Category 3 structure. A B_{10D} value of 20,000,000 cycles [S] is assumed per contact. At 10 actuations per week, n_{op} is 520 cycles per year and the $MTTF_D$ is 384,615 years. Under the particular requirements of EN 1010-1 for B1 (refer to the design features), a *DC* of 60% (cross monitoring of input signals without dynamic test, infrequent signal change caused by the application) is assumed.
- G1 and G2 are also each integrated into a channel of the downstream Category 3 structure. Their contribution to determining of the PFH_D is an $MTTF_D$ of 30 years per channel [M], 90% *DC* for G2 by plausibility check and 99% *DC* for G1 by monitoring for $\sin^2 + \cos^2 = 1$, plausibility checking and fault detection in the process.
- S1 possesses a B_{10D} value of 100,000 cycles [M]. At 10 actuations per week, n_{op} is 520 cycles per year and the $MTTF_D$ is 1,923 years. Owing to the forced signal change and start-up warning, S1 is modelled as a Category 2 subsystem, and a *DC* of at least 60% is assumed (sticking following repeated inching is not detected, however). Testing is performed in K1 and K3, the probability of failure of which is already considered in the downstream Category 3 subsystem and need not therefore also be considered in addition in the test channel. So as not to provoke an error message in SISTEMA, an $MTTF_D$ value of 100 years is substituted in the test channel. Since testing is performed immediately upon demand of the safety function, an adequate test rate is assured. The separate subsystem of S1 thus attains an average probability of dangerous failure of $5.3 \cdot 10^{-7}$ per hour. Since it is not practicable for the control system to bring about the safe state automatically in the event of the inching button sticking, and the PL_r is not greater than c, involvement of the operator is also permissible (see subclause 6.2.5).
- K1 + K3 and K2 + K4 are considered in two channels of a Category 3 subsystem in all three safety functions under analysis. 100 years [M] for K1 and K2, 50 years [M] for K4 and 30 years [M] for K3 are substituted for the $MTTF_D$. The *DC* of 99% for K1 and K2 is produced by direct comparison of the supplied status information in K4. The *DC* of 99%

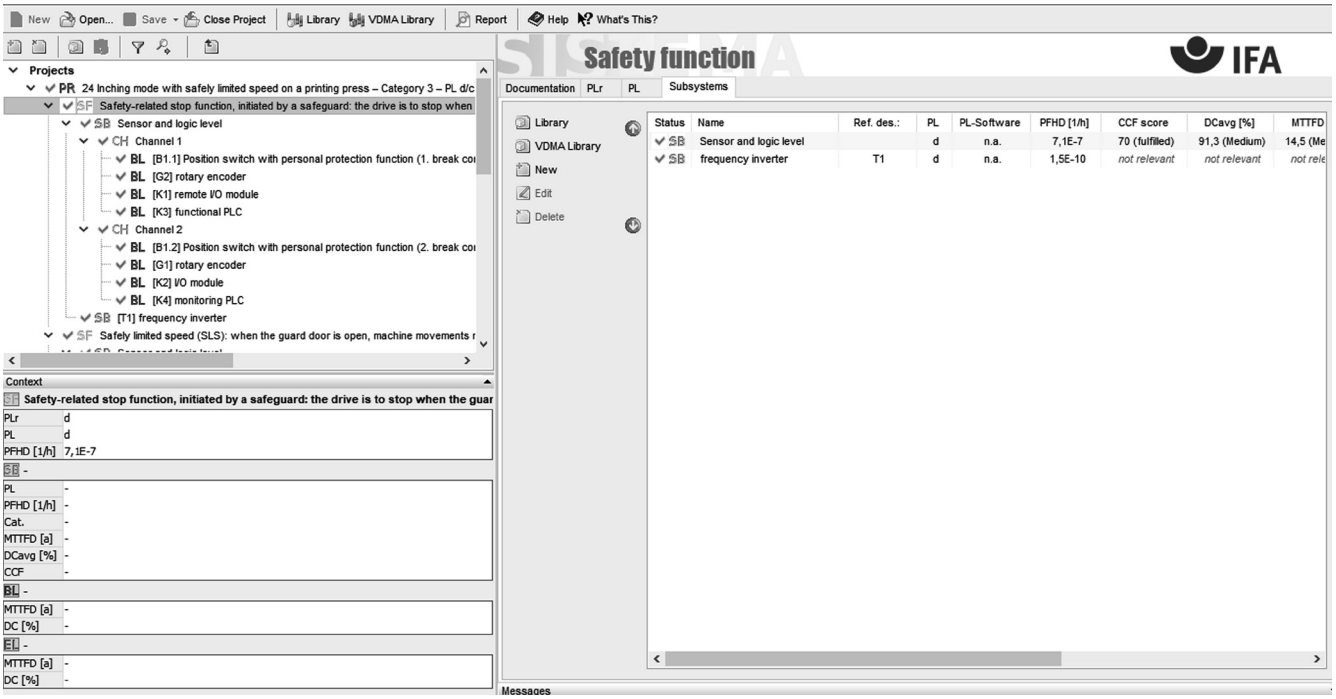
for K3 is based upon parallel processing of all safety-related information in K4 and upon the direct comparison in K4 with the intermediate results and output signals formed by K3. The self-tests implemented in K4 together with partial monitoring by the selection of STO1 read back by K3 result in a *DC* of 60% for K4.

- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- T1, including its integrated safety function STO, is considered in the analysis as an encapsulated subsystem with Category 3, PL d and a PFH_D of $1.5 \cdot 10^{-10}$ per hour.
- The safety-related stop function and the safely limited speed are engineered as a continuous Category 3 subsystem comprising B1.1/B1.2, G2/G1 and K1 to K4, which is combined with T1 to form an encapsulated Category 3 subsystem. For the first subsystem, a medium $MTTF_D$ per channel of 14.5 years and a medium DC_{avg} of 91% yield a PFH_D of $7.1 \cdot 10^{-7}$ per hour. Combination with T1 ($PFH_D = 1.5 \cdot 10^{-10}$ per hour) yields a PFH_D of $7.1 \cdot 10^{-7}$ per hour for both safety functions. This satisfies PL d.
- Inching mode is implemented by a combination of the Category 2 subsystem S1 ($PFH_D = 5.3 \cdot 10^{-7}$ per hour) with the two Category 3 subsystems comprising T1 ($PFH_D = 1.5 \cdot 10^{-10}$ per hour) and G2/G1 together with K1 to K4. With a medium $MTTF_D$ per channel of 14.5 years and a medium DC_{avg} of 91%, the second Category 3 subsystem attains a PFH_D of $7.1 \cdot 10^{-7}$ per hour. Combination of the three subsystems yields a PFH_D of $1.2 \cdot 10^{-6}$ per hour. This satisfies PL c.

More detailed references

- EN 1010-1: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (2004) +A1 (2010).
- Sicherheitsgerechtes Konstruieren von Druck- und Papierverarbeitungsmaschinen. Mechanik. Published by: Berufsgenossenschaft Druck und Papierverarbeitung, Wiesbaden, Germany 2004 http://dp.bgetem.de/pages/service/download/medien/BG_220-1_DP.pdf
- *Werner, C.; Zilligen, H; Köhler, B.; Apfeld, R.*: Safe drive controls with frequency inverters . IFA Report 4/2018e. 3rd ed. Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin, Germany 2019 (will be published in Summer 2019). www.dguv.de/ifa, Webcode: e635980
- Principles for the testing and certification of rotary and position measuring systems for functional safety (GS-IFA-M21_E). Published by: Institut für Arbeitsschutz der DGUV, Prüf- und Zertifizierungsstelle im DGUV Test, Sankt Augustin, Germany 2015. www.dguv.de, Webcode: d11973
- DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen. Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin, Germany 2015. http://publikationen.dguv.de/dguv/pdf/10002/203-079.pdf

Figure 8.49:
Determining of the PL by means of SISTEMA



8.2.25 Pneumatic valve control (subsystem) – Category 3 – PL e (Example 25)

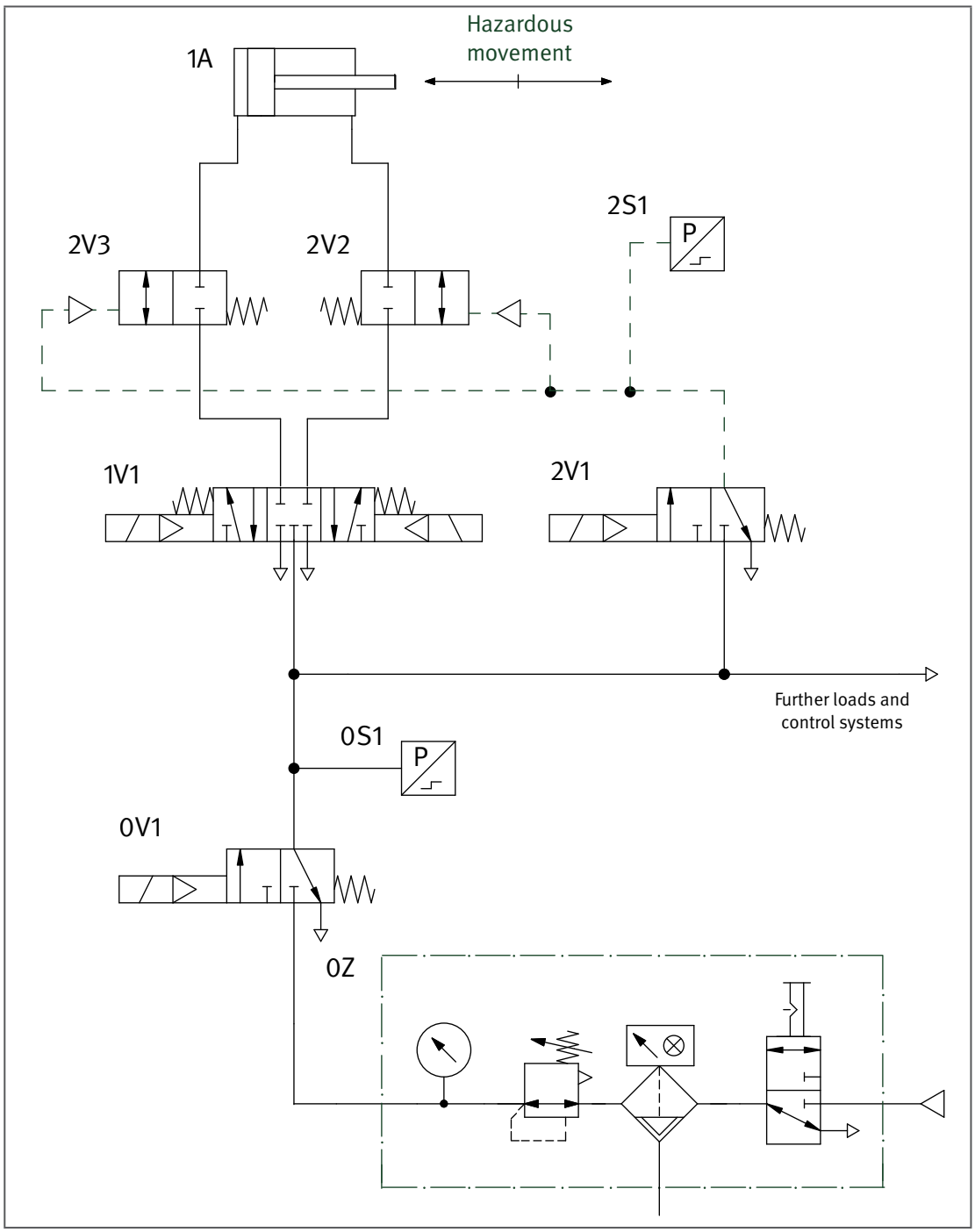
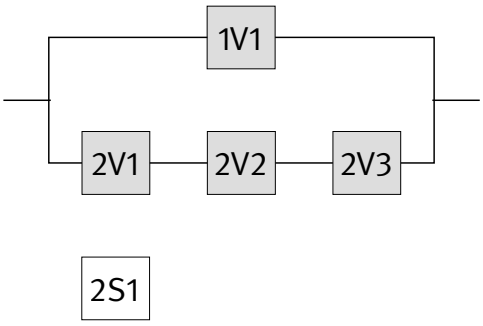


Figure 8.50: Tested pneumatic valves for redundant control of hazardous movements

Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position, implemented by safety sub-function SSC.
- Only the pneumatic part of the control system is shown here, in the form of a subsystem. Further safety-related parts of control systems (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.



Functional description

- Hazardous movements are controlled redundantly by directional control valves. Movements can be halted either by the directional control valve 1V1 or by the directional control valves 2V2 and 2V3. The latter are driven by the control valve 2V1.
- Failure of one of these valves alone does not result in loss of the safety function.
- All directional control valves are actuated cyclically in the process.
- The functioning of the control valve 2V1 is monitored by means of a pressure switch 2S1. Certain faults on the unmonitored valves become apparent in the work process. The valves 2V2 and 2V3 should be equipped with position monitors, or – since this is not yet state of the art – they should be checked regularly for correct operation. An accumulation of undetected faults can lead to loss of the safety function.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The directional control valve 1V1 features a closed centre position with sufficient overlap and spring-centred central position.
- The stop valves 2V2 and 2V3 are ideally screwed into the cylinder and driven by the valve 2V1 acting as a pilot valve.
- The safety-oriented switching position is assumed from any position by cancellation of the control signal.
- A single-channel PLC for example is employed for the processing of signals from the pressure monitor 2S1.

Calculation of the probability of failure

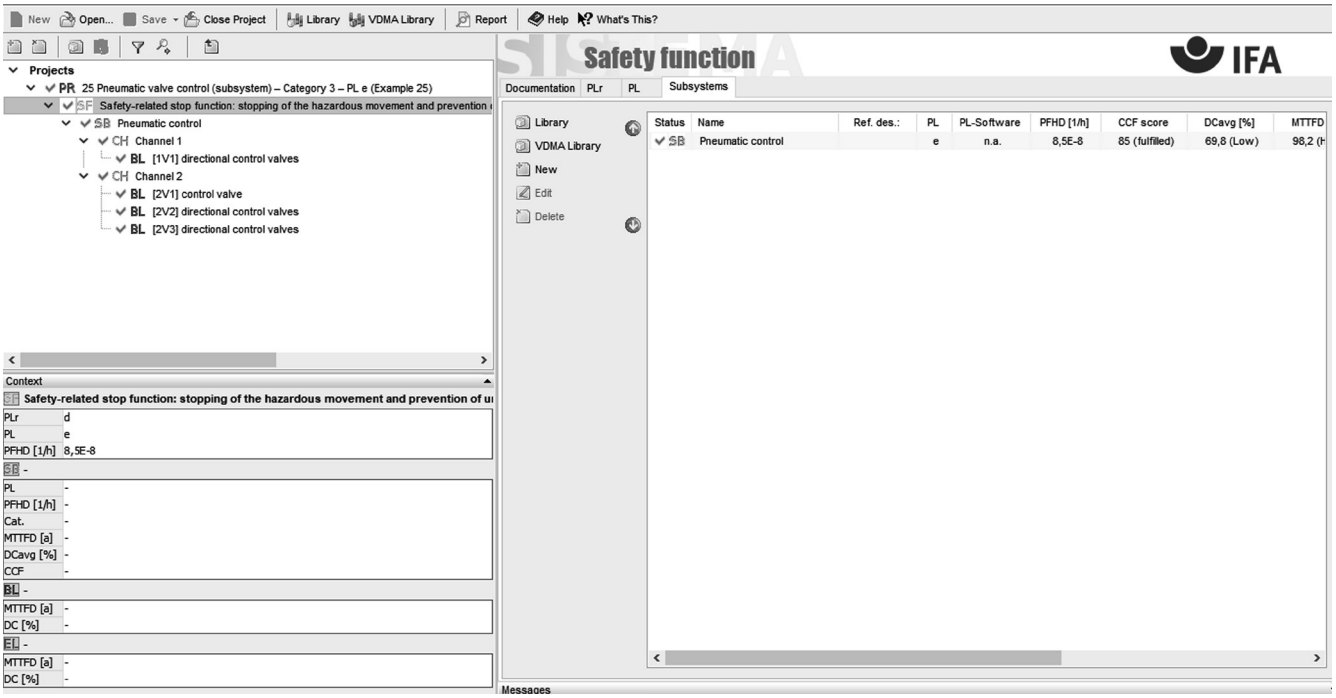
- $MTTF_D$: B_{10D} values of 20,000,000 cycles [S] are assumed for the valves 1V1, 2V1, 2V2 and 2V3. At 240 working days, 16 working hours and a cycle time of 20 seconds, n_{op} is 691,200 cycles per year. The $MTTF_D$ for 1V1, 2V1, 2V2 and 2V3 is thus 289 years. Capping of the two channels to 100 years results in a symmetrized $MTTF_D$ value per channel of 98 years (“high”).
- DC_{avg}: pressure monitoring of the control signal for the stop valves results in a *DC* of 99% for 2V1. Fault detection via the process results in a *DC* of 60% for 1V1, and regular checking of operation in a *DC* of 60% for 2V2/2V3. Averaging thus produces a DC_{avg} of 69.8% (“low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)

The combination of the pneumatic control elements satisfies Category 3 with a high $MTTF_D$ (98.2 years) and low DC_{avg} (69.8%). This results in an average probability of dangerous failure of $8.5 \cdot 10^{-8}$ per hour. This satisfies PL e. Following the addition of further safety-related control components in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.

More detailed references

- VDMA technical rule 24584: Safety functions of regulated and unregulated (fluid) mechanical systems (08.16).
- *Uppenkamp, J.*: Teil-Sicherheitsfunktionen nach VDMA Einheitsblatt 24584 – Beispiele zweikanaliger elektropneumatischer Steuerungen. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin, Germany 2017.
  www.dguv.de/medien/ifa/de/pra/hydraulik_pneumatik/beispiele-teil-sicherheitsfunktionen.pdf

Figure 8.51:
Determining of the PL by means of SISTEMA



8.2.26 Pneumatic valve control – Category 3 – PL e (Example 26)

This example has been deleted, since the technology is no longer relevant.

8.2.27 Hydraulic valve control (subsystem) – Category 3 – PL e (Example 27)

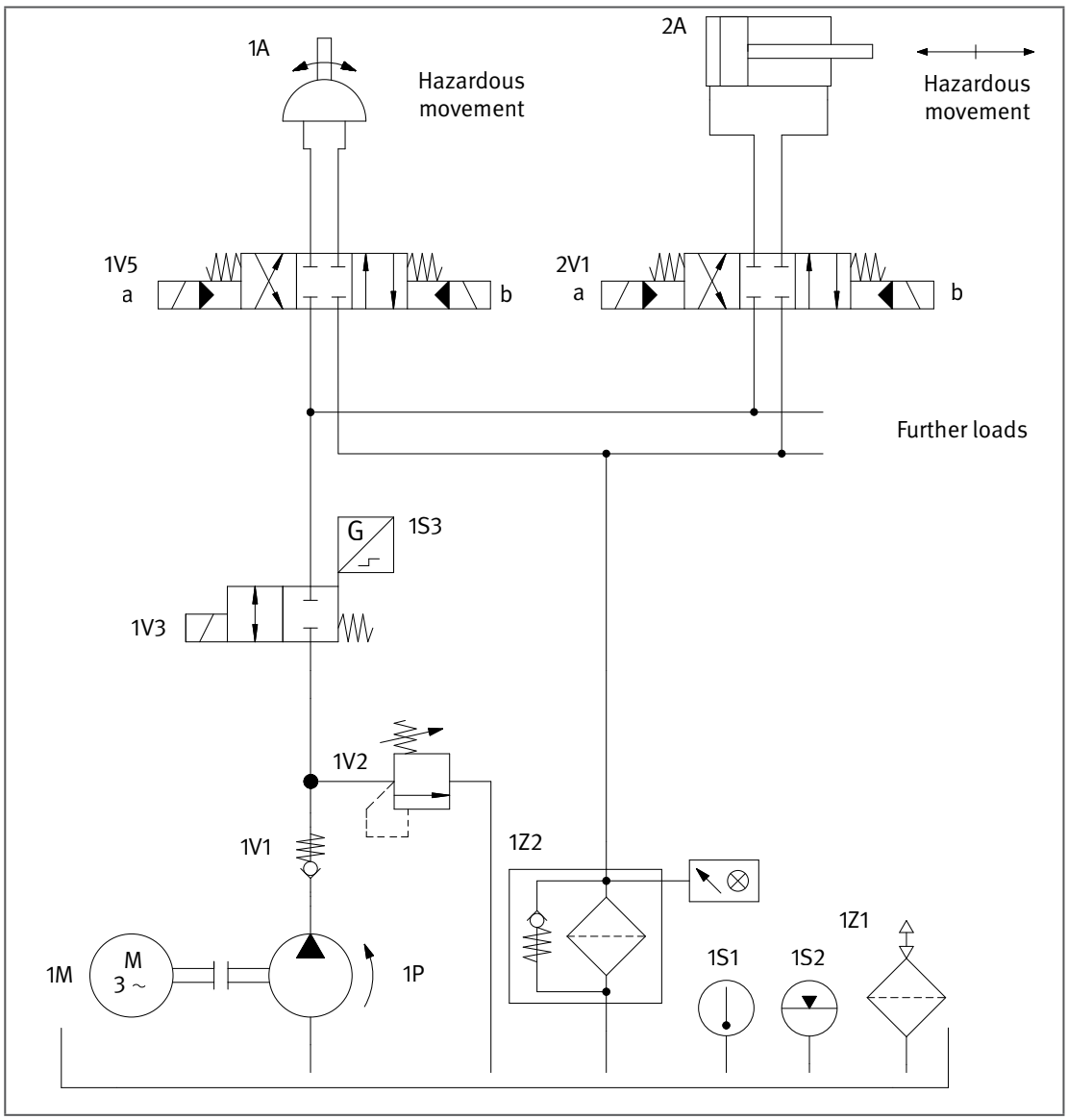


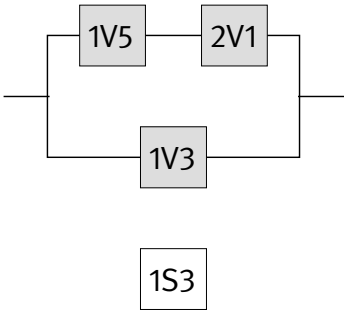
Figure 8.52: Tested hydraulic valves for redundant control of hazardous movements

Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control system is shown here, in the form of a subsystem. Further SRP/CS (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are executed by two actuators, 1A and 2A, in the same hazard zone. The two movements can be stopped either by the two directional control valves 1V5 and 2V1, or at a higher level by the directional control valve 1V3.
- Failure of one of these valves alone does not result in loss of the safety function.
- 1V5 and 2V1 are actuated cyclically in the process. 1V3 closes only in response to a demand of the safety function, but at least once per shift.



- A technical measure for fault detection is implemented only on 1V3 (position monitoring by 1S3). Certain faults on the unmonitored valves become apparent in the work process. An accumulation of undetected faults may lead to loss of the safety function.

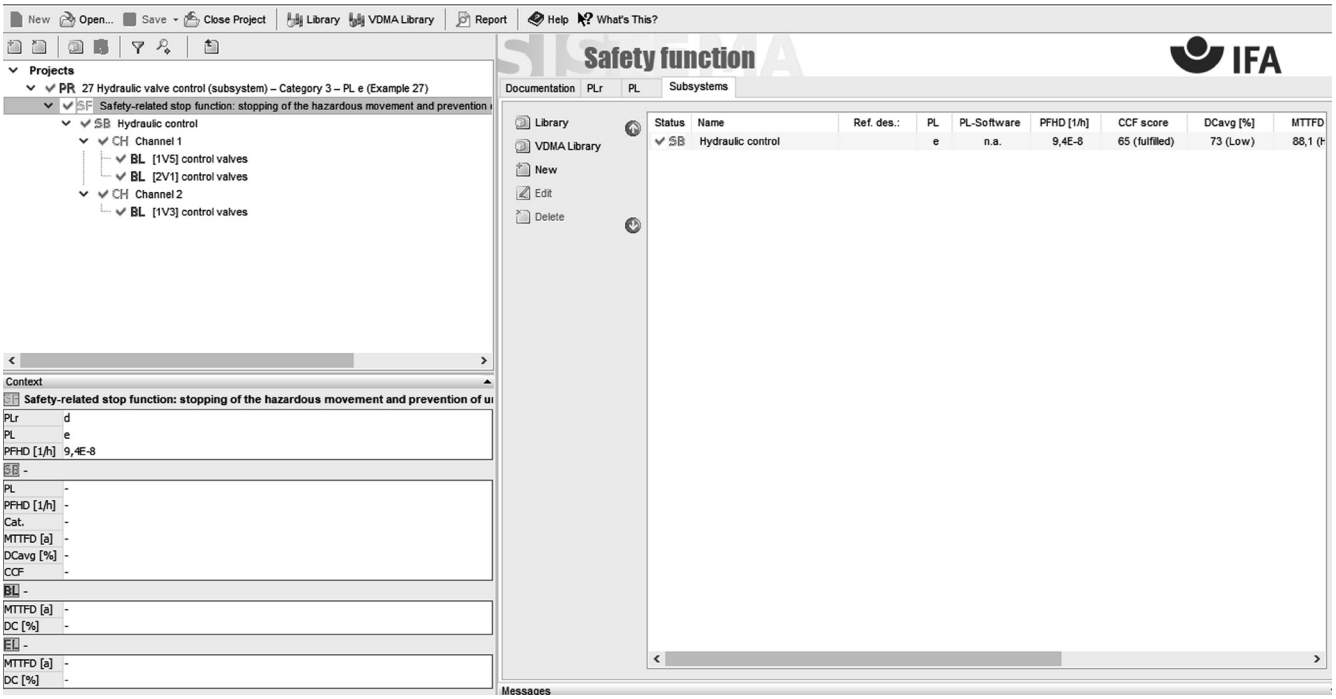
Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The directional control valves 1V5 and 2V1 feature a closed centre position with sufficient overlap and spring-centred central position. 1V3 employs electrical position monitoring, since 1V3 is not switched cyclically.
- The safety-oriented switch position is attained in each case by removal of the control signal (electrical or hydraulic).
- A single-channel PLC for example is employed for processing signals from the electrical position monitor.

Calculation of the probability of failure

- $MTTF_D$: an $MTTF_D$ of 150 years is assumed for the directional control valves 1V3, 1V5 and 2V1 [M]. Capping of the second channel (1V3) to 100 years produces a symmetrized $MTTF_D$ value of 88 years (“high”).
- DC_{avg}: a *DC* of 99% for 1V3 is based upon the direct monitoring of the switching state by 1S3. The *DC* of 60% in each case for the directional control valves 1V5 and 2V1 is based upon indirect monitoring by the process. Averaging thus produces a DC_{avg} of 73% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the hydraulic control elements satisfies Category 3 with a high $MTTF_D$ (88 years) and low DC_{avg} (73%). This results in an average probability of dangerous failure of $9.4 \cdot 10^{-8}$ per hour. This satisfies PL e. Following the addition of further SRP/CS in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.

Figure 8.53:
Determining of the PL by means of SISTEMA



8.2.28 Position monitoring of movable guards – Category 4 – PL e (Example 28)

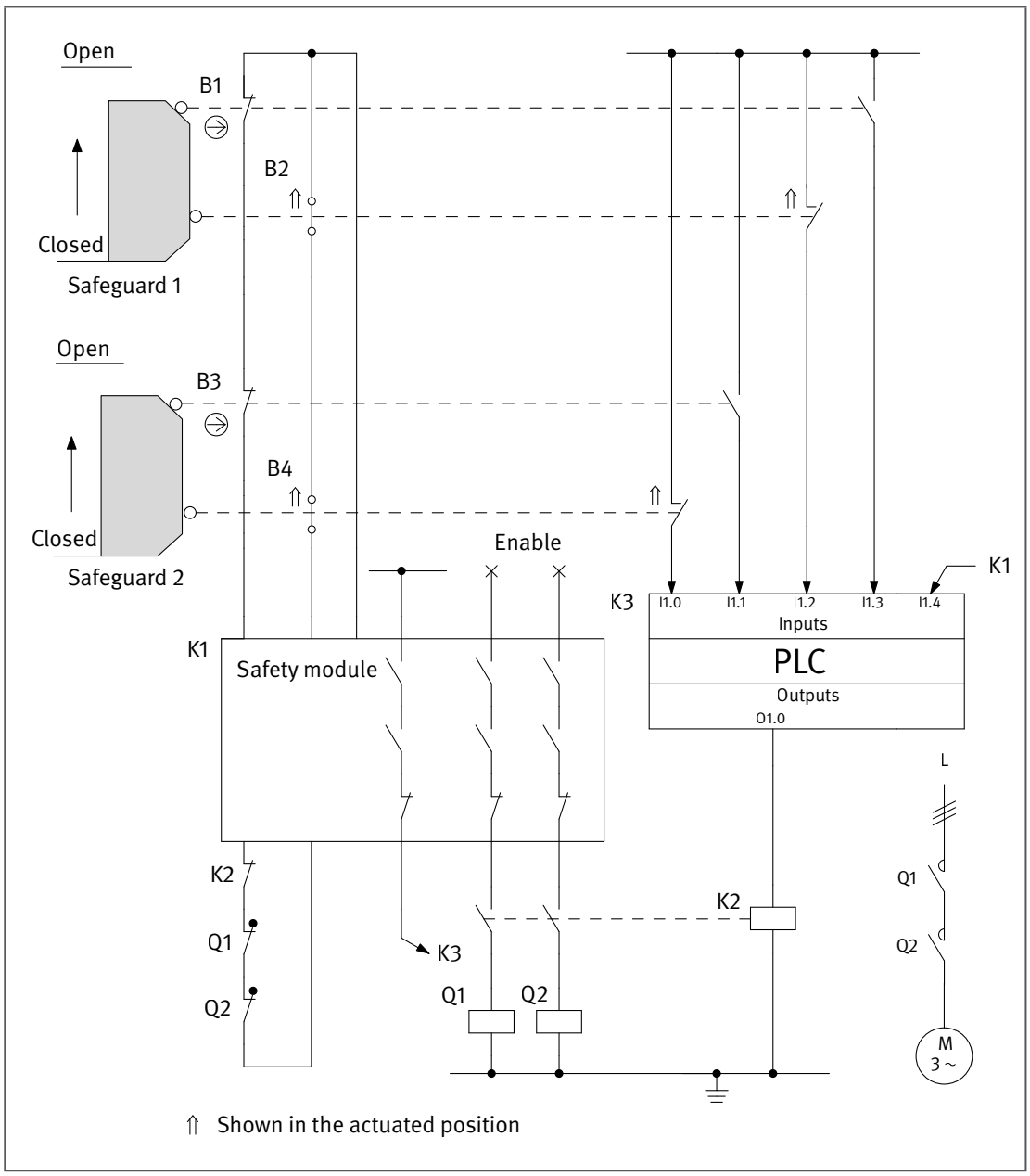


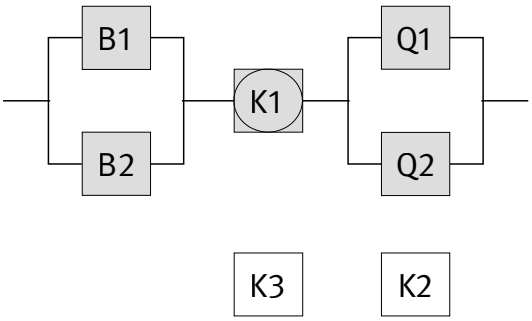
Figure 8.54: Position monitoring of movable guards for the prevention of hazardous movements

Safety function

- Safety-related stop function, initiated by a safeguard: opening of a movable guard (safety guard) initiates the safety function STO (safe torque off).

Functional description

- A hazard zone is safeguarded by two movable guards (safety guards). Opening of a safety screen is detected by two position switches B1/B2 respectively B3/B4 comprising break contact/make contact combinations and evaluated by a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.



- For fault detection purposes, all position switch states are read by a second contact into a standard PLC K3, the chief purpose of which is functional control. In the event of a fault, K3 can de-energize the contactors Q1 and Q2 independently of K1 by means of a contactor relay K2. Faults in K2, Q1 and Q2 are detected by the safety module K1. The safety function is retained in the event of a component failure. The majority of component failures are detected and lead to operating inhibition. An accumulation of undetected faults does not result in loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the guards is assured for actuation of the position switches.
- B1 and B3 are position switches with a direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the position switches are laid separately or with protection.
- Faults in the actuating and operating mechanism are detected by the use of two position switches differing in the principle of their actuation (break and make contact combination).
- Several safeguards may be cascaded. Cascading limits the facility for K1 to detect faults (see Annex E). The position switches are however additionally monitored by K3; this results in faults being detected even where safeguards are cascaded.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactor relay K2 possesses mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contactors Q1 and Q2 possess mirror contacts in accordance with IEC 60947-4-1, Annex F.
- The PLC K3 satisfies the normative requirements set out in subclause 6.3.

Calculation of the probability of failure

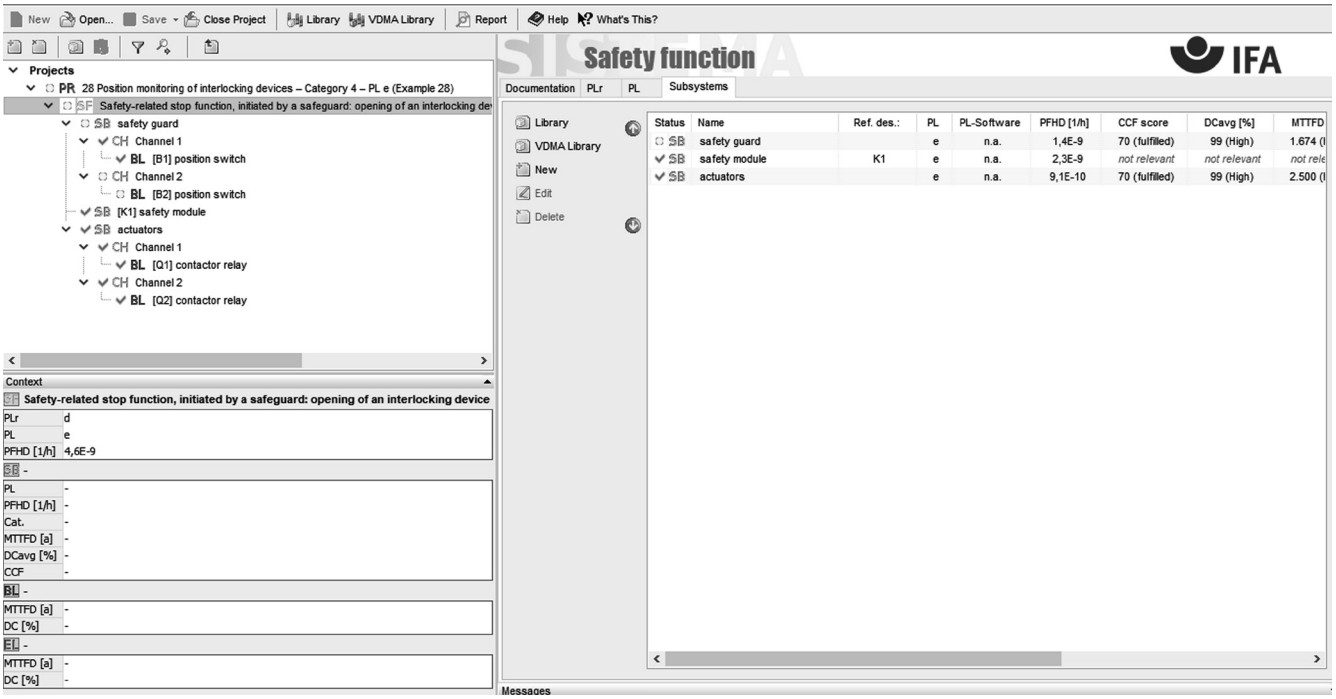
- The circuit arrangement can be divided into three subsystems as shown in the safety-related block diagram. The probability of failure of the safety module K1 is added at the end of the calculation ($2.3 \cdot 10^{-9}$ per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows. Since each guard door (guard) forms part of a dedicated safety function, calculation is shown here by way of example for safeguard 1.
- $MTTF_D$: for the position switch B1 with direct opening action and roller actuation, the B_{10D} is $20 \cdot 10^6$ switching cycles [M]. For position switch B2 (make contact), the B_{10D} is $1 \cdot 10^5$ switching cycles [M]. At 365 working days, 16 working hours per day and a cycle time of 1 hour, the n_{op} for these components is 5,840 cycles per year. The $MTTF_D$ of B1 and B2 is 34,246 years and 171 years for B2 respectively. For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical durability of 1,000,000 switching cycles [M]. On the assumption that 50% of failures are dangerous, the B_{10D} value is produced by doubling of the B_{10} value. The value assumed above for n_{op} results in an $MTTF_D$ of 3,424 years per channel for Q1 and Q2. Altogether, the symmetrized $MTTF_D$ value per

channel in the two subsystems is 100 years (“high”). The position switch B2 exhibits a limited operation time of 17.1 years. Its replacement in good time is recommended.

- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the break/make contact combinations in K1 and K3. The *DC* of 99% for the contactors Q1 and Q2 is derived from monitoring at each energization of K1. The *DC* values stated correspond to the DC_{avg} of the subsystem concerned.
- Adequate measures against common cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)

The subsystems B1/B2 and Q1/Q2 each correspond to Category 4 with a high $MTTF_D$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure in each case of $2.3 \cdot 10^{-9}$ per hour. Following addition of the subsystem K1, the average probability of dangerous failure is $4.6 \cdot 10^{-9}$ per hour. This satisfies PL e.

Figure 8.55:
Determining of the PL by means of SISTEMA



8.2.29 Cascading of emergency stop devices by means of a safety module – Category 3 – PL e (Example 29)

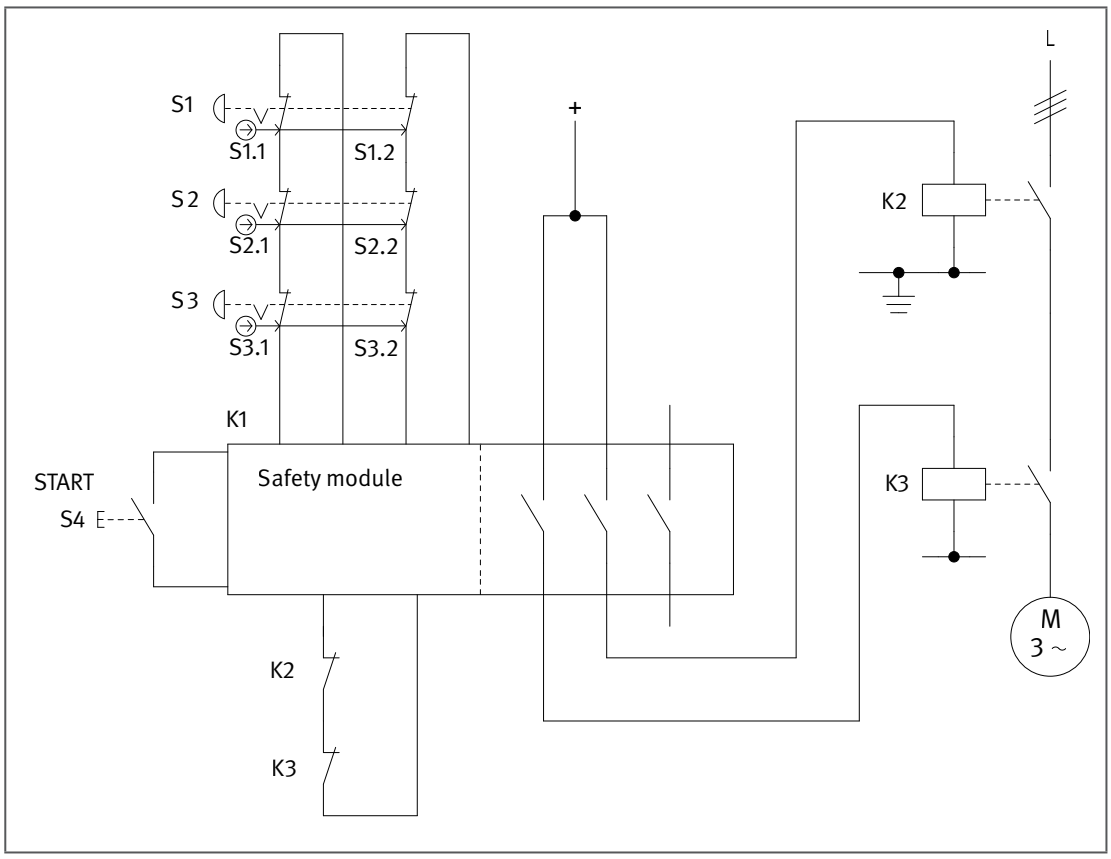


Figure 8.56: Cascading of emergency stop devices by means of a safety module (emergency stop function, STO)

Safety function

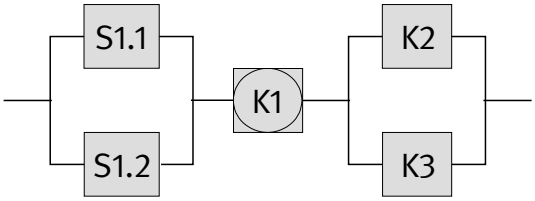
- Emergency stop function, STO by actuation of an emergency stop device

Functional description

- Hazardous movements or states are interrupted or prevented by actuation of an emergency stop device. As shown by Example 3 in subclause 5.3.2, each emergency stop device initiates a safety function of its own. S1 is considered below as being representative of all the devices. S1 is evaluated in a safety module K1, which actuates two redundant contactor relays K2 and K3.
- The signals from the emergency stop devices are read redundantly into the safety module K1 for fault detection. K1 also features internal test measures. The contactor relays K2 and K3 are also monitored in K1, by means of mechanically linked readback contacts. K2 and K3 are switched by the switch S4 at each start-up command, approximately twice each month. An accumulation of more than two faults in the period between two successive actuations can lead to loss of the safety function.
- It is not assumed that more than one emergency stop device is pressed simultaneously.
- Organizational measures ensure that each emergency-stop device is actuated at least once a year.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The emergency stop devices S1, S2 and S3 are switching devices with direct opening contacts in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the switching devices are laid with protection.



- The safety module K1 satisfies all requirements for Category 4 and PL e.
- K2 and K3 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

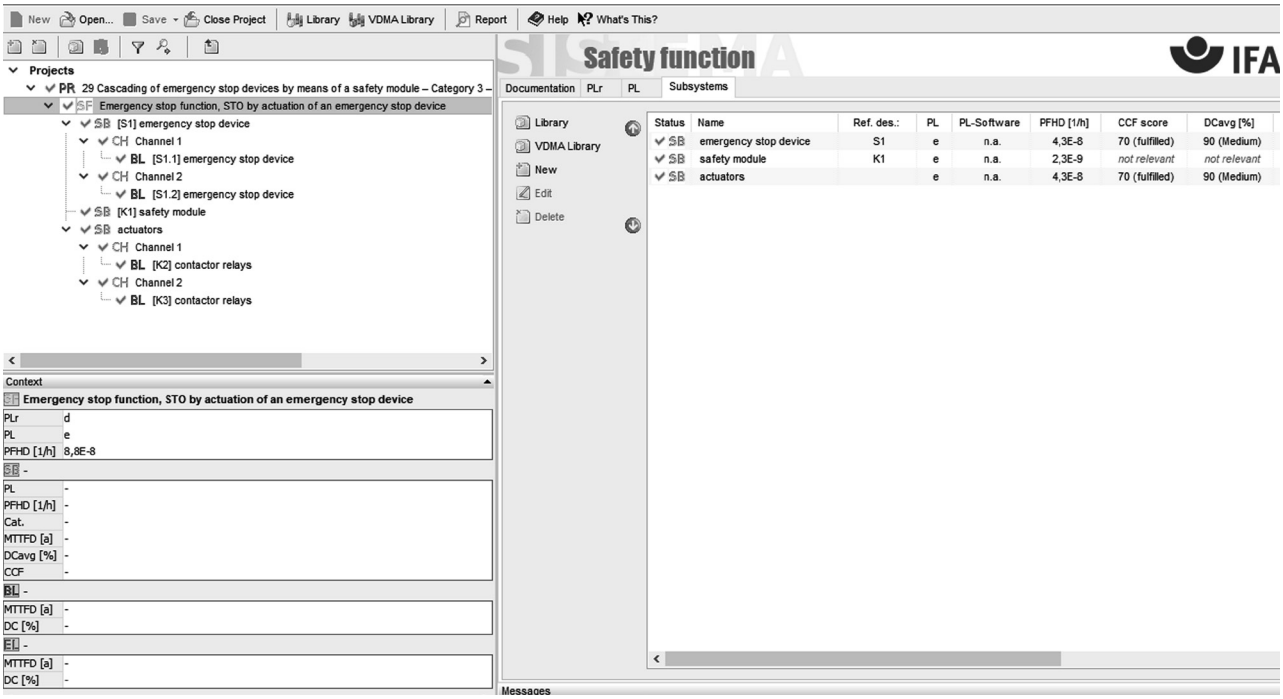
Remark

- The emergency stop function is a complementary protective measure to EN ISO 12100 [3].

Calculation of the probability of failure

- S1, S2 and S3 are standard emergency stop devices to EN ISO 13850. In the two-channel model, a B_{10D} value of 100,000 switching cycles [S] is substituted for each contact of an emergency-stop device. The probability of failure of the safety module K1 is added at the end of the calculation ($2.3 \cdot 10^{-9}$ per hour [M], suitable for PL e).
- $MTTF_D$: for the contactor relays K2 and K3, the B_{10} value corresponds under inductive load (AC 3) to an electrical durability of 1,000,000 switching cycles [M]. On the assumption that 50% of failures are dangerous, the B_{10D} value is produced by doubling of the B_{10} value. With twelve demands upon the emergency stop function and 24 start commands per year, n_{op} is 36 cycles per year and the $MTTF_D$ is 55,556 years. This is also the symmetrized $MTTF_D$ for the channel, which is capped to 100 years (“high”).
- DC_{avg}: the *DC* for K2 and K3 and for S1.1 and S1.2 is 90%. The *DC* is based upon testing and the detection of cross-circuits by the safety module K1. This is also the DC_{avg} (“medium”). An adequate test rate of the emergency-stop devices is assured (refer to the information in subclauses 6.2.14 and D.2.5.1).
- Adequate measures against common cause failure (70 points): separation (15), well-tried components (5), over-voltage protection etc. (15) and environmental conditions (25 + 10)
- At twelve demands upon the emergency stop function per year, the average probability of dangerous failure PFH_D for the emergency stop device S1 is $4.3 \cdot 10^{-8}$ per hour.
- The subsystem K2/K3 satisfies Category 3 with a high $MTTF_D$ (100 years) and medium DC_{avg} (90%). This results in an average probability of dangerous failure of $4.3 \cdot 10^{-8}$ per hour. Following addition of the subsystem K1, the average probability of dangerous failure is $8.8 \cdot 10^{-8}$ per hour. This satisfies PL e. The PL_r of d is thus surpassed.

Figure 8.57:
Determining of the PL by means of SISTEMA



8.2.30 Contactor monitoring module – Category 3 – PL e (Example 30)

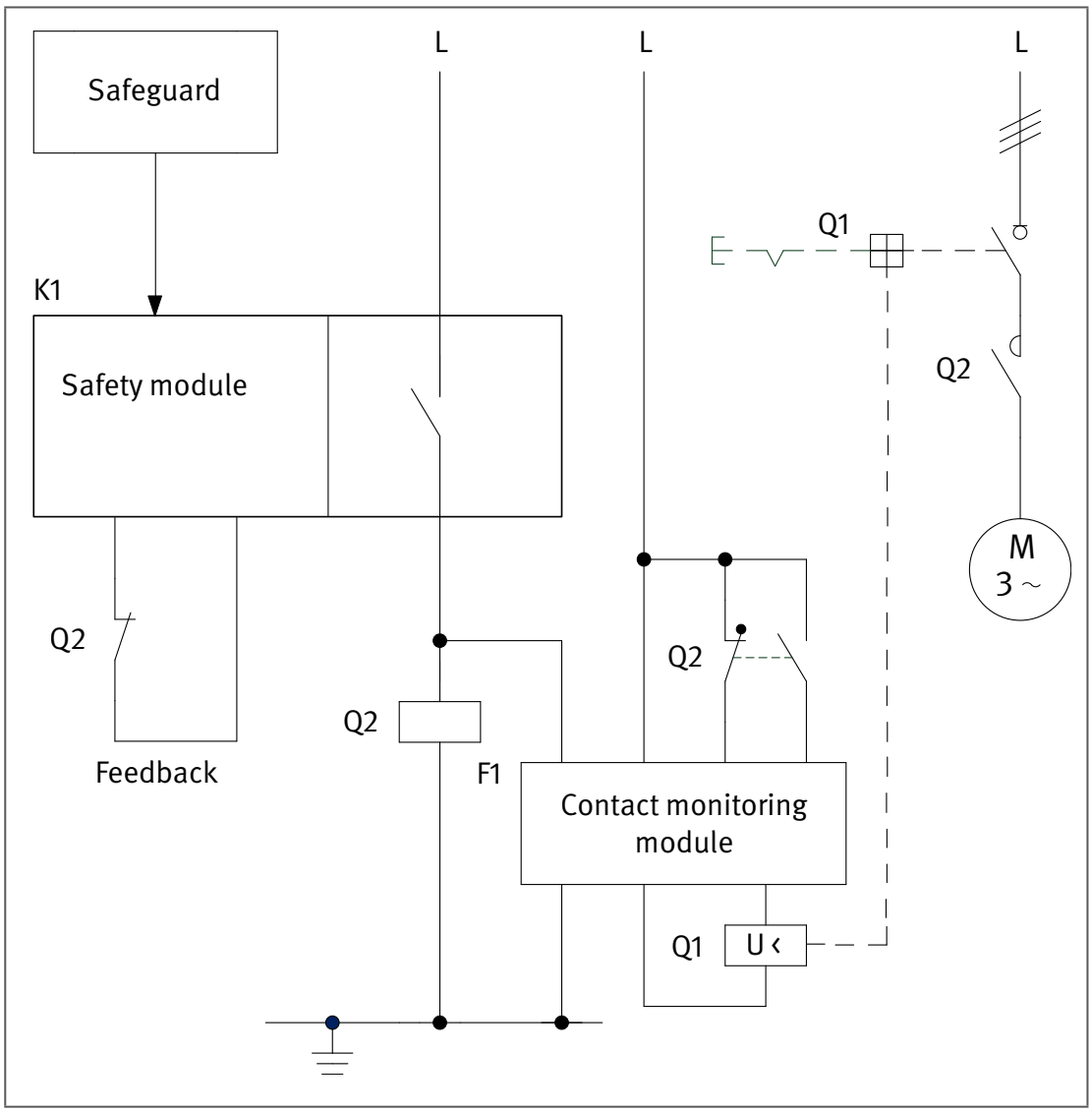


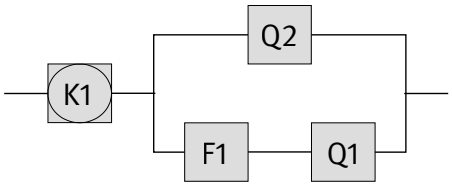
Figure 8.58: Initiation of STO (safe torque off) by means of a safety module and contactor monitoring module

Safety function

- Safety-related stop function, initiated by a guard: opening of the interlocking device initiates the safety function STO (safe torque off).

Functional description

- A hazard zone is safeguarded by means of a guard, opening of which is detected by a safety module K1. The safety module actuates a contactor Q2 and a combination comprising a contactor monitoring module F1 and an undervoltage release Q1. The dropping-out of Q2 interrupts hazardous movements and prevents hazardous states from arising. The contactor monitoring module F1 has the function of monitoring the main contacts of the contactor Q2 for contact welding. Should Q2 fail to drop out, F1 trips the upstream circuit-breaker or motor starter Q1 via the latter's undervoltage release. The circuit-breaker or motor starter then switches off the motor.
- The safety function is preserved in the event of a component failure.
- An accumulation of faults between two successive actuations can lead to loss of the safety function.



Design features

- The circuit-breaker Q1 is checked regularly by means of a test function that is to be implemented manually. The interval between the tests should not exceed one-hundredth of the $MTTF_D$ of Q1; the test could be performed for example during maintenance of the machine. The contactor Q2 is tested continually by the contactor monitoring module. Loss of the safety function between the tests, as is possible with Category 2, cannot occur. The single-fault safety is thus assured and the requirements of Category 3 are met.
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- For reasons of simplification, details of the safeguard have been omitted from the presentation.
- The safeguard acts upon a safety module K1 that satisfies all requirements for Category 3 or 4 and PL e.
- The auxiliary contacts of the contactor Q2 are mechanically linked in accordance with IEC 60947-5-1, Annex L.
- Faults are analysed for Q2 (with mirror contacts) and for the internal relay of the contactor monitoring module F1 as for mechanically linked contacts.

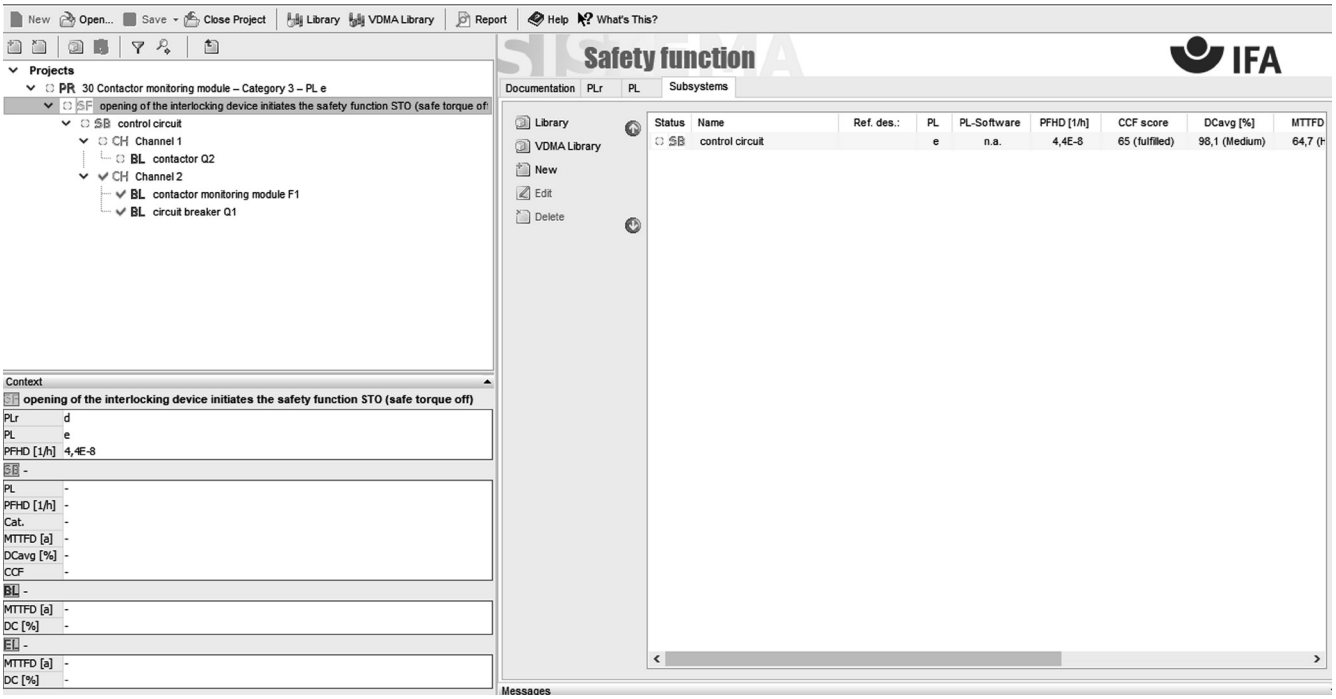
Remark

- Consideration must be given to the response time caused by the contactor monitoring module F1 with regard to the dropping-out of Q1.

Calculation of the probability of failure

- The safety function permits division into two subsystems. The subsystem consisting of the safeguard and the safety module K1 is not considered in this example.
- $MTTF_D$: for the contactor monitoring module F1, the $MTTF_D$ is 125 years at a maximum n_{op} of 350,400 cycles per year [M]. Under inductive load (AC 3), the B_{10D} value attained for Q1 is 10,000 switching cycles and the B_{10D} value attained for Q2 1,300,000 switching cycles. With assumed actuation daily on 365 working days, n_{op} is 365 cycles per year for Q1, and the $MTTF_D$ is 274 years. At 365 working days, 16 working hours and a cycle time of 1 minute, n_{op} is 350,400 cycles per year for Q2, and the $MTTF_D$ is 37 years. For the channel consisting of F1 and Q1, this results in an $MTTF_D$ of 85 years. Overall, the resulting symmetrized $MTTF_D$ value per channel is 64 years (“high”).
- DC_{avg}: the *DC* of 99% for Q2 is based upon testing by means of the contactor monitoring module F1. A *DC* of 99% for F1 is achieved by fault-detection measures within the contactor monitoring module. The circuit-breaker Q1 is tested by means of the manual test function that is to be implemented; this produces a *DC* of 90%. A *DC* of 99% is substituted for F1. Averaging thus yields a DC_{avg} of 98% (“medium”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The subsystem, comprising Q1, Q2 and F1, satisfies Category 3 with a high $MTTF_D$ (64 years) and medium DC_{avg} (98%). This results in an average probability of dangerous failure of $4.4 \cdot 10^{-8}$ per hour. This satisfies PL e. Following addition of the subsystem, comprising safeguard and safety module K1, the PL may under certain circumstances be lower.
- In consideration of estimation erring on the safe side as described above, a T_{10D} value of 3.7 years is produced for the wearing element Q2 for replacement as specified.

Figure 8.59:
Determining of the PL by means of SISTEMA



8.2.31 Pneumatic valve control (subsystem) – Category 4 – PL e (Example 31)

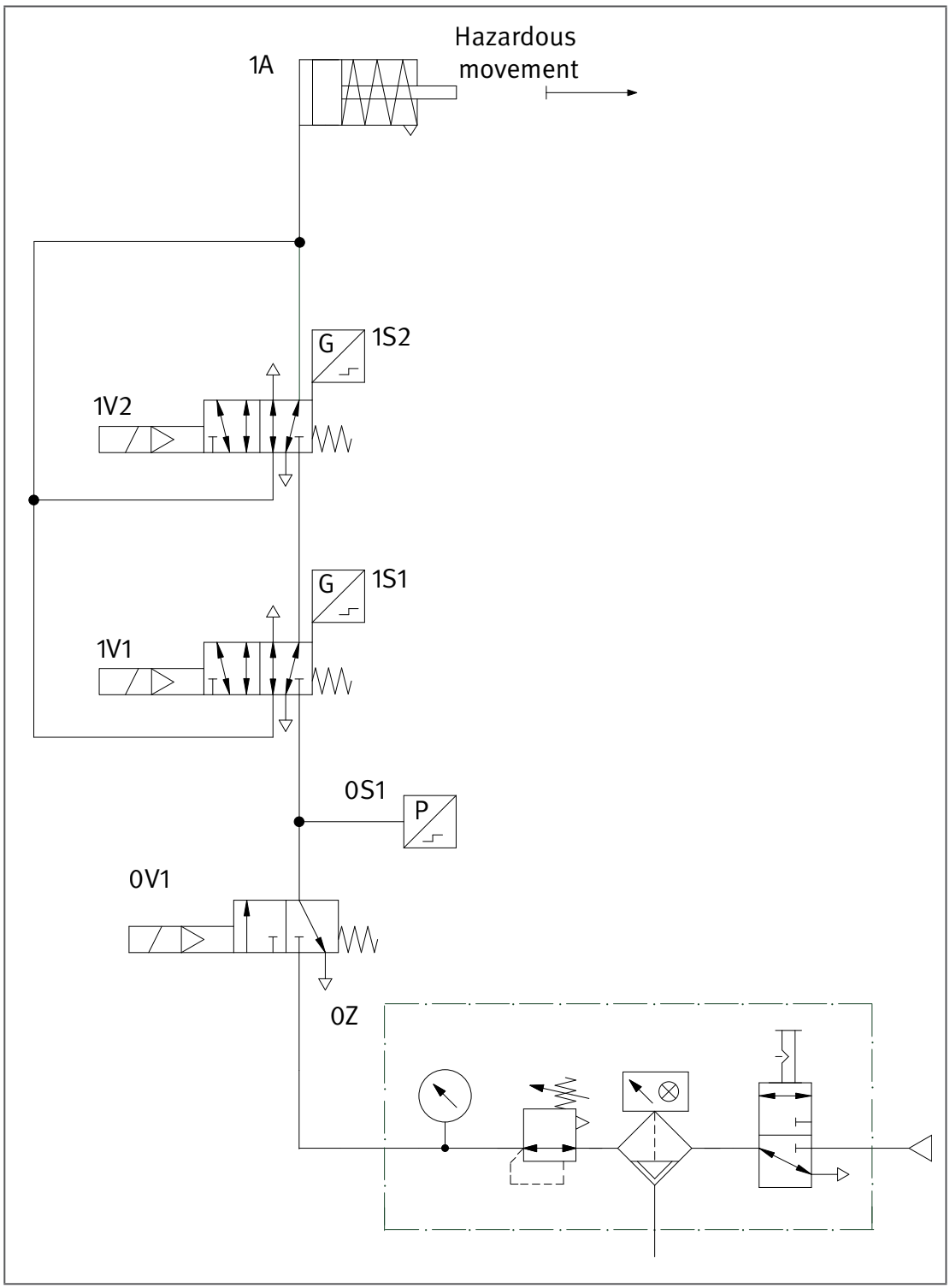
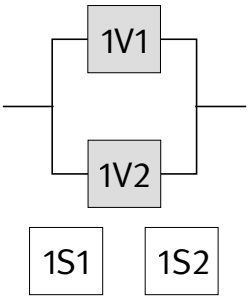


Figure 8.60
Tested pneumatic valves for redundant control of hazardous movements

Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position, implemented by safety sub-function SDE.
- Only the pneumatic part of the control system is shown here, in the form of a subsystem. Further SRP/CS (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.



Functional description

- A hazardous movement of the cylinder is controlled redundantly by the valves 1V1 and 1V2. The movements can be halted either by the directional control valve 1V1 or 1V2.
- Failure of one of these valves alone does not result in loss of the safety function.
- Should at least one of the control signals be cancelled, the piston side of the cylinder is vented.
- A single valve fault is detected by the integral position monitoring function when the control signal is cancelled; following a fault, initiation of the next hazardous movement is prevented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V1 and 1V2 are directional control valves with sufficient overlap, spring-return and electrical position monitoring.
- Cancellation of the control signals places the valve in the safety-oriented switching position.
- Signal processing by the electrical position monitoring function satisfies the relevant requirements for the control of failures.

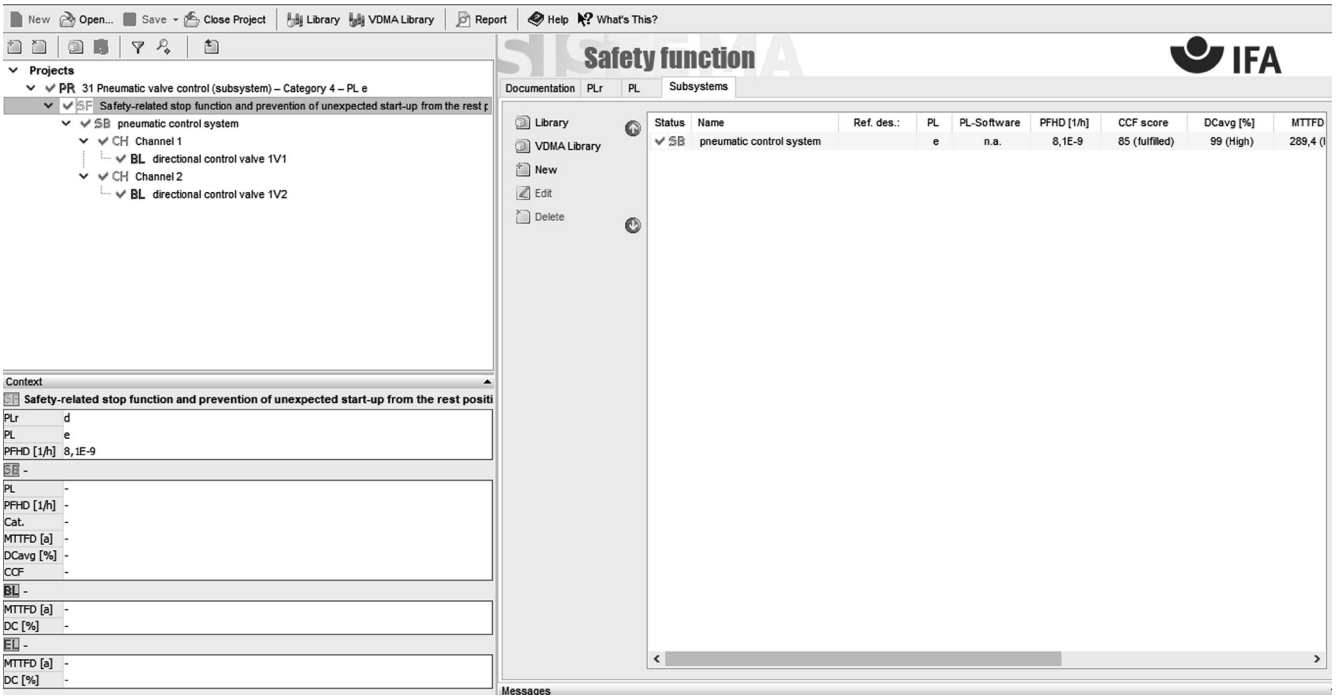
Calculation of the probability of failure

- $MTTF_D$: a B_{10D} value of 20,000,000 cycles [M] is assumed for the directional control valves. At 240 working days, 16 working hours and a cycle time of 20 seconds, n_{op} is 691,200 cycles per year and the $MTTF_D$ is 289 years (“high”). This is also the $MTTF_D$ value per channel.
- DC_{avg}: direct monitoring of the switching states yields a *DC* of 99% for 1V1 and 1V2. The resulting DC_{avg} is also 99% (“high”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements satisfies Category 4 with a high $MTTF_D$ (289 years) and a high DC_{avg}(99%). This results in an average probability of dangerous failure of $8.1 \cdot 10^{-9}$ per hour. This satisfies PL e. Following the addition of further SRP/CS in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.

More detailed reference

- VDMA technical rule 24584: Safety functions of regulated and unregulated (fluid) mechanical systems (08.16)

Figure 8.61:
Determining of the PL by means of SISTEMA



8.2.32 Hydraulic valve control (subsystem) – Category 4 – PL e (Example 32)

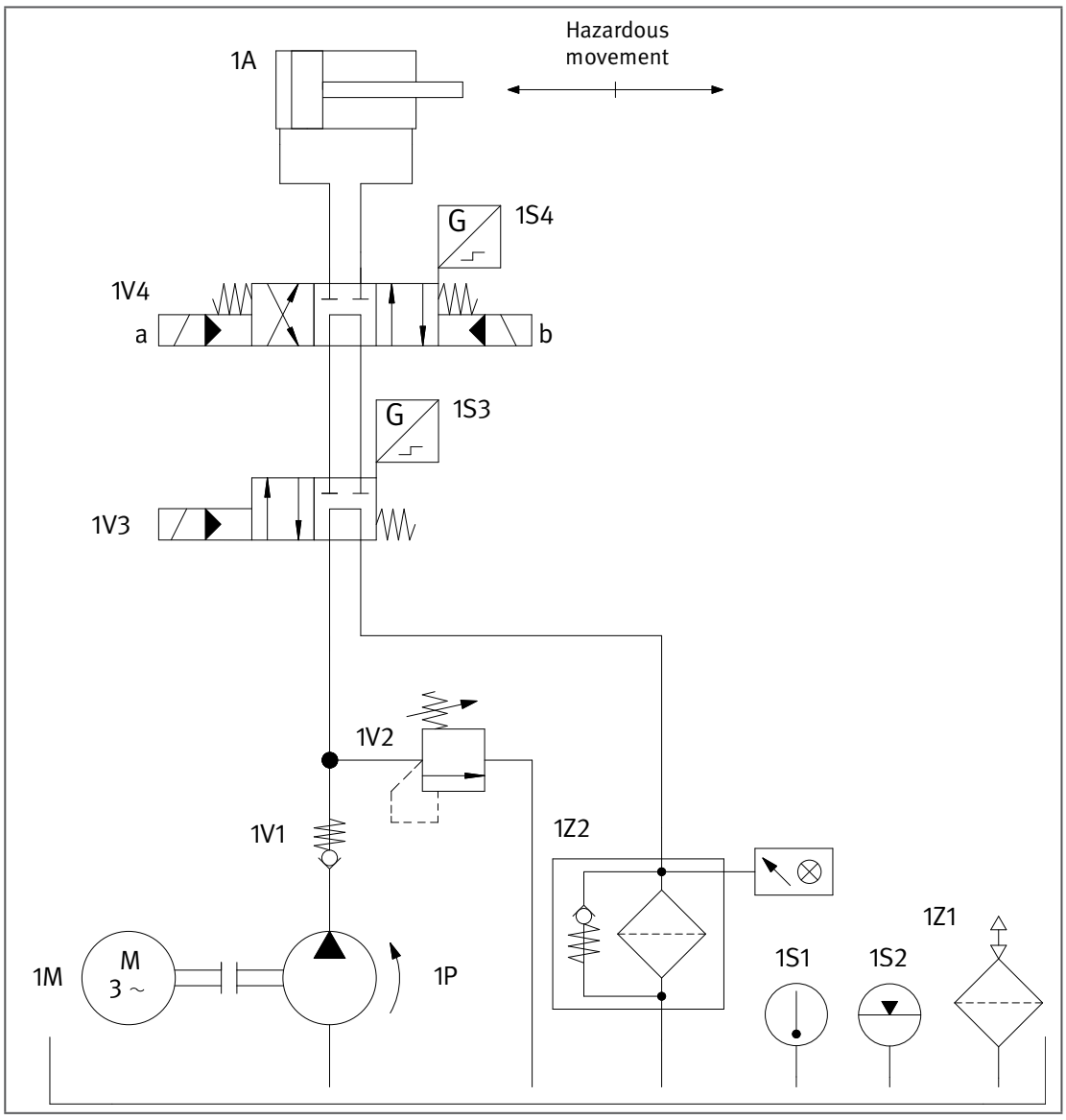


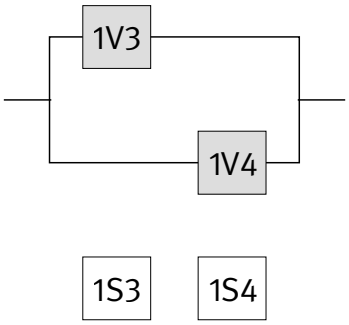
Figure 8.62: Tested hydraulic valves for redundant control of hazardous movements

Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control system is shown here, in the form of a subsystem. Further SRP/CS (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are controlled by two directional control valves (1V3 and 1V4).
- Failure of one of the two valves alone does not result in loss of the safety function.
- The two directional control valves are actuated cyclically.
- Each directional control valve is equipped with a direct position monitor (1S3 and 1S4). Failure of either of the two directional control valves is detected; following a fault, initiation of the next hazardous movement is prevented.



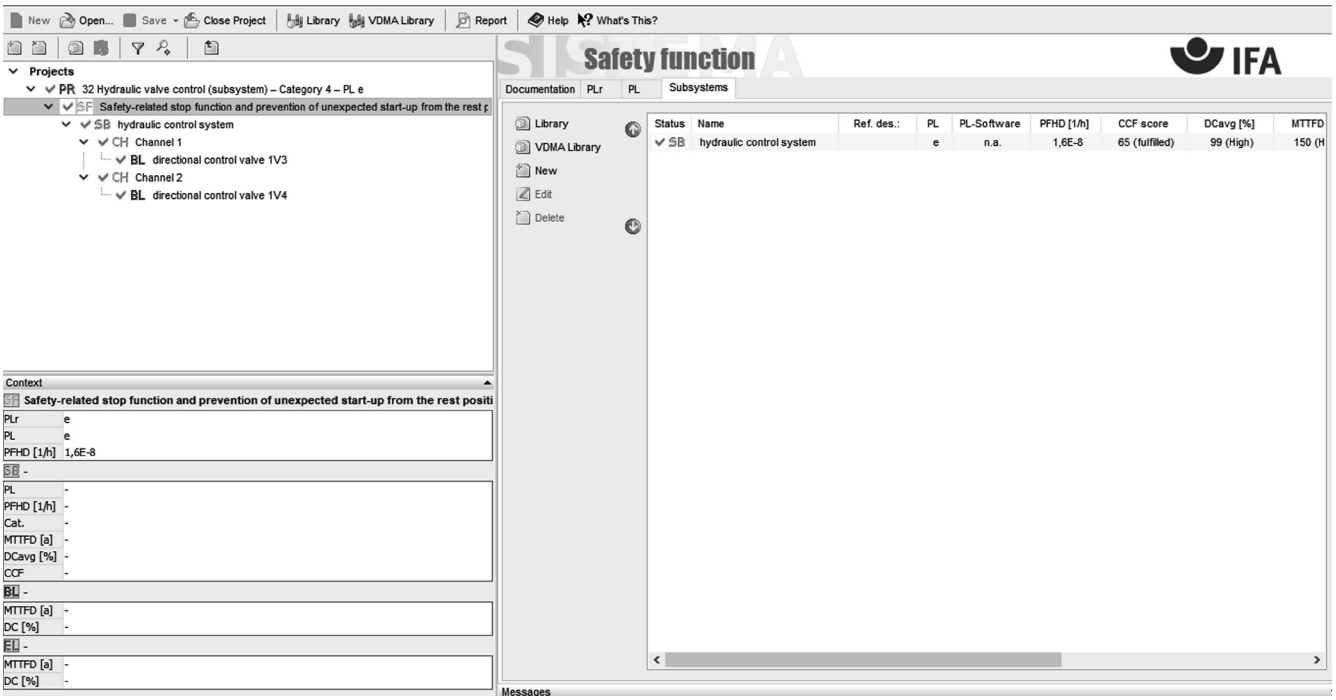
Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- Directional control valves 1V3 and 1V4 possess a closed centre position with sufficient overlap, spring-centred central position/return, and electrical position monitoring.
- The safety-oriented switching position is assumed from any position by cancellation of the control signal.
- Signal processing by the electrical position monitoring function satisfies the relevant requirements for the control of failures.

Calculation of the probability of failure

- $MTTF_D$: an $MTTF_D$ of 150 years is assumed for the directional control valves 1V3 and 1V4 [M].
- DC_{avg}: the *DC* of 99% for the directional control valves 1V3 and 1V4 is based upon direct monitoring of the switching states. Averaging thus produces a DC_{avg} also of 99% (“high”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the hydraulic control elements satisfies Category 4 with a high $MTTF_D$ and high DC_{avg} (99%). This results in an average probability of dangerous failure of $1.6 \cdot 10^{-8}$ per hour. This satisfies PL e. Following the addition of further SRP/CS in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.

Figure 8.63:
Determining of the PL by means of SISTEMA



8.2.33 Electrohydraulic press control – Category 4 – PL e (Example 33)

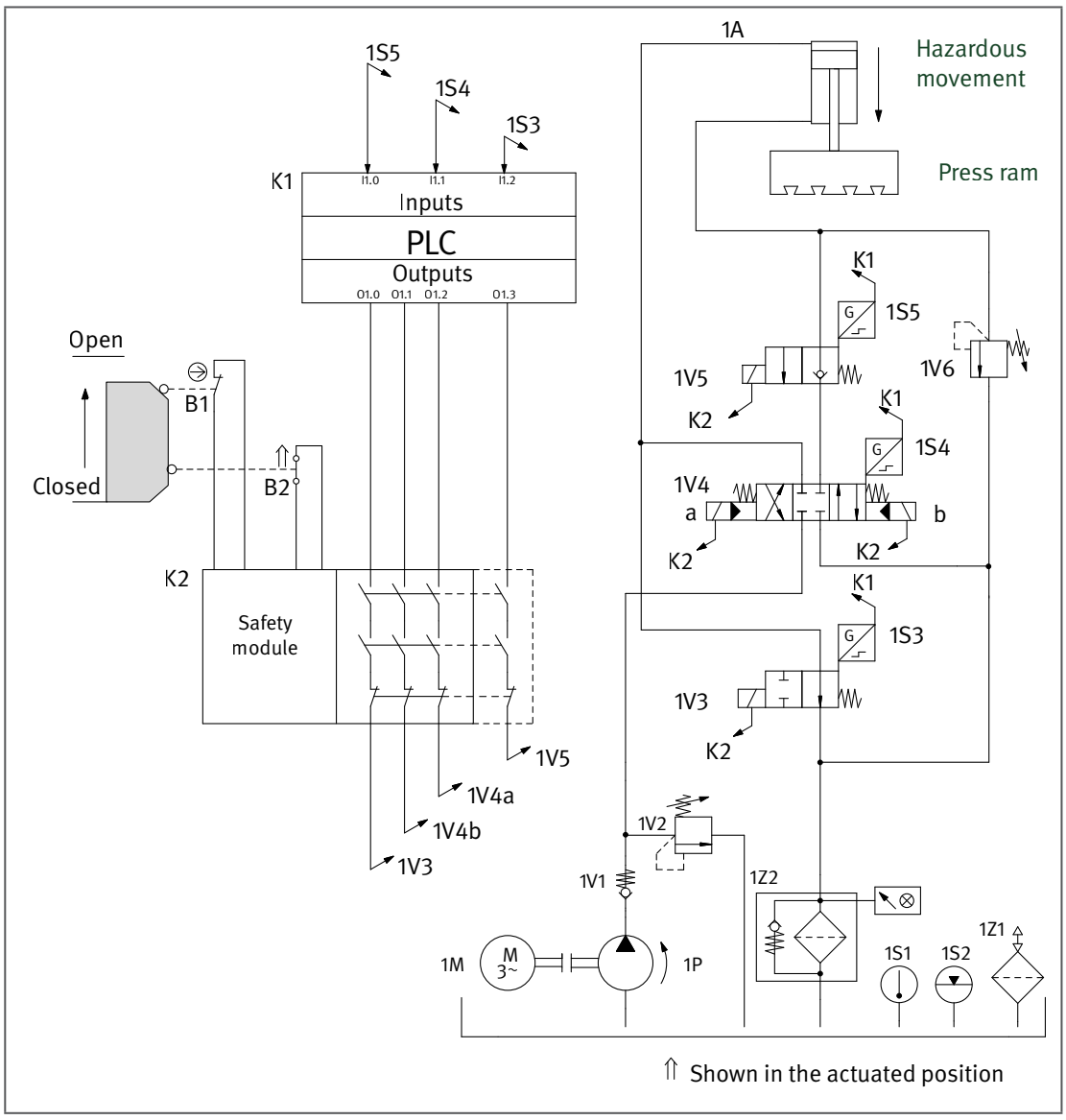


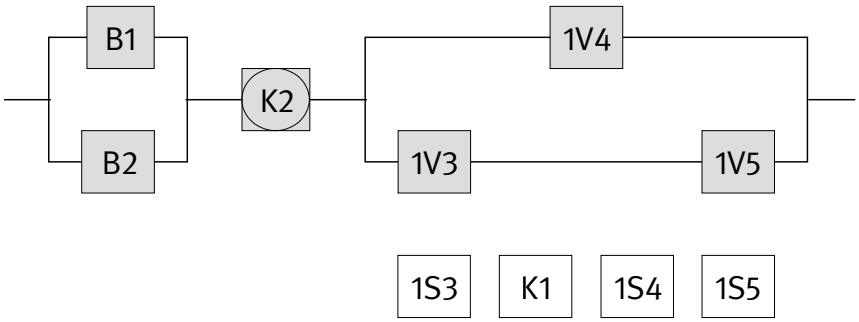
Figure 8.64: Press control, electrical monitoring of a movable guard with hydraulic stopping of the hazardous movement

Safety function

- Safety-related stop function, initiated by a safeguard: stopping of the hazardous movement

Functional description

- The hazard zone is safeguarded by means of a movable guard, the position of which is detected by two position switches B1 and B2 in the form of a break contact/make contact combination. The signals are read into a standard safety module K2, which is looped into the enabling path for the electrical pilot control K1 (a conventional PLC) for the hydraulic actuators. Hazardous movements or states are controlled on the actuator side by three directional control valves (1V3, 1V4 and 1V5). In response to a demand of the safety function, all valves are de-energized electrically by K2, and are placed by their return springs in the closed centre position (1V4) or closed position (1V3 and 1V5). The oil return from the end of the cylinder above the piston to the reservoir is interrupted simultaneously by the valves 1V4 and 1V5. 1V5 is a poppet valve that is designed to shut off the volumetric flow without leakage. Valve 1V4, which also controls the direction of movement of the cylinder, is a piston-type directional control valve that also exhibits a certain degree of leakage in the closed centre position. Although the valve 1V3 is only indirectly involved in the stop function, it may have a negative impact upon the safety function. Should 1V3 and 1V4 stick at



the same time, pressure builds up at the end of the cylinder above the piston, whilst the end below it remains shut off by 1V5. Owing to the pressure ratio in the cylinder, the pressure-relief valve 1V6 then opens and the ram of the press drops.

- Failure of one of the valves does not result in loss of the safety function. All valves are actuated cyclically.
- Each valve is equipped with a position monitoring facility, 1S3, 1S4 and 1S5, for fault detection purposes. Failure of any of the three valves is detected in the conventional PLC K1, which prevents the next hazardous movement from being initiated following a fault.
- A single fault in one safety component does not result in loss of the safety function. In addition, single faults are detected at or prior to the next demand. An accumulation of undetected faults does not result in loss of the safety function.

Design features

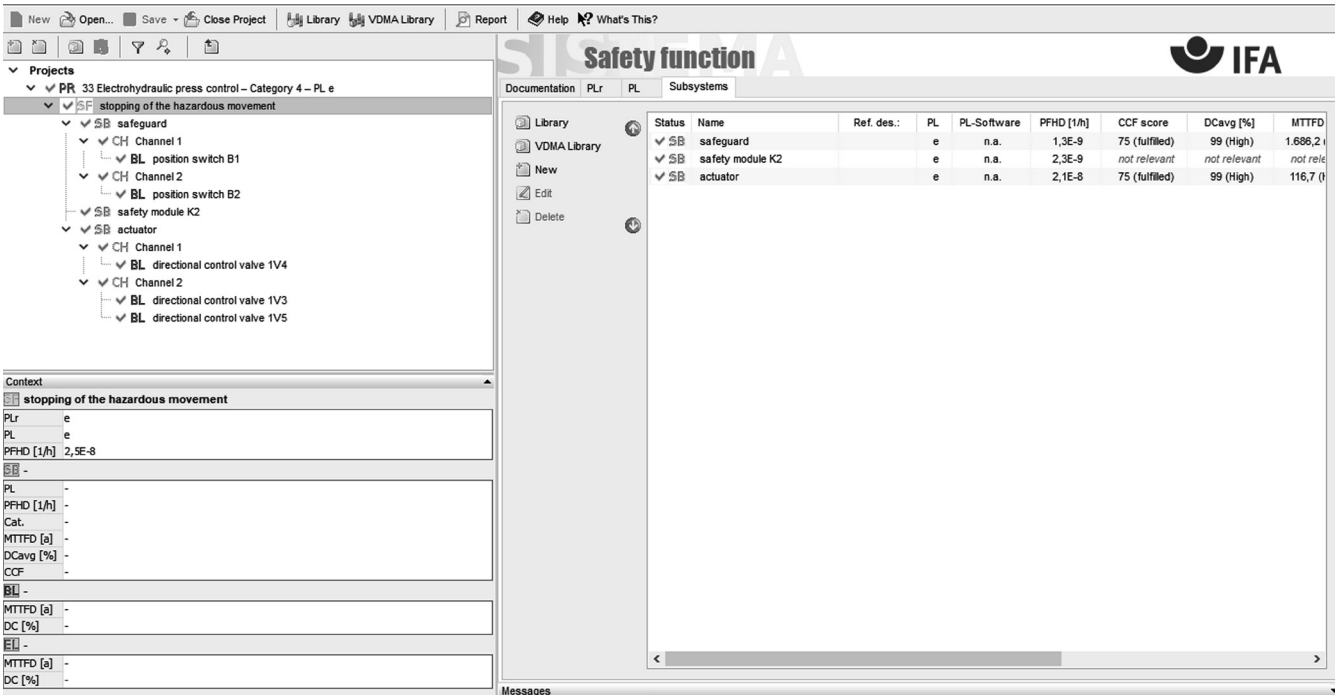
- Basic and well-tried safety principles and the requirements of Category B are observed. Protective circuits (such as contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the guard is assured for actuation of the position switch.
- The switch B1 is a position switch with a direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The safety module K2 satisfies all requirements for Category 4 and PL e.
- The supply conductors to the position switches are laid separately or with protection.
- A standard PLC without safety functions is employed for K1.
- The valves 1V3, 1V4 and 1V5 possess a closed centre position/closed position with sufficient overlap, spring-centred central position/return, and position monitoring.
- The safety-oriented switching position is assumed from any position by cancellation of the control signal.
- The pressure-relief valve 1V6 for protecting the cylinder 1A and the components below it against the effect of the pressure ratio satisfies the requirements of EN 693:2001, subclause 5.2.4.4.

Calculation of the probability of failure

- K2 is considered as a subsystem with a probability of failure of $2.3 \cdot 10^{-9}$ per hour [M]. The remaining part of the control system is grouped separately by electromechanical and hydraulic components to form two Category 4 subsystems, the probability of failure of which is calculated below.
- $MTTF_D$: for the position switch B1 with direct opening action, the B_{10D} is $20 \cdot 10^6$ switching cycles [M]. For the electrical make contact of the position switch B2, the B_{10D} is 1,000,000 switching cycles [M]. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} is 35,040 cycles per year for these components, and the $MTTF_D$ is 5,707 years for B1 and 285 for B2. An $MTTF_D$ of 150 years [M] is assumed for each of the valves 1V3, 1V4 and 1V5. This yields an $MTTF_D$ value per channel of 100 and 88 years (“high”) respectively for the two subsystems.

- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the two switching states in K2. The *DC* of 99% for the two valves is based upon direct monitoring of the switching states by the PLC K1. This results in a DC_{avg} of 99% (“high”) for the two subsystems.
- Measures against common cause failures (75 points) for the two subsystems: separation (15), well-tried components (5), FMEA (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)
- The electromechanical and hydraulic parts of the control system correspond to Category 4 with a high $MTTF_D$ and a high DC_{avg} (99%). This results in an average probabilities of dangerous failure of $1.3 \cdot 10^{-9}$ per hour and $2.1 \cdot 10^{-8}$ per hour. Addition inclusive of K2 produces an average probability of dangerous failure for the complete safety function of $2.5 \cdot 10^{-8}$ per hour. This satisfies PL e.

Figure 8.65:
Determining of the PL by means of SISTEMA



8.2.34 Position monitoring of movable guards – Category 4 – PL e (Example 34)

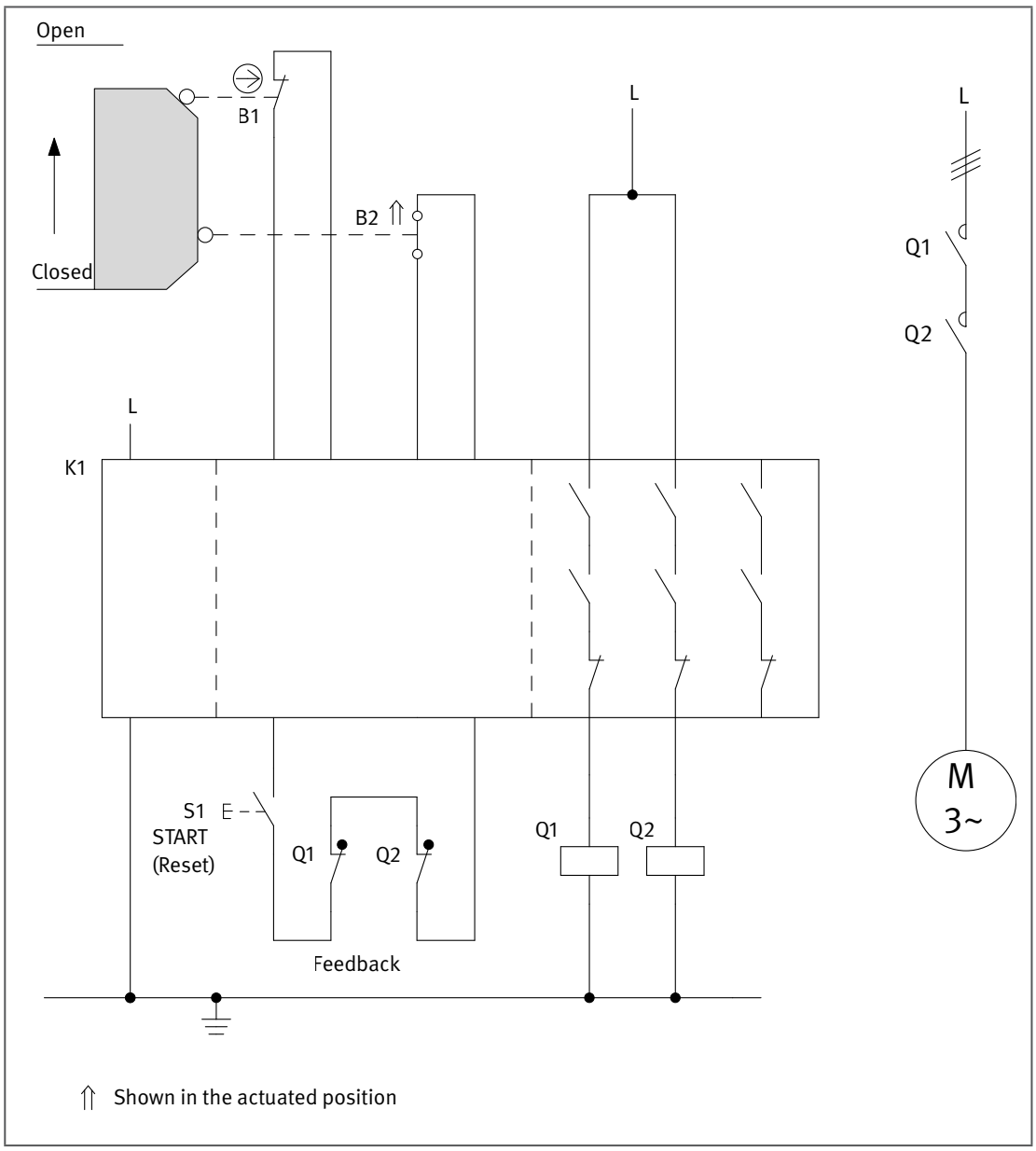


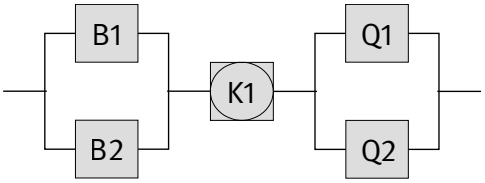
Figure 8.66: Position monitoring of movable guards by means of a safety module

Safety function

- Safety-related stop function, initiated by a movable guard: opening of the movable guard (safety guard) initiates the safety function STO (safe torque off).

Functional description

- A hazard zone is safeguarded by a movable guard (safety guard). Opening of the safety guard is detected by two position switches B1/B2 employing a break contact element/make contact element combination, and evaluated in a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.
- The position switches are monitored for plausibility in K1 for the purpose of fault detection. Faults in Q1 and Q2 are detected by a start-up test in K1. A start command is successful only if Q1 and Q2 had previously dropped out. Start-up testing by opening and closing of the guard is not required.



- The safety function remains intact in the event of a component failure. Faults are detected during operation or at actuation (opening and closing) of the guard by the dropping out of Q1 and Q2 and operating inhibition.
- An accumulation of more than two faults in the period between two successive actuations can lead to loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection) as described in the initial paragraphs of chapter 8 are implemented.
- A stable arrangement of the guards is assured for actuation of the position switches.
- The switch B1 is a position switch with direct opening action in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to position switches B1 and B2 are laid separately or with protection.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactors Q1 and Q2 possess mirror contacts in accordance with IEC 60947-4-1, Annex F.

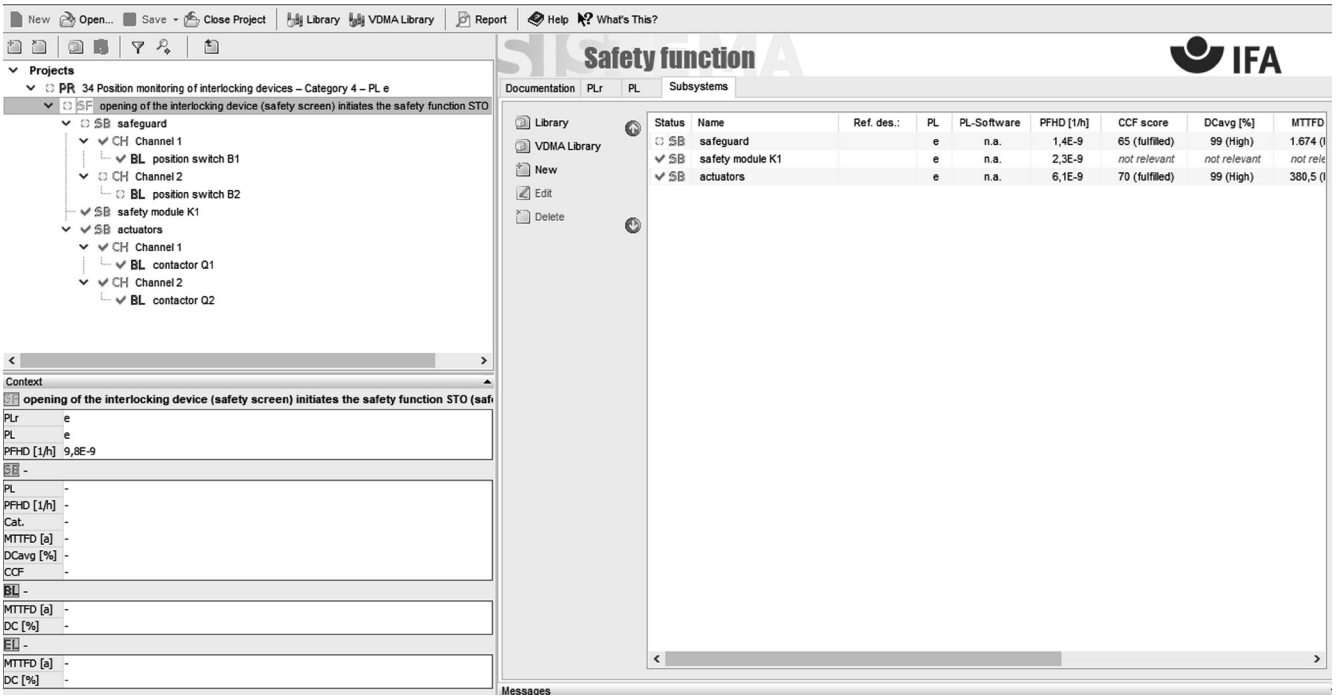
Remarks

- Category 4 is not observed if several mechanical position switches for different guards are cascaded (connected in a series arrangement), since this limits fault detection in the switches (see Annex E).

Calculation of the probability of failure

- The circuit arrangement can be divided into three subsystems as shown in the safety-related block diagram. The probability of failure of the standard safety module K1 is added at the end of the calculation ($2.3 \cdot 10^{-9}$ per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows.
- $MTTF_D$: for the position switch B1 with roller actuation, the B_{10D} is $20 \cdot 10^6$ operation cycles [M]. For the position switch B2 (make contact element), the B_{10D} is $1 \cdot 10^5$ operation cycles [M]. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} for these components is 5,840 cycles per year and the $MTTF_D$ is 1,674 years for B1 and B2. For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical durability of 1,000,000 operation cycles [M]. On the assumption that 50% of failures are dangerous, the B_{10D} value is produced by doubling of the B_{10} value. The value assumed above for n_{op} results in an $MTTF_D$ of 3,424 years per channel for Q1 and Q2. The position switch B2 exhibits a limited operation time of 17.1 years. Its replacement in good time is recommended.
- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the break/make contact element combinations in K1. The *DC* of 99% for contactors Q1 and Q2 is derived from regular monitoring by K1 during start-up. The *DC* values stated correspond to the DC_{avg} for the subsystem concerned.
- Adequate measures against common cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)
- The subsystems B1/B2 and Q1/Q2 each satisfy Category 4 with a high $MTTF_D$ and high DC_{avg} (99%). This results in an average probability of dangerous failure of $2.3 \cdot 10^{-9}$ per hour for each subsystem. Following addition of the subsystem K1, the average probability of dangerous failure is $4.6 \cdot 10^{-9}$ per hour. This satisfies PL e.

Figure 8.67:
Determining of the PL by means of SISTEMA



8.2.35 Two-hand control – Category 4 – PL e (Example 35)

Changes with respect to the second edition (BGIA Report 2/2008e):

The PFH_D value for the logic unit K1 and the B_{10D} values for the pushbuttons S1 and S2 were brought into line with more realistic manufacturers‘ values

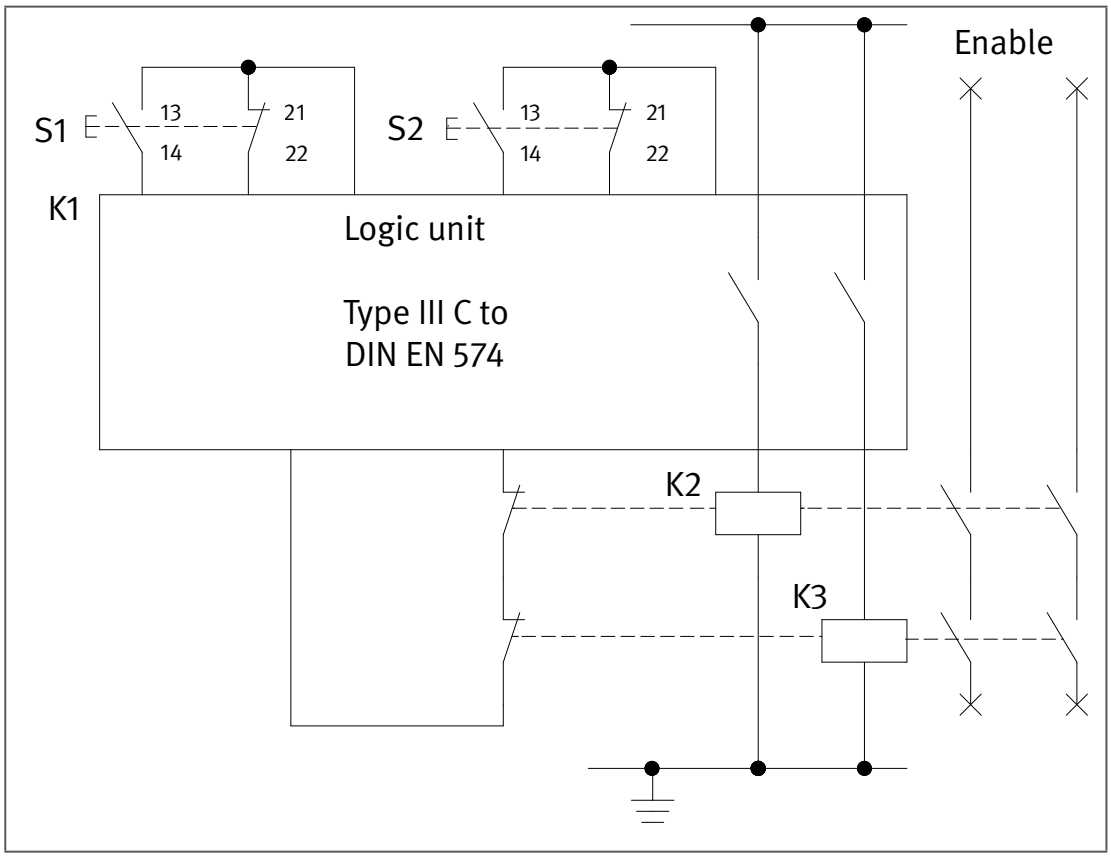


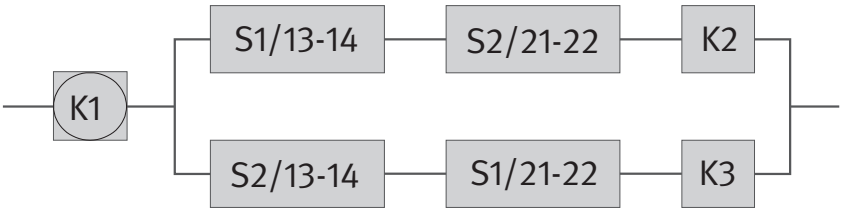
Figure 8.68: Two-hand control, signal processing by a logic device with downstream contactor relays

Safety function

- Controlled location of the operator‘s hands outside the hazard zone during a hazardous movement: when at least one of the two pushbuttons S1/S2 is released, enabling is cancelled and remains blocked until both pushbuttons are released and pressed again synchronously.

Functional description

- The logic unit K1 monitors operation of the actuators (pushbuttons) S1 and S2. Only when both pushbuttons are operated synchronously (i.e. within a maximum time of 500 ms as specified in EN 574) from within the released state do the contactor relays K2 and K3 pick up, resulting in enabling. When at least one of the pushbuttons S1/S2 is released, K2/K3 cancel enabling.
- K2 and K3 have the function of contact multiplication/load adaptation. The actual prevention of the hazardous movement, for example by separation of the electrical or hydraulic energy, is dependent upon the application and is not shown here.
- Faults in the actuating mechanism are detected in S1/S2 to the greatest extent possible by the use of two contacts employing different principles (break and make contact combination). In accordance with Recommendation for Use (RfU) CNB/M/11.033/R/E Rev 06, mechanical faults on the actuators can be excluded when they satisfy IEC 60947-5-1.



- Faults in S1/S2 and in K2/K3 (with break contacts in the feedback circuit) are detected in K1 and lead to sustained de-energization via K2 and K3. All individual faults are detected at or prior to the next demand of the safety function.
- Frequent actuation of the electromechanical elements results in a sufficiently high test rate (forced dynamics).

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (such as contact protection), as described in subclause 8.1, are implemented.
- The actuators S1 and S2 of the two-hand control satisfy IEC 60947-5-1. In accordance with RfU CNB/M/11.033/R/E Rev 06, mechanical faults can therefore be excluded.
- Faults in the conductors to S1 and S2 are detected in the logic device. If this were not possible, the conditions to EN ISO 13849-2, Table D.4 for a fault exclusion for conductor short circuits would have to be observed. Owing to the low currents, pushbuttons with gold-plated contacts are recommended.
- Refer to EN 574, subclauses 8 and 9 with regard to fitting of the pushbuttons and measures for the avoidance of accidental actuation and defeating. The safety distance from the hazard zone must be sufficiently great.
- The logic unit K1 satisfies Type III C to EN 574, with self-monitoring and detection of internal faults. K1 is a tested safety component for use in Category 4 and PL e.
- The contactor relays K2 and K3 possess mechanically linked break contacts in accordance with IEC 60947-5-1, Annex L for feedback.

Remarks

- The example shown is suitable for application for example on mechanical presses (EN 692).

Calculation of the probability of failure

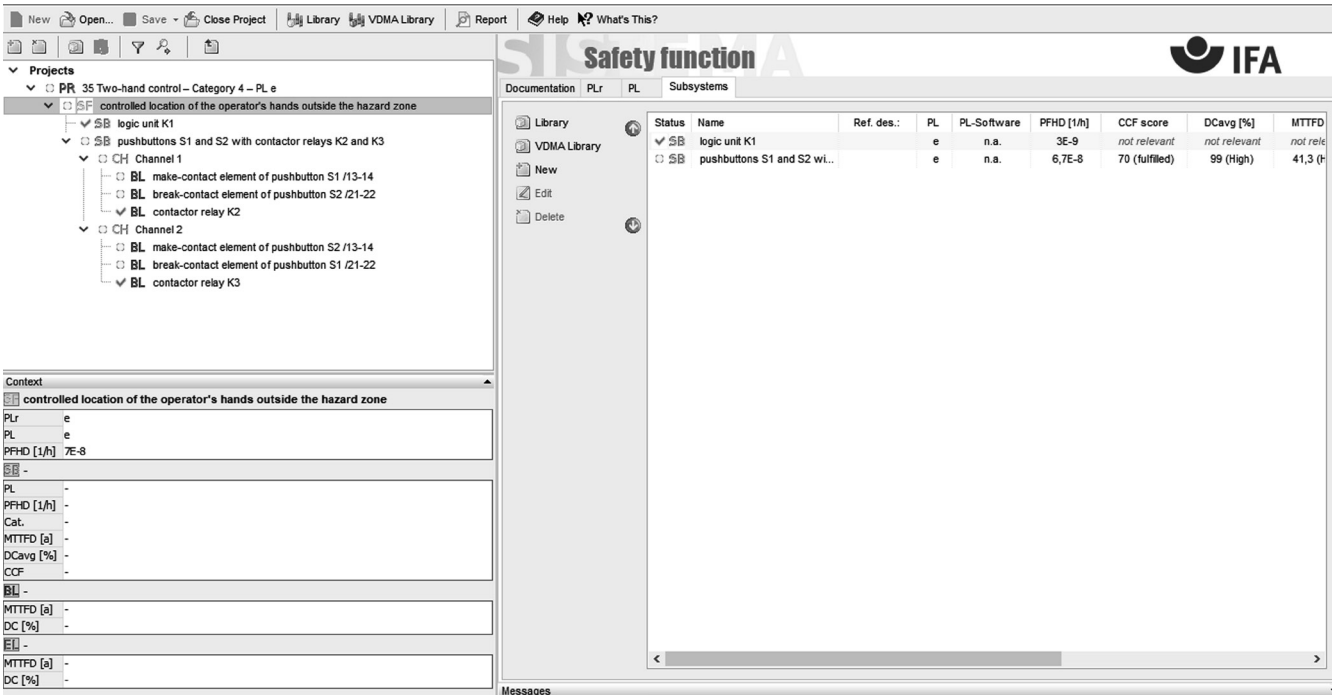
- K1 is considered as a subsystem with a probability of failure of $3.0 \cdot 10^{-9}$ per hour [M]. The remaining part of the control system is grouped to form a Category 4 subsystem the probability of failure of which is calculated below.
- Since S1 and S2 must initiate de-energization independently of each other when released, they are connected logically in series. For this purpose, one make contact 13-14 and one break contact 21-22 were each assigned to a control channel. The safety-related block diagram differs substantially in this respect from the functional circuit diagram. If the reliability data are available only for the pushbuttons as a whole (actuation mechanism and break and make contacts), the failure values for the pushbuttons may be employed as an estimation erring on the safe side for the failure values for the contacts (plus operating mechanism).
- $MTTF_D$: owing to the defined control current generated by K1 (low electrical load; the mechanical durability of the contacts is the determining factor), B_{10D} values of 2,000,000 switching cycles [M] are assumed in each case for S1 and S2. At 240 working days, 8 working hours and a cycle time of 30 seconds, n_{op} is 230,400 cycles per year for these components, and the $MTTF_D$ is 86.8 years per contact. Since K2 and K3 also switch control currents, B_{10D} values of 20,000,000 cycles [S] and resulting $MTTF_D$ values of 868 years apply to each of them. Should the requirements be higher (longer working hours or a shorter cycle time), higher B_{10D} values validated by the manufacturer may be required for K2/K3. Overall, the resulting $MTTF_D$ value per channel is 41 years (“high”).

- DC_{avg}: a *DC* of 99% for S1 and S2 is achieved by virtue of direct monitoring with the aid of the break/make contact combinations in K1. The *DC* of 99% for K2 and K3 is based upon readback of the mechanically linked break contacts in the feedback circuit of K1. The high frequency of actuation in the application results in frequent testing (see subclause 6.2.14). Averaging results in a DC_{avg} of 99% ("high").
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements satisfies Category 4 with a high $MTTF_D$ per channel (41 years) and high DC_{avg} (99%). For the combination of S1, S2, K2 and K3, the average probability of dangerous failure is calculated at $6.7 \cdot 10^{-8}$ per hour. If a value of $3.0 \cdot 10^{-9}$ per hour [E] for K1 is added, the result is an average probability of dangerous failure of $7.0 \cdot 10^{-8}$ per hour. This satisfies PL e. The probability of failure of downstream power components may have to be added for completion of the safety function.
- The wearing elements S1 and S2 should each be replaced at intervals of approximately eight years (T_{10D}).

More detailed references

- EN 574: Safety of machinery – Two-hand control devices – Functional aspects – principles for design (1996) + A1 (2008). (replacement by EN ISO 13851 is planned)
- Recommendation for Use. Published by: Vertical Group 11 (VG 11) in the Co-ordination of Notified Bodies. http://ec.europa.eu/DocsRoom/documents/14265/attachments/1/translations/en/renditions/native CNB/M/11.033/R/E Rev 06, p. 181, November 2015

Figure 8.69:
Determining of the PL by means of SISTEMA

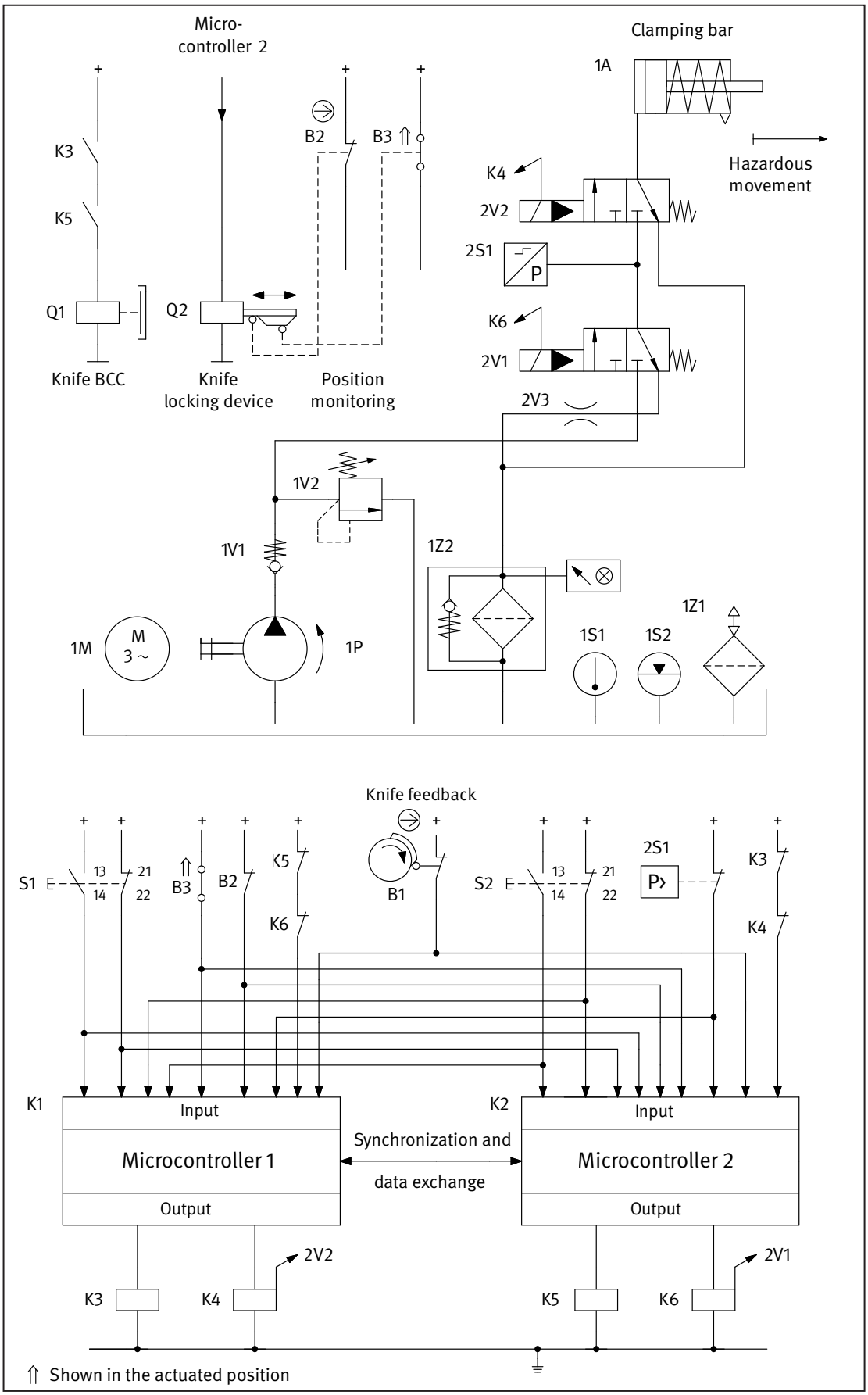


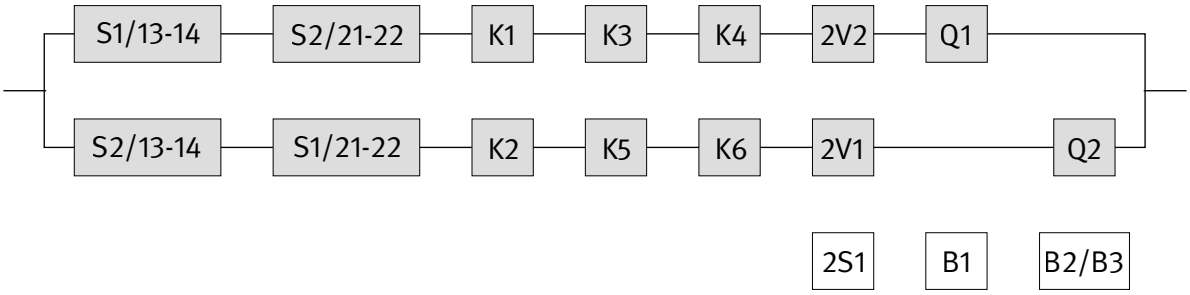
8.2.36 Processing of signals from a light barrier – Category 4 – PL e (Example 36)

This example has been deleted, since the technology is no longer relevant

8.2.37 Paper-cutting guillotine with programmable electronic logic control – Category 4 – PL e (Example 37)

Figure 8.70:
Control of an electric knife drive and a hydraulic clamping bar





Safety function

- Controlled location of a single operator's hands outside the hazard zone during the press and cutting movement: when at least one of the two pushbuttons S1/S2 is released, enabling is cancelled and remains blocked until both pushbuttons are released and pressed again synchronously.

Functional description

- Actuation of the two-hand control (THC) S1 and S2 initiates the hazardous movements (processing cycle) of the clamping bar (hydraulic) 1A and of the knife (electromechanical). If, during this cycle, either of the pushbuttons S1 or S2 is released or a signal change occurs in the peripheral system of the machine (e.g. light curtain, not shown on the diagram) that is not expected by the control system, the cycle is stopped and the machine remains in this safe state. Owing to their immediate physical proximity to each other, the knife and the clamping bar constitute a common hazard zone. The hazard occurs cyclically. The knife is driven by an eccentric drive that draws its energy from a flywheel mass in constant motion. The drive is not shown explicitly. The clamping bar is driven linearly by a hydraulic arrangement employing a pump connected to the drive of the flywheel mass.
- When pushbuttons S1/S2 (THC) are pushed, the signal change is communicated to the two microcontrollers K1 and K2. Provided these signals satisfy the requirements for simultaneity in accordance with the standard (EN 574, Type III C) and all peripheral signals satisfy the condition for a start, K1 and K2 set the outputs for a valid cut request. Each microcontroller monitors both hazardous movements through the contactor relays K3 to K6. The closing movement of the clamping bar 1A can be prevented by the two hydraulic valves 2V1 and 2V2. Actuation of the brake/clutch combination (BCC) Q1 can be prevented via K3 and K5. A suitably dimensioned mechanical knife locking device Q2 must also be enabled cyclically by K2. Should faults be detected in Q1, the knife cycle can therefore be prevented in the following cycle at the latest.
- Faults in the switches S1/S2 or in the contactor relays with mechanically linked readback contacts K3 to K6 are detected in the microcontrollers by cross monitoring. The functioning of 2V1/2V2 is monitored by means of the pressure switch 2S1. Since the microcontrollers perform self-tests in addition in the background during operation, internal faults and faults in the peripherals can be detected here in time.
- All machine states are monitored and controlled by both microcontrollers. The cyclical nature of the cut operation causes all system states to be cycled through and compared with each other. Faults and deviations from defined intermediate states cause the machine to be halted at the latest upon completion of the cycle. This method is implied in the diagram by the signal "Feedback knife" B1 and the signal "Position monitoring" B2/B3 of the "Knife locking device" Q2.
- Brake wear is monitored with the aid of the position switch B1. B1 is actuated and a further cut prevented by the control system in response to the slightest increase in the overrun.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits as described in the initial paragraphs of Chapter 8 are implemented.
- The actuators S1 and S2 of the two-hand control satisfy IEC 60947-5-1.

- B1 and B2 are position switches with direct opening action to IEC 60947-5-1, Annex K.
- K3 to K6 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.
- The supply conductors to the position switches are laid either separately or with protection against mechanical damage.
- The software of the homogeneously redundant microprocessor structure satisfies the requirements of IEC 61508-3, clause 7 for SIL 3.
- A fault exclusion applies for the fault: “complete failure of the brake/clutch combination”, i.e. failure to disengage when the cut enable is cancelled following initiation of a cut. The reasoning for this fault exclusion is based upon many years of experience and the design features of the brake/clutch combination with the possibility of early detection of brake wear.
- The components B1 and B2/B3 are required for implementation of the measures required in EN 1010-3 for stopping and overrun of the knife.

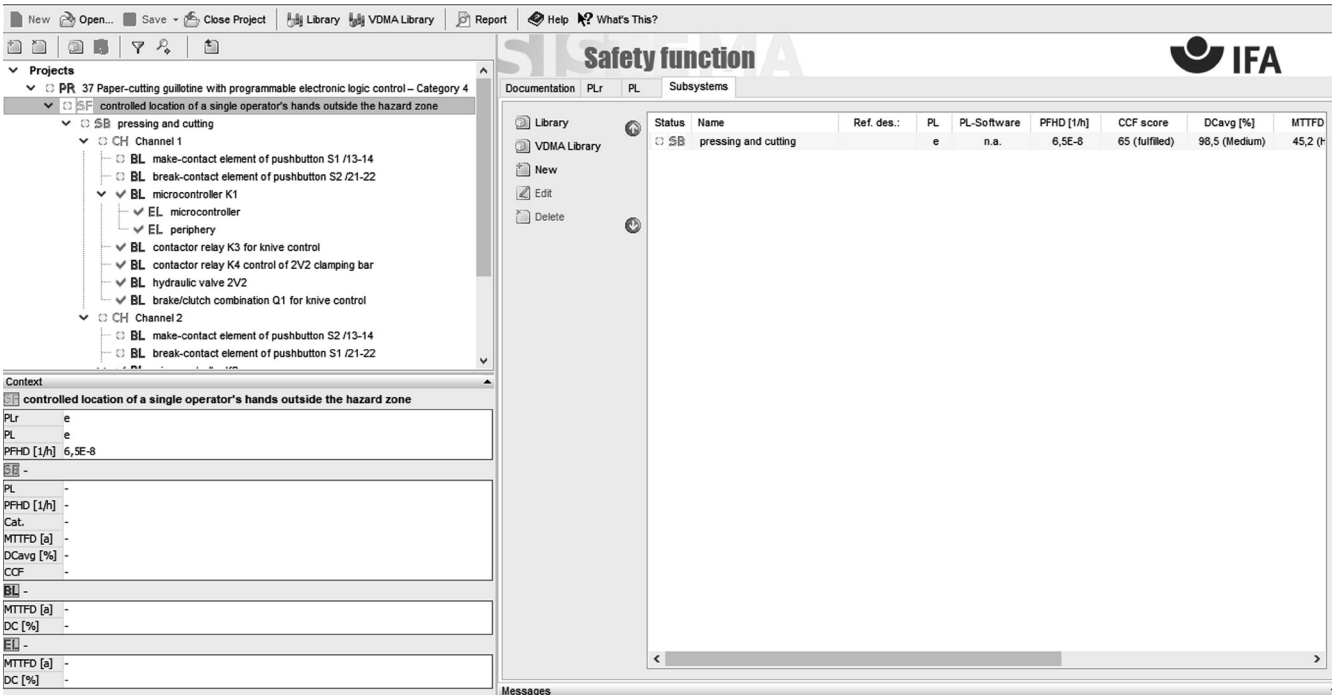
Calculation of the probability of failure

- The designated architecture for Category 4 for actuation of the knife drive and the clamping bar is implemented by two independent channels as described. Since the channels are virtually identical in their arrangement and are analysed with the use of identical numerical data, symmetrization is not required. For the sake of simplification, only single-channel actuation of Q1 is assumed. The probability of failure is therefore slightly lower in practice than that calculated.
- Since S1 and S2 must initiate de-energization independently of each other when released, they are connected logically in series. For this purpose, one make-contact 13-14 and one break-contact 21-22 were each assigned to a control channel. The safety-related block diagram differs substantially in this respect from the functional circuit diagram. The B_{10D} value for each individual contact is employed, constituting an estimation erring on the safe side.
- $MTTF_D$: at 240 working days, 8 working hours and a cycle time of 60 seconds, n_{op} is 115,200 switching cycles per year. Owing to many years‘ experience gained in the construction of these machines, together with relevant quality records and design measures such as the defined control current (low electrical load; the mechanical durability of the contacts is the determining factor), B_{10D} values of 2,000,000 switching cycles [E] each are assumed for S1 and for S2, and thus an $MTTF_D$ of 173 years. An $MTTF_D$ of 878 years [D] is stated for the microcontrollers including peripherals, in accordance with SN 29500-2. At low load, a B_{10D} of 20,000,000 switching cycles [S] and thus an $MTTF_D$ of 1,736 years applies for the contactor relays K3 to K6. The $MTTF_D$ value of 607 years for the brake/clutch combination Q1 is calculated from the B_{10D} value of 7,000,000 cycles [E]. The same value is assumed for the knife locking device Q2 in the second channel. The values for the two directional control valves 2V1 and 2V2 are 150 years [S]. These values result in an $MTTF_D$ one of each channel of 45.2 years (“high”).
- DC_{avg}: the *DC* of 99% for S1/S2 is based upon the cross monitoring of input signals without dynamic test, with frequent signal changes. The *DC* of 90% for K1/K2 is derived from self-tests performed by software and the dynamic cross monitoring of data with expectations regarding timing. The *DC* of 99% for K3 to K6 is derived from plausibility testing by means of mechanically linked contacts. For 2V1/2V2, the *DC* is 99% owing to indirect and direct electrical monitoring of the pressure with frequent signal changes. Wear in the clutch leads to a change in cutting behaviour. This behaviour is monitored by instruments. A *DC* of 99% is therefore assumed for Q1. Failure of Q2 is detected immediately owing to cyclical actuation and the monitoring elements B1 and B3. This is the reasoning for a *DC* of 99%. These values result in a DC_{avg} of 98.5% (within the tolerance for “high”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- For Category 4, the average probability of dangerous failure is $6.5 \cdot 10^{-8}$ per hour. This satisfies PL e.
- With allowance for the estimation erring on the safe side described above, a value of over 17 years (T_{10D}) is produced for the specified replacement of the wearing elements S1 and S2.

More detailed references

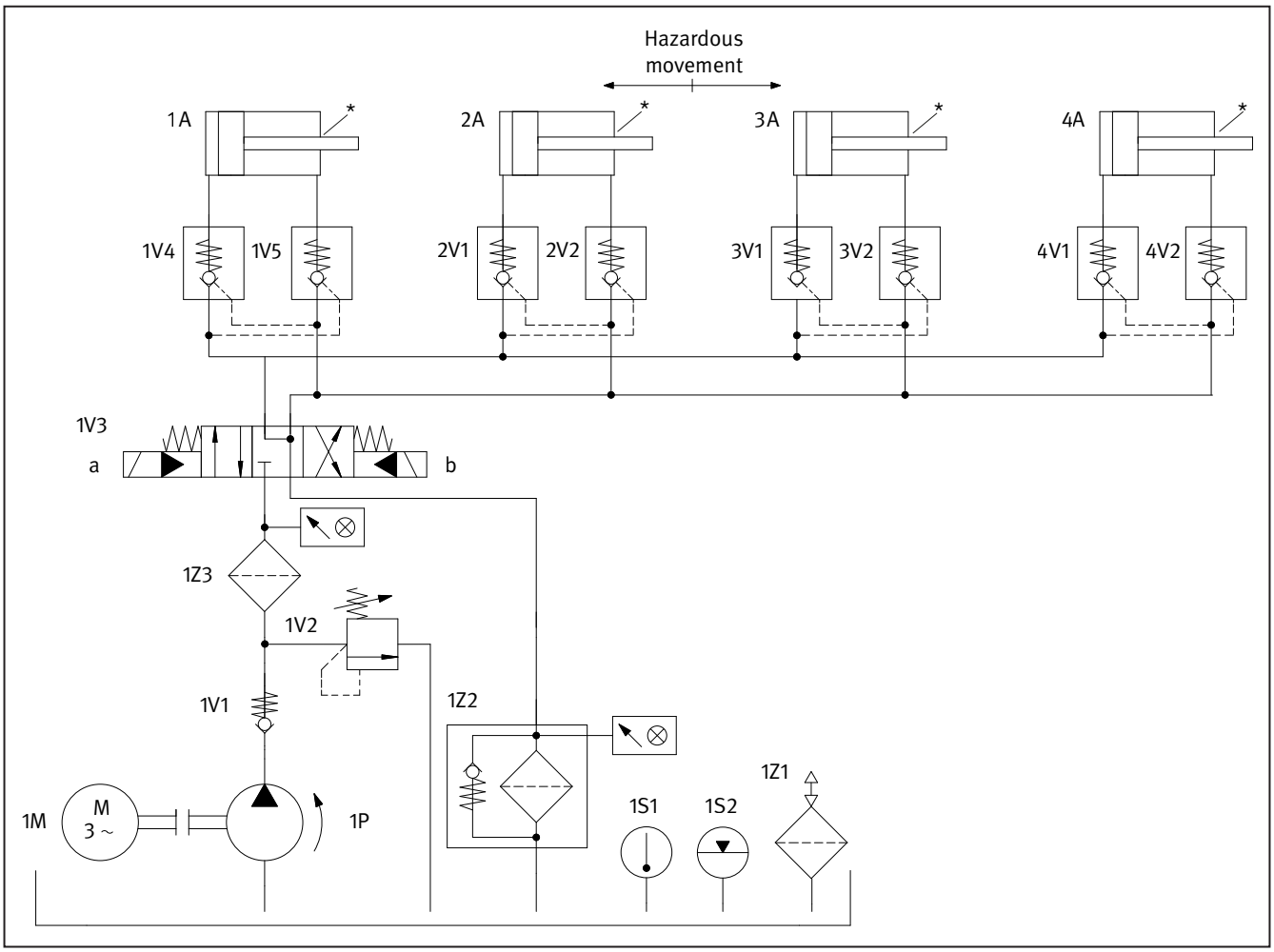
- EN 1010-3: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 3: Cutting machines (2002) + A1 (2009)
- EN 574: Safety of machinery – Two-hand control devices – Functional aspects – Principles for design (1996) +A1 (2008)
- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2009) + A1 (2012). IEC, Geneva, Switzerland 2009/2012

Figure 8.71:
Determining of the PL by means of SISTEMA



8.2.38 Hydraulic valve control (subsystem) – Category 4 – PL e (Example 38)

Figure 8.72:
Hydraulic valves for the control of hazardous movements

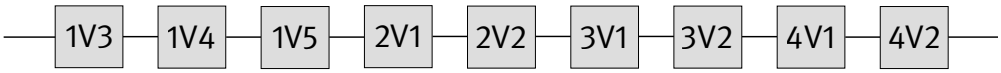


Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the hydraulic part of the control system is shown in this example, in the form of a subsystem. Further SRP/CS (e.g. safeguards and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

Functional description

- Hazardous movements are executed by four actuators, 1A to 4A. The movements are halted by the directional control valve 1V3 in conjunction with the pilot-operated non-return valves. Both the former and the latter constitute well-tried components for safety applications.
- Failure of the directional control valve or one of the pilot-operated non-return valves can result in loss of the safety function. The failure is dependent upon the reliability of the valves.
- No measures for fault detection are implemented.



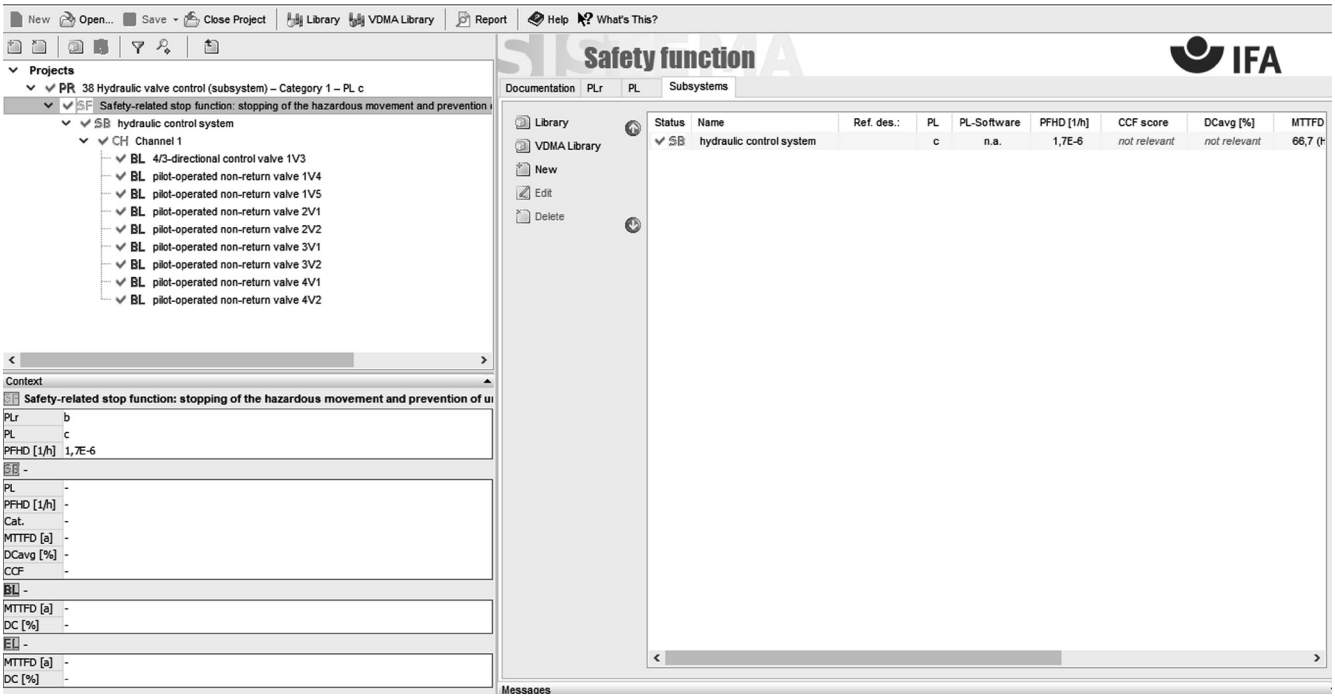
Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V3 is a directional control valve with sufficient overlap, spring-centred central position and fatigue-resistant springs.
- The valves 1V4, 1V5, 2V1, 2V2, 3V1, 3V2, 4V1 and 4V2 are pilot-operated non-return valves.
- The safety-oriented switching position is attained by cancellation of the control signal.
- Where necessary, the manufacturer/user must confirm that the directional control valve and the pilot-operated non-return valves constitute well-tried components for safety applications.
- The following specific measures are implemented to increase the reliability of the valves: a pressure filter 1Z3 upstream of the directional control valve, and suitable measures on the cylinder to prevent dirt from being drawn in by the piston rod (e.g. an effective wiper on the piston rods, see * in Figure 8.72).

Calculation of the probability of failure

- $MTTF_D$: an $MTTF_D$ of 600 years is assumed [S] in each case for the directional control valve and the pilot-operated non-return valves, since the number of switching cycles of the valves lies between 250,000 and 500,000 per year (n_{op}) for this application.
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The hydraulic part of the control system satisfies Category 1 with a high $MTTF_D$ (66.7 years). This results in an average probability of dangerous failure of $1.7 \cdot 10^{-6}$ per hour. This satisfies PL c.

Figure 8.73:
Determining of the PL by means of SISTEMA



9 References

[1] Directive 98/37/EC of the European Parliament and of the Council of 22 June 1998 on the approximation of the laws of the Member States relating to machinery. OJ EC (1998) No. L 207, p. 1-46; amended by Directive 98/79/EC, OJ EC L 331 (1998), p. 1-37. http://eur-lex.europa.eu

[2] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). OJ EC (2006) No. L 157, p. 24-86 http://eur-lex.europa.eu

[3] EN ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction (2011)

[4] ISO/TR 14121-2: Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods (2012)

[5] EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (2015)

[6] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2012)

[7] *Ostermann, H.-J.; von Locquenghien, D.*: Wegweiser Maschinensicherheit. Bundesanzeiger Verlagsgesellschaft, Cologne, Germany 2007

[8] *Reudenbach, R.*: Sichere Maschinen in Europa – Teil 1: Europäische und nationale Rechtsgrundlagen. 8th ed. Verlag Technik & Information, Bochum, Germany 2007

[9] EN 954-1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (1996)

[10] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0 to 7 (2010)

[11] IEC 62061: Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems (2015)

[12] *Bömer, T.*: Funktionale Sicherheit nach IEC 61508. In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz (Kennzahl 330 219). 2nd ed. Lfg. 2/14, XII/2014. Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin, Germany. Erich Schmidt, Berlin, Germany 2003 – looseleaf-ed. www.ifa-handbuchdigital.de/330219

[13] *Hauke, M.; Schaefer, M.*: Sicherheitsnorm mit neuem Konzept. O + P Ölhydraulik und Pneumatik 50 (2006) No. 3, p. 142-147. www.dguv.de/medien/ifa/de/pub/grl/pdf/2006_016.pdf

[14] DIN ISO/TR 23849: Guidance on the application of EN ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery (2014)

[15] *Hauke, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Rempel, P.; Ostermann, B.*: Amendment of EN ISO 13849-1 – A survey of the essential improvements in 2015. Published by: Institut für Arbeitschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin, Germany 2015. www.dguv.de/webcode/e89507

[16] *Schaefer, M.; Hauke, M.*: Performance Level Calculator – PLC. 5th ed. Published by: Institute for Occupational Safety and Health of the German Social Accident Insurance; German Electrical and Electronic Manufacturers' Association (ZVEI) – Division Automation, Frankfurt am Main, und Mechanical Engineering Industry Association – VDMA, Frankfurt am Main, Germany 2015. www.dguv.de/webcode/e20892

[17] Principles for testing and certification of DGUV-Test. www.dguv.de/webcode/e541144

[18] Summary list of titles and references of harmonised standards under Directive 98/37/EC on Machinery. Published by: European Commission. http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/machinery/index_en.htm

[19] IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2nd ed. Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin. Erich Schmidt, Berlin, Germany 2003 – looseleaf-ed. www.ifa-handbuchdigital.de

[20] IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (2016)

[21] VDMA-Einheitsblatt 24584: Safety functions of regulated and unregulated (fluid) mechanical systems (2016)

[22] *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld, R.*: Safe drive controls with frequency inverters. IFA Report 4/2018e. 3rd ed. Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin, Germany 2019. www.dguv.de/webcode/e635980 (will be published in Summer 2019)

[23] The SISTEMA Cookbook 6: Definitions of safety functions: What is important? Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin, Germany 2015. www.dguv.de/webcode/e109249

[24] *Apfeld, R.; Schaefer, M.*: Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachmesse und Kongress SPS/IPC DRIVES, 23.-25. November 2010, Nürnberg, Germany – Vortrag. www.dguv.de/webcode/d18471

[25] IEC 60204-1: Safety of machinery – Electrical equipment of machines – Part 1: General requirements (2016)

[26] Interpretation paper on substantial modification to machinery. Notice from the Federal Ministry of Labour and Social Affairs of 9 April 2015 – IIIb5-39607-3 . www.bmas.de/DE/Themen/Arbeitsschutz/Produktsicherheit/maschinen.html

[27] EN 1010-3: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 3: Cutting machines (2009)

[28] EN 1010-1:Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (2010)

[29] *Apfeld, R.; Huelke, M.; Lüken, K.; Schaefer, M.* et al.: Manipulation von Schutzeinrichtungen an Maschinen. Published by: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin, Germany 2006. www.dguv.de/webcode/d6303 and www.stopp-manipulation.org

[30] DGUV Information 209-068/069 (bisher: BGI/GUV-I 5048-1/2): Ergonomische Maschinengestaltung, Checkliste, Auswertungsbogen und Informationen (02.2018). Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin, Germany 2018. www.dguv.de/webcode/d3443

[31] VDI/VDE 3850: Development of usable user interfaces for technical plants. Blatt 1: Development of usable user interfaces for technical plants – Concepts, principles and fundamental recommendations (2014). Blatt 2: Development of usable user interfaces for technical plants – Features, design and applications of user interfaces with touchscreen (2015). Blatt 3: Development of usable user interfaces for technical plants – Interaction devices for screens (2017)

[32] *Hauke, M.; Apfeld, R.*: The SISTEMA Cookbook 4: When the designated architectures don't match. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin, Germany 2012. www.dguv.de/webcode/e109249

[33] *Birolini, A.*: Reliability Engineering: Theory and Practice. 6th ed. (2010)

[34] *Apfeld, R.; Hauke, M.; Schaefer, M.; Rempel, P.; Ostermann, B.*: The SISTEMA Cookbook 1: From the schematic circuit diagram to the Performance Level – quantification of safety functions with SISTEMA. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin, Germany 2010. www.dguv.de/webcode/e109249

[35] EN ISO 14119: Safety of machinery – Interlocking devices associated with guards – Principles for design and selection (2013)

[36] Vertical Recommendation for Use Sheets (RfUs) – Status on November 2015, Number CNB/M/11.050/R/E Rev 05, S. 191, Hrsg.: European Co-Ordination of Notified Bodies Machinery Directive 2006/42/EC + Amendment, 2015 http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm

[37] IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2010)

[38] Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Published by: Fachbereich Energie Textil Elektro Medienerzeugnisse, Cologne, Germany 2014. www.bgetem.de, Webcode: 12677093

[39] IEC 61784-3: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions (2016)

[40] *Reinert, D.; Schaefer, M.*: Sichere Bussysteme für die Automation. Hüthig, Heidelberg 2001

[41] *Huckle, T.*: Kleine BUGs, große GAUs. Vortrag zum Thema „Softwarefehler und ihre Folgen“. www5.in.tum.de/~huckle/bugsn.pdf

[42] IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements (2010)

[43] IFA-Report 2/2016: Sicherheitsbezogene Anwendungssoftware von Maschinen – Die Matrixmethode des IFA. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany 2016. www.dguv.de/webcode/d1023063

[44] Software-Assistent SOFTEMA: Spezifikation zur IFA-Matrixmethode bei sicherheitsbezogener Anwendungssoftware. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin, Germany. www.dguv.de/webcode/d1082520

[45] *Friedrich, J.; Kuhrmann, M.; Sihling, M.; Hammerschall, U.*: Das V-Modell XT Für Projektleiter und QS-Verantwortliche kompakt und übersichtlich. Springer, Berlin, Germany 2009

[46] IEC 61131-3: Programmable controllers – Part 3: Programming languages (2013)

[47] MISRA Development Guidelines for Vehicle Based Software. Published by: The Motor Industry Software Reliability Association. www.misra.org.uk

[48] IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (2010)

[49] SN 29500: Ausfallraten – Bauelemente – Erwartungswerte. Published by: Siemens AG, Center for Quality Engineering, Munich, Germany 1994 bis 2005

[50] *Mai, M.; Reuß, G.*: Self-tests for microprocessors incorporating safety functions or: „Quo vadis, fault?“. BGIA-Report 7/2006e. Published by: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin, Germany 2006. www.dguv.de/ifa, Webcode: e91093

[51] EN 82079-1: Preparation of instructions for use - Structuring, content and presentation– Part 1: General principles and detailed requirements (2012)

[52] ISO 9355: Ergonomic requirements for the design of displays and control actuators – Part 1: Human interactions with displays and control actuators (1999), Part 2: Displays (09/06), Part 3: Control actuators (12/99)

[53] Leitfaden Software-Ergonomie; Gestaltung von Bedienoberflächen, VDMA Verlag, Frankfurt am Main, Germany 2004

[54] EN ISO 9241-11: Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts (2018)

[55] EN 574: Safety of machinery – Two-hand control devices – Functional aspects – Principles for design (2008)

[56] IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2016)

[57] BGIA Report 2/2008e: Functional safety of machine controls. Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin, Germany 2009. www.dguv.de/webcode/e91335

[58] EN ISO 4413: Hydraulic fluid power – General rules and safety requirements for systems and their components (2010)

[59] EN ISO 4414: Pneumatic fluid power – General rules and safety requirements for systems and their components (2010)

[60] EN ISO 14118 (ehm. EN 1037): Safety of machinery – Prevention of unexpected start-up (2018)

[61] ISO 1219-1: Fluid power systems and components – Graphical symbols and circuit diagrams – Part 1: Graphical symbols for conventional use and data-processing applications (2012)

[62] ISO 1219-2: Fluid power systems and components – Graphical symbols and circuit diagrams – Part 2: Circuit diagrams (2012)

[63] ISO 8573-1: Compressed air – Part 1: Contaminants and purity classes (2010)

Annex A:
Examples of risk assessment

Changes with respect to the second edition (BGIA Report 2/2008e):

- Definition of the safety function extended
- Estimation of the frequency and duration of exposure described in more detail
- Consideration of the incidence and severity of accidents extended

Example 1: Closing edge protection

Figure A.1 shows the risk assessment for the safety function

- SF1 – Stopping of the closing movement and reversing upon detection of an obstacle

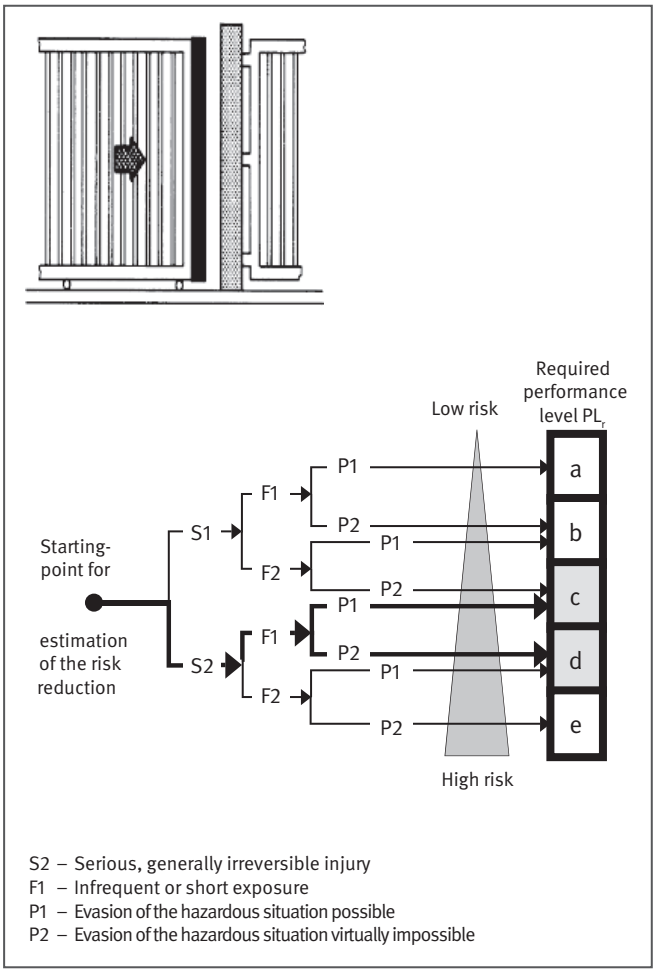
of a closing edge protection device[1]. The movement of powered windows, doors and gates (see Figure A.1) is generally associated with the formation of crushing and shearing points. These hazard zones generally exist only when the moving wing is approaching its final positions. Injury to persons in such hazard zones can be avoided, for example by the use of closing edge protection devices. Closing edge protection devices, such as pressure-sensitive edges, are fitted to the closing edges of the moving wings. When an obstacle is detected, the closing movement is interrupted and a reverse movement is initiated.

Crush and shear points on powered windows, doors and gates may cause severe and, under some circumstances, fatal injury. A severity of injury of S2 must therefore be assumed. Persons are infrequently (frequency lower than once every fifteen minutes) and only briefly (total duration of exposure less than 1/20 of the entire operation time) present in the area of the crushing and shearing points (F1). Under normal circumstances, persons at risk are able to move out of the hazard zone formed by the moving wing (P1). This yields a required Pe Level PL_r of c. This result is confirmed by the EN 12453 product standard. The standards committee evidently saw no reason to deviate from this owing to the incidence and severity of accidents. Example 13 in [1] shows how this safety function can be achieved.

[1] In the past, closing edge protection devices were governed by the Construction Products Directive. Since the pressure-sensitive edges use constitute safety components under the Machinery Directive, however, closing edge protection devices are also evaluated in accordance with this directive.

On fast-moving gates it is virtually impossible for persons to move out of the danger zone in time. The assessment of P2 instead of P1 thus yields a required Performance Level PL_r of d for these products.

Figure A.1:
Risk assessment for closing edge protection devices on powered windows, doors and gates



Example 2: Autonomous transport vehicles

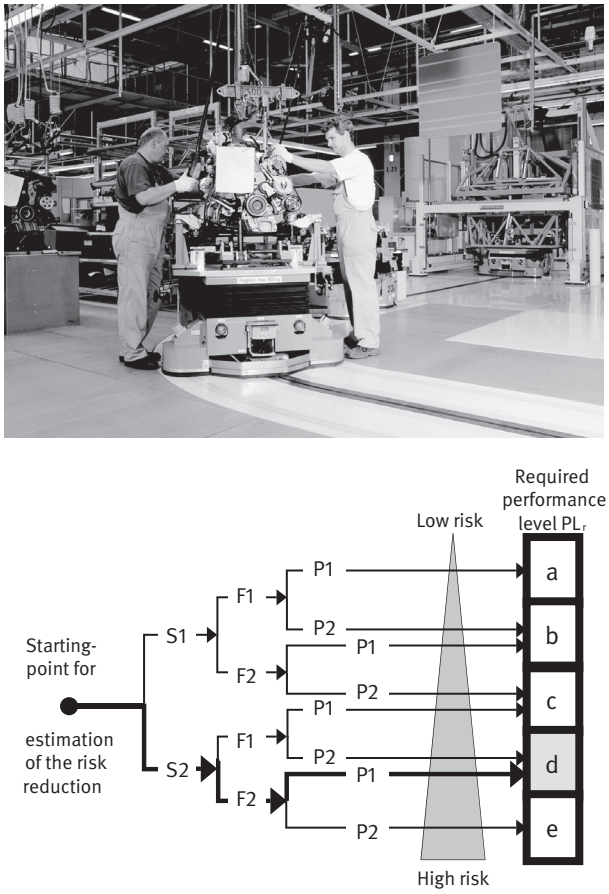
On autonomous transport vehicle, collision protection is assured by the safety function

- SF1 – Stopping of the transport vehicle upon approaching an obstacle

Since an autonomous transport vehicle may, under certain circumstances, be carrying a load weighing in the order of tons, severe irreversible injury is probable should a collision occur with the vehicle travelling at full speed (S2). The paths travelled by the vehicle are freely accessible to persons; the presence of a person in the danger

zone must therefore be assumed to be relatively frequent (frequency greater than once every 15 minutes) (F2). Since the vehicle travels at a very low speed (generally 3 to 5 km/h), a pedestrian is generally able to take evasive action when such a vehicle approaches (P1). This therefore results in a required Performance Level PL_r of d for SF1 (see Figure A.2). This result is confirmed by the EN 1525 product standard. The standards committee evidently saw no reason to deviate from this owing to the incidence and severity of accidents.

Figure A.2:
Risk assessment for collision protection on an autonomous guided vehicle



S2 – Serious, generally irreversible injury
F2 – Frequent or long exposure
P1 – Evasion of the hazardous situation possible

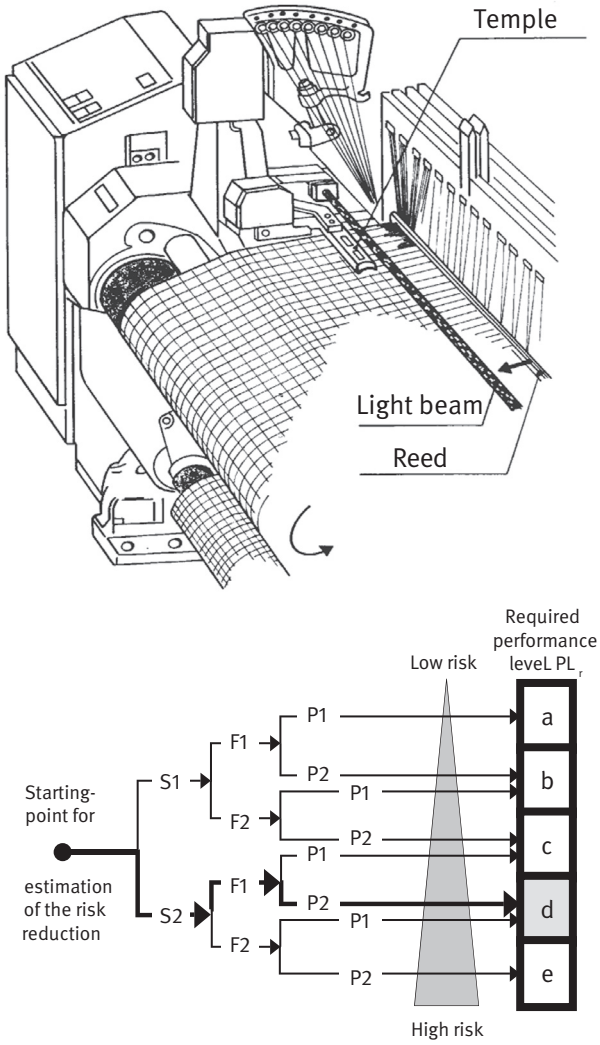
Example 3: Weaving machine

Weaving machines are employed for the fully automatic weaving of textiles. The essential hazard is that of crushing between the reed and the temple. In order to reconnect the ends of broken warp threads, the operator must intervene in the hazard zone with the machine stationary. Unexpected restarting is prevented by the safety function

- SF1 – In the event of intervention in the hazard zone: prevention of unexpected start-up by safe torque off (STO) of all drives

Should the machine restart, the operator's fingers may be crushed or broken (S2). The frequency of exposure to the hazard can be described as low (less frequently than once every 15 minutes); the entire exposure duration is lower than 1/20 of the entire operation time (F1). Should the operator already have his or her hands in the hazard zone when the machine restarts unexpectedly, the movement is so fast as to make evasion virtually impossible (P2). This therefore results in a required Performance Level PL_r of d for SF1 (see Figure A.3). This result is confirmed by the EN ISO 11111-6 product standard. The standards committee evidently saw no reason to deviate from this owing to the incidence and severity of accidents.

Figure A.3:
Risk assessment for a weaving machine



S2 – Serious generally irreversible injury
F1 – Infrequent or short exposure
P2 – Evastion of the hazardous situation virtually impossible

Example 4: Rotary printing press

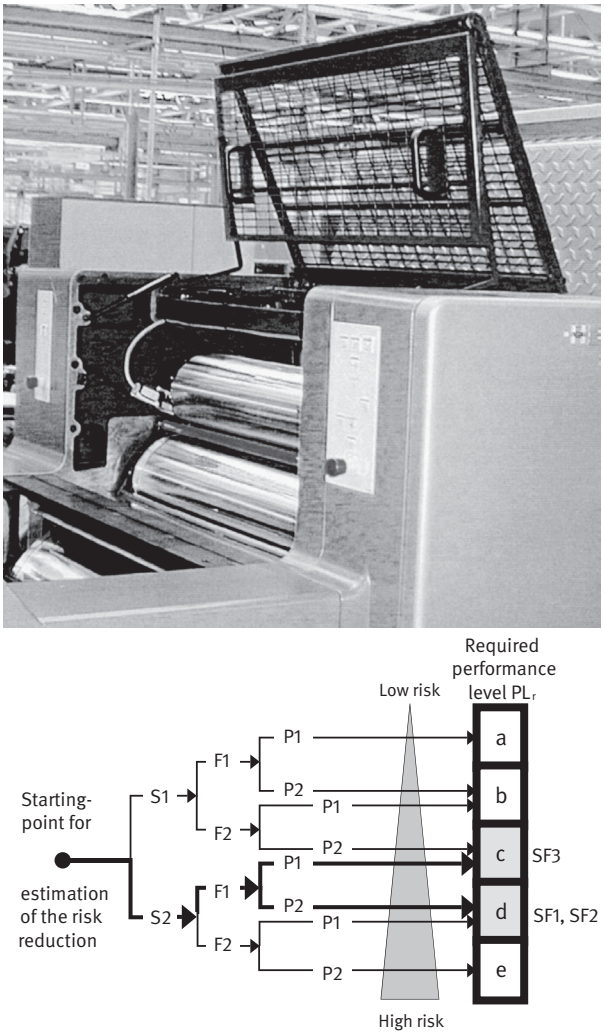
In a web-fed rotary printing press, a paper web is fed through a number of cylinders. High operating speeds and rotational speeds of the cylinders are reached, particularly in newspaper printing. Essential hazards exist at the entrapment points of the counter-rotating cylinders. This example considers the hazard zone on a printing press on which maintenance work requires manual intervention at reduced machine speeds. The access to the entrapment point is protected by a guard door (safeguarding). The following safety functions are implemented:

- SF1 – Opening of the guard door during operation causes the cylinders to be braked to a halt.
- SF2 – When the guard door is open, any machine movements must be performed at limited speed.
- SF3 – When the guard door is open, movements are possible only whilst an inching button is pressed.

Entrapment between the cylinders causes severe injuries (S2). Since tasks are performed in the hazard zone only during maintenance work, the frequency of exposure to the hazard can be described as low (less frequently than once every 15 minutes); the entire exposure duration is lower than 1/20 of the entire operation time (F1). At production speeds, no possibility exists of avoiding the hazard (P2). This therefore results in a required Performance Level PL_r of d for the safety functions SF1 and SF2 (see Figure A.4). The safety function SF3 can however be used only if the printing press has first been halted (SF1) and the permissible rotational speed of the cylinders limited (SF2). This results in the possible machine movements being predictable for the operator, who is thus able to evade hazardous movements (P1). A required Performance Level PL_r of c is therefore adequate for SF3 (see Figure A.4). In deviation from application of the risk graph, the EN 1010-1:2010 product standard applicable for this machine specifies a PL_r of d for the SF3 safety function. The risk reduction by SF1 and SF2 was unfortunately not considered by this standard.

Chapter 8, Example 24 describes how the safety functions described here can be implemented.

Figure A.4:
Risk assessment on a rotary printing press



S2 – Serious, generally irreversible injury
F1 – Infrequent or short exposure
P1 – Evasion of the hazardous situation possible
P2 – Evasion of the hazardous situation virtually impossible

Reference

[1] *Werner, C.*; *Zilligen H.; Köhler B.*; *Apfeld R.*: Safe drive controls with frequency converters. IFA Report 4/2018e. 3rd ed. Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV). Berlin, Germany 2019 (will be published in Summer 2019). www.dguv.de/ifa, Webcode: e635980

Annex B:
Safety-related block diagram and FMEA

Changes with respect to the second edition (BGIA Report 2/2008e):

- Convention for the expression of PFH_D (formerly: *PFH*), $MTTF_D$, λ_S, λ_D, λ_{DD}, λ_{DU}, B_{10D}, T_{10D} adapted to the new version of the standard (with the index in capitals)
- Explanations of the use of failure type distributions added
- Explanations added concerning the issue of obtaining B_{10D} from B_{10}
- "Reference" subclause updated

For demonstration of the Category and Performance Level (PL) to EN ISO 13849-1, the structure of a safety-related system must be analysed with respect to the safety function to be implemented (possibly involving separate analysis of several functions). For the obligatory quantitative demonstration of the PL, system information must be suitably prepared to permit calculation of the quantitative value PFH_D (probability of a dangerous failure per hour), or direct calculation of the PL based upon it. Two important steps in this process are the safety-related block diagram and the failure mode and effects analysis (FMEA) performed for each block [2].

B.1 Purpose and generation of a safety-related block diagram

The result of the safety-oriented analysis of the system structure is presented conveniently in the form of a block diagram, which can be described as a "safety-related block diagram". The diagram is intended to show whether the safety function is executed in whole or part by a single-channel or multi-channel solution, and the available diagnostics by which internal component failures can be detected. Since – with regard to the aspect of relevance here, i.e. quantification of the probabilities of failure – diagnostics represents a means of compensating for component failures, the term "failure detection" will be used in this Annex in place of the usual term "fault detection".

In the field of machine safety, it is generally accepted that in the event of a control-system failure, a substitute response should occur in place of the safety function originally implemented, and that the substitute reaction should initiate a safe state, such as operating inhibition with de-energized outputs (shut-down system). In accordance with EN ISO 13849-1, the Category and PL are intended to indicate only the safety quality, and not the probability of fault-free operation, i.e. the "availability". For this reason, signal paths that initiate a safe state in the event of a fault are regarded as being fully equivalent to functional units that may perform complex safety functions. A "single safety signal path" in this context is however a "channel" in its own right only when it is continually engaged. If the safety path cannot become active until a failure in the main function path proper has been detected, its safety benefit is dependent upon the quality of the failure detection mechanism. This quality is described by the diagnostic coverage of the failure detection mechanism. In such cases, the safety path generally provides only test equipment with shut-off path. Architectural features of this kind must be expressed correctly on the safety-related block diagram. The differentiated presentation of a true two-channel arrangement and a monitored single channel can be seen clearly from a comparison of Figures 10 and 11 in the standard.

Consideration must also be given to whether components or circuit elements are present which, although they do not execute the safety function or the safety-related substitute function in the event of a fault, may be able to prevent other components from properly executing the safety or substitute function should certain component failures occur. Such circuit components include those providing necessary auxiliary functions such as the power supply or control functions that are not (intentionally) relevant to safety but that may have an impact upon safety-related parts. Where components and parts of circuits may impact negatively upon the safety function, its substitute function, or diagnostics functions in the event of failures, they must always be considered in a function block. For example, components for assurance of electromagnetic compatibility (EMC) must be examined with regard to whether their failure, for example short-circuiting of a capacitor, has negative effects upon safety-related circuits.

Parts of circuits with defined inputs and outputs may be regarded as a function block. In order to keep the number of required function blocks as low as possible, parts of circuits that are arranged functionally in series, i.e. circuits that execute different signal processing steps sequentially, can be grouped to form a function block. Blocks differing from this arrangement should logically be grouped only to the extent that redundancies such as separate shut-off paths and the mutual diagnostics of

[2] The FMEA described here also considers the detection of failures (diagnostics), and can therefore also be termed FMEDA (failure mode, effects and diagnostic analysis).

function blocks are still expressed. The circuit analysis must ultimately produce a block diagram in which all the structures that are of relevance to safety are reflected:

- Single or parallel signal paths ("channels") that are used to execute the safety function
- Signal paths that execute a safety-related substitute function in the event of a fault
- Circuits for the detection of failures (diagnostics)

Where auxiliary circuits that are required for performance of the safety function or for some other safety-related action (e.g. power supplies, oscillators) are able to influence one channel only, they should be grouped with the function block(s) of the channel concerned. Should these auxiliary circuits act upon several channels, they form a separate single-channel part (function block) on the safety-related block diagram. The same principle applies to circuits that are able to prevent performance of the safety function, another safety-related action or diagnostics owing to a particular manner of their failure. Examples include circuits for selection of a safe operating mode, or certain components for the assurance of EMC. The content of each function block must be determined unambiguously by circuit diagrams and parts lists. Owing to the way in which it is created and its particular function, the safety-related block diagram differs generally from block diagrams serving other purposes, such as those geared to the mechanical structure of assemblies.

Figure B.1 shows, by way of example, the safety-related block diagram of a Category 2 single-channel machine control system featuring:

- A microcontroller
- A light barrier for the monitoring of hazard zones
- A "watchdog" for the detection of certain controller malfunctions
- A closed-loop motor drive control (frequency inverter) driven by the controller
- A device for de-energization of the motor that can be actuated by the watchdog (pulse inhibit)

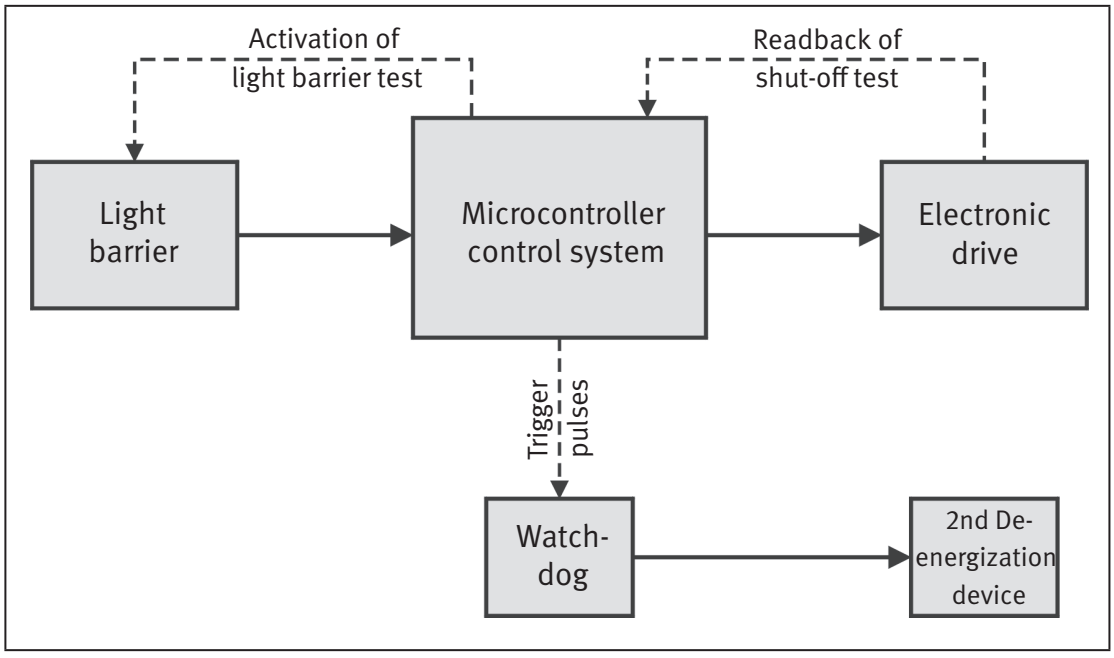


Figure B.1: Example safety-related block diagram of a Category 2 single-channel machine control system

The safety function entails de-energization of the motor as soon as, and for as long as, the light beam of the light barrier is interrupted ("safe torque off"). Besides the safety function, the microcontroller and the downstream drive control perform a number of other machine functions which, since they are not safety functions, will not be considered here. Although in this example, the safety function is implemented entirely electrically, the principles described for the safety-related block diagram and the FMEA apply to all technologies.

The safety-related block diagram contains only function blocks that are related to the "safe torque off" safety function; it does not contain control or display devices for other machine functions. In the event of a fault, some components in these circuit parts may have negative repercussions for the safety function. Only then should these components be included in the function blocks that they could cause to fail.

The safety-related block diagram will often take the form of one of the "designated architectures" in accordance with EN ISO 13849-1, subclause 6.2.2 (subclauses 6.2.1 to

6.2.7 of this report), as in the example presented here. In such cases, the method described in subclause 4.5.4 of the standard (supplemented by Annexes B, C, D, E, I and K of the standard) may be applied for quantitative calculation of the Performance Level. It is not advisable however to shoehorn a different structure into the form of one of these architectures. It may be possible to break an existing system structure down into parts each of which then corresponds to a designated architecture.

Should a breakdown of this kind not be possible, a dedicated model must be produced for quantitative calculation of the safety-related reliability for the safety-related block diagram concerned. An introduction to suitable modelling techniques can be found for example in [1].

B.2 Purpose and characteristic of an FMEA for quantification

For quantitative demonstration of the PL, the average probability of a dangerous failure per hour (PFH_D) must be estimated. This can be achieved with the aid of a mathematical model (e.g. a *Markov* model) generated for the system under consideration. If however the form of one of the "designated architectures" in accordance with subclauses 6.2.3 to 6.2.7 can be identified formally from the safety-related block diagram, as in the example in Figure B.1, the method in this standard referred to above can be applied for quantitative calculation of the PL.

In both cases, the dangerous (i.e. unfavourable from a safety perspective) failure rate, specifically its reciprocal, the $MTTF_D$ (mean time to dangerous failure), and the *DC* (diagnostic coverage) of the function blocks in the safety-related block diagram must be known. For calculation of these values, a special variation of the FMEA is used that employs the component failure rates in the form of quantitative values. The special form of the FMEA used here differs in this respect from the majority of other FMEA types, which are used for other purposes such as the early detection of problems and fault avoidance during development [2].

A particular feature of an FMEA for quantification purposes is its structure according to the function blocks of the safety-related block diagram. The principle is that a separate FMEA is performed for each of these function blocks, and produces results only for the function block concerned. The results for each function block are not combined until later, by inclusion together in the calculation of the PFH_D/PL by way of a system-specific mathematical model or the simplified quantification method in EN ISO 13849-1.

B.2.1 Performance of an FMEA for quantification

The essential procedure employed for an FMEA for quantification is demonstrated below with reference to the "light barrier" function block from Figure B.2.

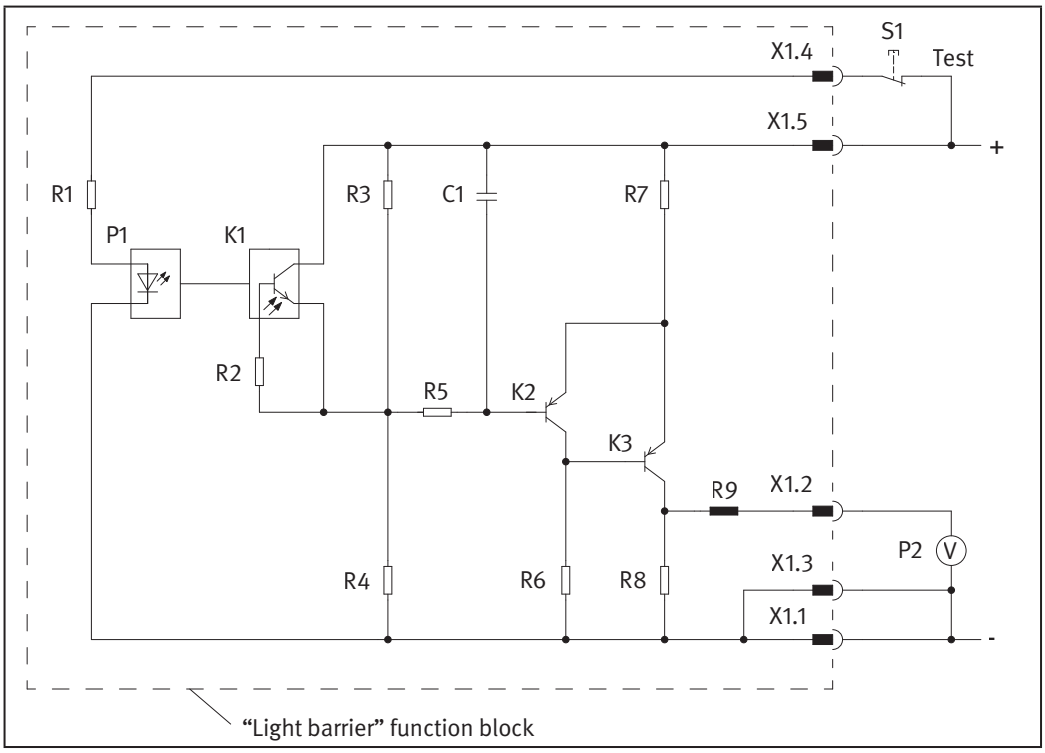


Figure B.2:
Assumed circuit (simple example) of the "light barrier" function block from the safety-related block diagram from Figure B.1

For this purpose, the circuit has deliberately been kept simple. Only components framed by the dashed line belong to the function block. The elements S1 and P2 constitute a substitute circuit for the actual inclusion of the function block within the system in accordance with Figure B.1. As long as the phototransistor K1 continues to receive light from the infrared LED P1, it maintains the transistor K2 blocked, as a result of which the transistor

K3 is conductive and a positive output voltage, which can be measured by the voltmeter P2, is present on terminal X1.2. If the light beam is interrupted, K1 blocks, K2 becomes conductive and K3 switches off the output voltage. The test of the "light barrier" function block, which is performed by the microcontroller control system in Figure B.1 in accordance with the program, can be simulated by the pushbutton S1 and the voltmeter P2: the light source P1 is switched off temporarily and the output voltage observed for whether it drops to 0 V as intended. The signal-processing elements of the "light barrier" function block (K1 to K3, R2 to R9, C1) are required to behave in the same way as in response to a "real" demand of the safety function caused by interruption of the light beam. This test is described below as "Test 1".

B.2.2 Dangerous failure mode of a function block

The first step entails identification of the dangerous failure mode of the function block. Generally, not only may individual elements fail, but an entire function block may also fail in various ways as a result. The modes of failure that are unfavourable from a safety perspective are regarded as the "dangerous" failure mode of a function block. Some failures cause immediate, dangerous failure of the entire system, with the result that neither the original safety function, nor a safety-oriented substitute function can be performed. Other failures increase the probability of this happening in that a smaller number of further failures is now sufficient to cause the system to fail dangerously. Should no redundancy exist for the function block suffering failure, i.e. no second channel capable of assuming its function, and should diagnostics fail to perform sufficiently rapidly an action producing a safe state, the dangerous failure of the function block leads to dangerous failure of the system. However, even when, owing to the existence of redundancy or a rapid failure response by other circuit components, none of the possible failure modes of the function block under analysis causes a dangerous system failure, its "dangerous" failure mode can and must be identified. The dangerous failure mode is that leading to the function block no longer making its intended contribution to safe behaviour of the system. On occasions it may be necessary for several failure modes that are characterized by different but equally harmful block behaviour to be considered (e.g. continuous energization and oscillation on the output). The simplest solution is therefore to describe the dangerous failure mode in terms of the loss of the function block's safety-related functionality. Diagnostics features are considered later and will be ignored at this stage. In the example under consideration here (light barrier, Figure B.2), the output voltage of the function block is to drop to zero for as long as the phototransistor K1 fails to receive light from the LED P1, since this constitutes the contribution of this function block to performance of the safety function: "safe torque off when the light beam is interrupted".

The dangerous failure mode of the function block can thus be described as "presence of an output voltage greater than zero during non-illumination of the phototransistor K1".

B.2.3 Component failure rates

Component failure rates may be obtained from a number of sources. Examples for electronic components are listed in [3 to 6]. These sources all contain generic data relevant to multiple manufacturers. Collections of failure rates also exist for mechanical, pneumatic and hydraulic components. For certain components that are not listed in the relevant indexes (such as special ASICs), the failure rate must be obtained from the manufacturer. Many common quantification techniques, including the simplified method in EN ISO 13849-1 subclause 4.5.4, assume a constant failure rate over time. This represents an idealized view. With appropriate dimensioning and, if necessary, preventive replacement, components can be prevented from reaching the wear phase, during which the failure rate rises sharply, before the end of the mission time T_M.

A quick source of generally conservative (pessimistic) estimations of failure rates can be found in EN ISO 13849, Part 1, Annex C. In particular, a method is shown here by which failure rates for discrete, cyclically operating electromechanical, fluid power and mechanical components can be derived from the "B_{10D}" values (see Table D.2 of this report).

Should a conservative estimate of the failure rate not be chosen, it must be ensured for each component that the value employed is valid under the conditions of use (temperature, current, voltage, power dissipation, etc.) in the application in question. The inherent heating effect must also be taken into account. Standard data sources, such as [3 to 6], provide measures by which the base failure rates applicable under defined reference conditions can be converted to values applicable under different conditions. Suitable conversion formulae (but not base failure rates) can be found in [7].

B.2.4 Production of an FMEA on a function-block basis for quantification purposes

In the FMEA, the components of the function block are first assessed separately, and the complete assessment for the block is then derived from them. For practical purposes, a table documenting both the process and the results is employed. The level of accuracy employed for performance of the FMEA may be varied; the accuracy employed is reflected in variation in the overhead associated with generation of the tables required. One possible execution is shown by way of example in [8]. Binding rules do not exist. The variant shown in Figure B.3 represents a compromise between a high degree of accuracy and corresponding overhead on the one hand and excessive simplification on the other, and takes the accuracy and availability of the data used into account. The figures used are assumed example values.

Description of the function block:	Light barrier
Dangerous failure mode of the function block:	Presence of an output voltage greater than zero during non-illumination of the phototransistor K1
Data source of failure rates:	XYZ database

Component reference	Component class	Relevant component temp. (°C)	Base failure rate (FIT)	Temperature factor	Proportion of safe failures	Proportion of dangerous failures	Detectab. by test No	DC	λ (FIT)	λ_S (FIT)	λ_D (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)	Note
R1	Chip resistor, MF	55	0,5	1,20	1	0	–	–	0,60	0,60	0,00	0,00	0,00	
R2	Chip resistor, MF	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	1)
R3	Chip resistor, MF	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R4	Chip resistor, MF	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R5	Chip resistor, MF	50	0,5	1,15	0,5	0,5	1	1	0,58	0,29	0,29	0,29	0,00	
R6	Chip resistor, MF	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R7	Chip resistor, MF	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R8	Chip resistor, MF	50	0,5	1,15	1	0	–	–	0,58	0,58	0,00	0,00	0,00	
R9	RF inductor, SMD	50	1,8	1,12	1	0	–	–	2,02	2,02	0,00	0,00	0,00	
C1	Chip capacitor, ceram.	50	1,1	1,60	0	1	1	0,5	1,76	0,00	1,76	0,88	0,88	2)
P1	Infrared LED	60	2,5	2,24	1	0	–	–	5,60	5,60	0,00	0,00	0,00	
K1	Phototransistor	60	3,4	1,80	0,5	0,5	1	1	6,12	3,06	3,06	3,06	0,00	
K2	Transistor, SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
K3	Transistor, SMD	50	3,2	1,22	0,5	0,5	1	1	3,90	1,95	1,95	1,95	0,00	
X1	5-pin connector	50	1,5	1,00	0,5	0,5	1	1	1,50	0,75	0,75	0,75	0,00	3)
–	PCB with 36 solder p.	50	1,8	1,00	0,5	0,5	1	0,9172	1,80	0,90	0,90	0,83	0,07	4)
								Totals:	31,23	19,71	11,52	10,57	0,95	
								$MTTF_D$ (a):	9905,9			*DC* (%):	91,72	

Notes:
1) Open circuit and excessively high ambient temperature may cause an excessively high dark current to flow through K1.
2) Open circuit renders the circuit susceptible to electromagnetic interference; detectability is not assured.
3) Short-circuits within X1 may cause dangerous failures.
4) Distribution of DD/DU is the same as the average distribution of all other elements.

Figure B.3:
Reasonable form of execution of an FMEA table for the "light barrier" function block in Figure B.2

The components of the function block are listed in rows together with their failure rates. The usual unit for the failure rate is "FIT" (failures in time); 1 FIT = 10^{-9} per hour. The only weighting factor indicated here for the base failure rate is the temperature factor. Other adjustment factors may justifiably be ignored when the components are on average electrically overdimensioned, which is frequently the case. In such cases, their electrical load then lies pre-

dominantly below the reference load upon which the base failure rate is based, with the result that the corresponding adjustment factors are < 1. Omission of these factors thus constitutes an estimation erring on the safe side and at the same time a reduction in the required effort, since the precise electrical operating values for the components need not all be determined individually. Should it be known, however, that the load upon certain components lies above the reference load, the relevant adjustment factors must be considered. If the base failure rate of individual components predominates within the function block, as is often the case for example for processors and power semiconductors, precise examination and if applicable consideration of all necessary adjustment factors for the components concerned must be examined precisely and given consideration where applicable.

In the next step, the total failure rate λ of each component is divided into the proportions λ_S ("safe" mode, i.e. safe failure) and λ_D ("dangerous" mode, i.e. dangerous failure). For this purpose, information such as the "dangerous failure mode" of the function block must be known (see above). A "puristic" approach requires this to be performed in two steps.

Firstly, the total failure rate is distributed between the various failure types (e.g. open circuit, short circuit, drift, change in function). Information on the failure type distribution of a range of components can be found for example in IEC 61709 [7] and IEC/TR 62380 [4]. Typical failure type distributions can also be found in commercial FMEDA software. The data in the various sources are not consistent. Unnecessary selection of a different source for the failure type distribution from component to component is not acceptable.

In the second step, the proportions accounted for by each failure type are assigned to λ_S or λ_D, according to whether the failure type concerned causes the function block to fail in its safe or unsafe mode. A continuation in function without change is regarded in this case as a safe-mode failure.

Figure B.3 shows a simplified pragmatic approach that does not rely upon a particular source for the failure type distributions and that is limited to determining which of the three following cases applies to a component:

a) All failure types result in safe-mode failure of the function block, or have no impact upon its behaviour.

b) At least one failure type exists that causes the function block to fail safely, and one failure type that causes it to fail dangerously.

c) All failure types cause the function block to fail in its dangerous mode.

In case a), the total failure rate λ is assigned to the failure rate λ_S in the safe failure mode (example: infrared LED P1). By the same token, in case c), the total failure rate λ is attributed to the failure rate λ_D in the dangerous failure mode (example: capacitor C1). In case b), the total failure rate λ is divided equally between λ_S and λ_D (example: transistor K2).

The simplified procedure shown in case b) is normally justified for components making only a small contribution to the total failure rate of the function block when it contains a large number of such components. Individual components with an above-average contribution to the total failure rate of the function block may have to be considered separately. The failure rate may also be divided equally between λ_S and λ_D for complex integrated circuits such as processors. The same applies to solder joints/printed circuit boards. Caution is required with discrete or low-integration components with a relatively high failure rate. Should for example a contactor or a power semiconductor contribute substantially to the total failure rate of the function block, failure should be assumed in cases of doubt to be predominantly dangerous. This applies even more to elements of safety outputs that switch output currents.

For components intended to enhance the circuit's resistance to disturbance phenomena, such as electromagnetic interference or excessive ambient temperature, it is advantageous to distinguish between two possible cases for assessment of the function block's behaviour. If the incidence of disturbance phenomena is merely "possible" and the function of the circuit measure is essentially to increase the availability of the device under (infrequent) unfavourable conditions, simultaneous presence of the "disturbance phenomenon" in the event of component failure need not be assumed during assessment of the function-block behaviour. Conversely, should the device's intended form of operation be associated with occasional to continuous presence of the disturbance or should this be anticipated in view of the typical operating conditions (e.g. installation within the range of known sources of electromagnetic interference or at a hot site), assessment of the component failure must take account of the disturbance. The same applies to assessment of the failure detectability provided by diagnostics measures for these components.

Where components are subject to wear, a substitute failure rate constant over time is generally applied. This is calculated by means of formula C.5 in EN ISO 13849, Part 1, Annex C.4.2. The B_{10D} value, which states the average number of switching cycles before dangerous failure, is required for this purpose. The B_{10D} value should ideally be obtained from the manufacturer of the component, who should also state which mode of failure was assumed for this purpose to be the dangerous mode

(e.g. the failure of contacts to open), since in principle, a mode of failure can be assessed as dangerous or not dangerous only with respect to a specific application. In many cases, only a manufacturer's B_{10} value (number of switching cycles before any form of failure) is available. For this case, calculation of the B_{10D} value by means of the formula $B_{10D} = B_{10}/RDF$ is sometimes recommended. RDF (ratio of dangerous failure) represents the fraction of the overall failure rate of an element that can result in a dangerous failure. EN ISO 13849-1, Annex C.4.2, Footnote 2 also follows this approach with RDF = 0.5. This method of calculation is however based upon simplified assumptions that may differ considerably from the actual conditions for the wearing parts under analysis here. For this reason, B_{10D} should be limited to twice the value of B_{10} when B_{10D} is determined by means of the quotient B_{10}/RDF. Owing to the relationship in formula C.3 in EN ISO 13849-1, Annex C.4.2, the method for determining the B_{10D} also has an impact upon the permissible component operation time T_{10D} and thus possibly also upon replacement intervals to be specified for the component.

The next step in the method entails consideration for diagnostics. Only diagnostics relating to dangerous-mode failures (of the function block) are considered. Consideration for whether a test or where applicable several tests are capable of detecting some or all of these failures need therefore be given only for components that exhibit a portion of dangerous-mode failures. The relevant effective test, and the diagnostic coverage *DC* for the components indicating the detectable portion of dangerous-mode failures, are entered in appropriate columns. Where the components concerned are discrete components as in the example shown in Figure B.2, one of the two *DC* values "0" for "undetectable" or "1" for "detectable" can often be assigned to the dangerous failure of a single component. In the case of complex integrated components and of discrete components the failure of which is capable of impairing the function of such a complex component, the component-related *DC* must be estimated in consideration both of the dangerous failure mode and of the available test method. Support in this assessment is provided by Table E.2, in which *DC* values of 0% ("none"), 60% ("low"), 90% ("medium") and 99% ("high") are assigned for standard test methods. During assignment of a *DC* to a component, it must also be considered that an evaluation result of "detectable" is permissible only if the system is actually capable of performing the intended safety-oriented operation. Detection of a failure within a circuit, for example, is useless if it is rendered ineffective owing to a shut-off path that has already failed.

In the example shown, the components R1, R6 to R9 and P1 do not need to be considered with regard to the aspect of diagnostics, since they are not capable of causing dangerous-mode failure of the "light barrier" function block. The dangerous-mode failure portion of each of these components is 0. Dangerous-mode failure of elements R2 to R5, K1 to K3 and X1 is detected fully by "Test 1" (the only test in this example), i.e. when LED P1 is switched off for test purposes, the test detects an output voltage of › 0. The component-related *DC* value of "1" is therefore assigned to these elements. The situation is different for the capacitor C1, which has the function of suppressing frequent but not continuous electromagnetic interference (note: this is assumed for the purpose of this example). Drift failures (limited changes in capacitance) are not critical; a short-circuit, however, results in the output (terminal X1.2) being incapable of being de-energized (dangerous failure mode of the function block). A short-circuit on C1 is detected by Test 1. In the event of an open circuit on C1, the electromagnetic interference is transported via K2 and K3 to the output of the function block. It is unclear how the downstream circuit will interpret this high-frequency alternating signal, and also whether the disturbance phenomenon is present during the test. In the worst case, the non-suppressed interference results in the output signal with superimposed disturbance not being interpreted by the downstream circuit as a demand of the safety function, despite phototransistor K1 not being illuminated (= dangerous failure of the "light barrier" function block). Should the fault not be present at the time of the test, Test 1 is not able to detect the capacitor open circuit. Since no reliable information on the failure-type distribution is available for the capacitor, it is assumed that – when the non-critical drift failures are disregarded – short circuits and open circuits each account for 50% of the failures. Both failure types lead to a dangerous failure of the function block; only short-circuiting of the capacitor, i.e. (an estimated) half of all dangerous capacitor failures, are however reliably detectable. The component-related diagnostic coverage is thus estimated at 50% or 0.5. The printed circuit board and its solder joints can introduce short circuits and open circuits into the circuit at various points. The pragmatic approach, implemented in Figure B.3, for estimation of the *DC* value for the solder joints and printed circuit board consists in assigning the average *DC* value to them that is produced for all other components of the function block from the formula $DC = \Sigma \lambda_{DD}/\Sigma \lambda_D$. The inclusion of the printed circuit board and solder joints thus has no influence upon the *DC* value calculated for the complete function block.

In each row of the table, i.e. for each component:

λ = temperature factor · base failure rate (if applicable with further correction factors, see above)

λ_S = proportion of safe failures · λ

λ_D = proportion of dangerous failures · λ

$\lambda_{DD} = DC \cdot \lambda_D$

$\lambda_{DU} = (1 - DC) \cdot \lambda_D$

These λ values are summed by column in the table. The sum λ_D and the sums λ_D and λ_{DD} yield the $MTTF_D$, i.e. the mean time to a dangerous failure of the function block, and the *DC* of the function block respectively:

$MTTF_D = 1/\lambda_D$

$DC = \lambda_{DD}/\lambda_D$

The only input values required for determining the PL for one of the designated architectures in accordance with subclauses 6.2.3 to 6.2.7 are the $MTTF_D$ and *DC*. The example shown yields an $MTTF_D$ value of 9,905.9 years and a *DC* of 91.72%. If a different quantification method is employed, values from the FMEA table such as λ_{DD} and λ_{DU} may also be used.

B.3 Parts count method

Time and effort can be saved by use of a simpler method instead of an FMEA. If a detailed analysis of the circuit behaviour is not performed for the various failure types of the individual elements, the parts count method is an alternative (cf. Annex D of this report). This method was originally found in the MIL Handbook 217F (superseded by [6]), and a variant of it is described in EN ISO 13849, Part 1, Annex D.1. If at the same time relatively conservative (high) failure rates are assumed, the failure rates require no adjustment to the actual operating conditions. In addition, a dangerous failure proportion of 50% – with regard to the function block – is frequently assumed for many components. The table is thus simplified if superfluous columns for weighting and proportioning of the failure rates are omitted from the FMEA table. The parts count method normally delivers poorer (lower) $MTTF_D$ values than the FMEA results, since higher failure rates are generally input, and components are also considered that are capable of causing only safe-mode function-block failures.

If the parts count principle is applied to the example described above (light barrier), with assumption of the failure rates adjusted for temperature in Figure B.3 and a blanket proportion of dangerous failures for all components of 50%, the resulting $MTTF_D$ value is 7,310.8 years. This value is approximately 26% poorer than the FMEA result. The inferior value is due in this example solely to the omission of a circuit analysis. If a *DC* value is required for the function block, the component-related *DC* for each component must estimated as with the FMEA method or, for example with reference to Annex E, the *DC* of the entire function block.

The FMEA method for quantification purposes presented in this annex of the report with reference to an electronic circuit can be transferred to other technologies. It can therefore be applied formally in the same manner for example to mechanical, hydraulic and pneumatic systems.

References

[1] *Goble, W. M.*: Control Systems Safety Evaluation and Reliability. 3rd ed. Published by: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010

[2] IEC 60812: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA) (01.06.). IEC 60812: 2006: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[3] SN 29500: Ausfallraten Bauelemente, Erwartungswerte. Published by: Siemens AG, Corporate Technology, Technology & Innovation Management, Munich, Germany 2004-2014
(Order from: michaela.pabst@siemens.com or thomas.haizmann@siemens.com)

[4] IEC/TR 62380: Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment. Published by: International Electrotechnical Commission (IEC), Geneva, 2004; withdrawn in 2017. According to IEC, replaced by IEC 61709:2017, cf. [7]

[5] Telcordia SR-332, Issue 3: Reliability Prediction Procedure for Electronic Equipment. Published by: Ericsson Inc., Piscataway, New Jersey 2011

[6] Handbook of 217Plus Reliability Prediction Models. Quanterion Solutions Incorporated, Utica, New York 2015

[7] IEC 61709: Electric components – Reliability – Reference conditions for failure rates and stress models for conversion (02.17.).

[8] IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2010). Annex C.

Annex C:
Fault lists, fault exclusions and safety principles

C.1 Fault lists

The faults to be assumed for mechanical, pneumatic, hydraulic and electrical components during the validation of an SRP/CS and the fault exclusions that are possible can be found in fault lists in EN ISO 13849-2 [1], Annexes A to D. Individual product standards such as IEC 61800-5-2 [2] and IEC 61496-1 [3] also contain fault lists or supplements to the fault lists stated. Document 340 220 in the IFA Manual [4] explains the background and origins of the fault lists.

C.2 Fault exclusions

Without the assumption of fault exclusions, some safe control systems would not be achievable at reasonable expense. Reasons for fault exclusion include, in particular, the physical impossibility of a certain type of fault or the technical improbability of a fault occurring, and also generally accepted technical experience (see also subclause 7.3 of EN ISO 13849-1). Fault exclusions are also possible for newly developed components. The precise reasoning for each fault exclusion must be stated in the technical documentation. EN ISO 13849-2 describes possible fault exclusions for certain discrete components, where considered permissible. The information in the following examples has been updated where required to bring it into line with standard practice.

C.2.1 Examples of fault exclusions on components

C.2.1.1 Fluid power components

The fault exclusions formulated for pneumatic and hydraulic components are frequently similar. Fault exclusions specific to one of the forms of fluid power also exist, however.

Example of fault exclusions common to fluid power components of both types:

- Directional control valves

  The fault assumption: “failure to switch or failure to switch completely” can be excluded under the following conditions: positive mechanical operation of the moving parts, provided the actuating force is sufficiently high. On hydraulic directional control valves, a fault exclusion can be formulated for the failure of a special type of seat and cartridge valve (refer to the remarks in EN ISO 13849-2, Table C.3) to open when it controls the main volumetric flow of the pressure medium in conjunction with at least one further valve.

C.2.1.2 Electrical components

- Optocouplers

  The fault assumption of a “short-circuit between any two input and output connections” can be excluded under the following conditions: the optocoupler is constructed in accordance with overvoltage Category III to IEC 60664-1. If an SELV/PELV power supply is employed, pollution degree 2/overvoltage Category II is sufficient. Measures are taken to ensure that an internal fault in the optocoupler cannot lead to an excessive rise in the temperature of its insulating materials.

- Printed circuit board/populated printed circuit board

  In accordance with the standard, the fault assumption of a “short-circuit between adjacent tracks/pads” can be excluded provided the following conditions are met:

  – A base material of at least EP GC to IEC 60893-1 is employed.

  – Creepage distances and clearances are dimensioned to at least IEC 60664-5 (for distances greater than 2 mm: IEC 60664-1) with pollution degree 2/overvoltage Category III. If both conductor tracks are powered by an SELV/PELV power supply, pollution degree 2/overvoltage Category II with a minimum clearance of 0.1 mm applies.

  – The assembled board is mounted in an enclosure giving ingress protection of at least IP 54, and the printed side is coated with an ageing-resistant varnish or other form of protective coating that is resistant to ageing and that covers all tracks.

  – In practice, it is now also acceptable for a high-quality solder resist or similar to be employed for the ageing-resistant varnish/protective coating. Supplementary coating of printed circuit boards in accordance with IEC 60664-3 may reduce the pollution degree forming the basis of the assumption, and thus also the required creepage distances and clearances.

  Where lead-free soldering methods and products are used, the formation of tin whiskers may give rise to electrical short-circuits. Tin whiskers are formed primarily on surfaces with a clean, shiny tin coating. The

projections, needle-like in form, may attain lengths of over 1 mm (note: a much lower value is stated in [1]) and cause electrical short circuits. The prevailing theory is that whiskers are caused by pressure arising during the tinning process. This possibility should be evaluated, particularly when fault exclusion is applied to a component, for example exclusion of a short-circuit.

If the risk of tin whisker formation is considered high, fault exclusion for a short circuit between component terminals on a PCB is not possible, even when the above conditions are satisfied. Whiskers on conductor tracks of PCBs have not been determined in the past. The conductor tracks are usually of copper, without tin coating. The reference [5; 6] can assist in assessment of the phenomenon.

- Conductors/cables

  The fault assumption of a "short-circuit between any two conductors" can be excluded when the conductors:

  – are permanently connected (fixed) and protected against external damage (e.g. by cable ducting, armouring); or

  – are laid in separate multicore cables or within an electrical compartment; or

  – are individually shielded with earth connection.

  A condition of the above is that the conductors and the compartment both satisfy the relevant requirements (see IEC 60204-1).

- Electromechanical position switches, manually operated switches

  Exclusion of the "Contact will not open" fault can be assumed subject to the following condition:

  – Contacts to IEC 60947-5-1:2003, Annex K open of their own accord. Note that this fault exclusion applies only to the electrical part of the switch (the fault exclusion is from the fault list for the electrical system). Subclause D.2.5 contains detailed information on the subjects of fault exclusion and modelling of electromechanical components.

C.3 Basic safety principles

Basic safety principles are governed in Tables A.1, B.1, C.1 and D.1 of the informative annexes of EN ISO 13849-2.

C.3.1 Applicable to all technologies

- Use of suitable materials and adequate manufacturing

  Materials and processes for manufacture and treatment are selected with consideration for the use and stresses.

- Proper dimensioning and geometry of all components

  All components are selected in consideration of their compatibility with the anticipated operating conditions. Further criteria include switching capacity, rate of operations, withstand voltage, pressure level, dynamic pressure behaviour, volumetric flow, temperature and viscosity of the hydraulic fluid, type and condition of the hydraulic fluid or compressed air.

- All components are resistant to the environmental conditions and relevant external influences.

  The SRP/CS is designed to be able to perform its functions under the external influences usually associated with the application. Important criteria include mechanical influences, climatic influences, the leak tightness of the enclosure, and the resistance to electromagnetic interference.

- Principle of de-energization (closed-circuit current principle)

  The safe state is attained by removal of the control signal (voltage, pressure), i.e. by de-energization. Important criteria include the safe state when the energy supply is interrupted, or effective spring return on valves in fluid power technology.

- Protection against unexpected start-up

  Unexpected start-up, caused for example by stored energy or upon restoration of the power supply, is prevented.

C.3.2 Examples of basic safety principles in fluid power technology

- Pressure limitation

  The pressure within a system or in subsystems is generally prevented from rising beyond a specified level by one or more pressure-relief valve(s). In pneumatic systems, pressure-control valves with self-venting are primarily employed for this purpose.

- Measures for the avoidance of impurities in the pressure medium

  The required purity grade of the pressure medium for the components used is attained by suitable equipment, generally a filter. In pneumatics, suitable dehumidification is also required.

C.3.3 Examples of basic safety principles in electrical technology

- Correct protective bonding

  One side of the control circuit, one terminal of each electromagnetically actuated device or one terminal of other electrical devices is connected to a protective earth conductor. This side of the device is not therefore used for example for deactivation of a hazardous movement. A short-circuit to ground cannot therefore result in (undetected) failure of a shut-off path.

- Transient suppression

  A facility for the transient suppression (RC element, diode, varistor) is connected in parallel with the load (not in parallel with the contacts).

C.3.4 Examples of basic safety principles in programmable systems/software

EN ISO 13849-2 does not describe basic safety principles for the use of programmable systems and software. The basic measures for SRESW and SRASW in accordance with subclauses 4.6.2 and 4.6.3 of the standard may however be regarded as basic safety principles (refer also to subclause 6.3). A further measure is monitoring of execution of the program in order to detect a defective sequence of commands/software modules, which may occur despite all care taken during verification and validation. Program sequence monitoring is generally implemented by means of an external, cyclically retriggered watchdog that must be capable of placing the SRP/CS in a defined safe state in the event of a defective execution of the program.

C.4 Well-tried safety principles

Tables A.2, B.2, C.2 and D.2 in the informative annexes of EN ISO 13849-2 address well-tried safety principles. Well-tried safety principles are employed in order to minimize or exclude critical faults or failures and thus to reduce the probability of faults or failures with an influence upon the safety function.

C.4.1 General well-tried safety principles for all technologies

- Overdimensioning/safety factor

  All equipment is subjected to loading below its rated values. The objective is to reduce the probability of failure.

- Positive mode of actuation

  Reliable actuation by rigid mechanical parts with positive, rigid rather than sprung connections. The objective is to attain reliable transmission of commands, for example by the direct opening of a contact when a position switch is actuated, even should the contact be welded.

- Limiting of electrical and/or mechanical parameters

  Force, distance, time, and rotational and linear speeds are reduced to permissible values by electrical, mechanical or fluid power equipment. The objective is to reduce the risk by improved control of hazards.

C.4.2 Examples of well-tried safety principles in fluid power technology

- Secure position

  The moving element of a component is held mechanically in a possible position (frictional restraint is not sufficient). Force must be generated in order for the position to be changed.

- Use of well-tried springs

  EN ISO 13849-2, Table A.2 contains detailed requirements for well-tried springs.

C.4.3 Examples of well-tried safety principles in electrical technology

- Limiting of electrical parameters

  Limiting of voltage, current, energy or frequency, for the avoidance of an unsafe state

- No undefined states

  Undefined states in the SRP/CS must be avoided. The SRP/CS must be designed such that its state can be predetermined during normal operation and under all anticipated operating conditions. This is to be achieved for example by the use of components with defined response behaviour (switching thresholds, hysteresis) and with a defined sequence of operations.

- Separation of non-safety and safety functions

  In order to prevent unexpectec influences upon safety functions, the functions concerned are implemented separately from non-safety functions.

C.4.4 Examples of well-tried safety principles in programmable systems/software

EN ISO 13849-2 does not describe well-tried safety principles for the use of programmable systems and software. The additional measures for SRESW and SRASW in accordance with subclauses 4.6.2 and 4.6.3 of the standard may however be regarded as well-tried safety principles (refer also to subclause 6.3). A further well-tried safety principle is the use of self-tests for the detection of faults in complex components such as microcontrollers. Table E.1 of the standard for estimation of the level of diagnostic coverage lists self-tests of this kind, such as memory tests and CPU tests. Information on the implementation of such tests can also be found in a BGIA Report [7]. Depending upon the application, “fault detection by the process” and “fault detection by comparison between channels” may be regarded as well-tried safety principles.

C.5 Well-tried components

Well-tried components for mechanical and electrical systems are dealt with by Tables A.3 and D.3 of the informative annexes of EN ISO 13849-2. Well-tried components are used in order to minimize or exclude critical faults or failures and thus to reduce the probability of faults or failures that impact upon the safety function. In accordance with the provisions for Category 1, general criteria for a well-tried component are that it:

a) has been widely used in the past with successful results in similar applications; or

b) has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

Complex electronic components (such as PLCs, microprocessors, ASICs) cannot be regarded as well-tried in the sense of the standard. Classification as a well-tried component is also dependent upon the application: a component may be considered well-tried in certain applications, whereas in other applications this must be excluded, for example owing to the environmental influences.

C.5.1 Example of a well-tried component in mechanical technology

- Spring

  A spring is deemed to be a well-tried component when the provisions in EN ISO 13849-2, Table A.2 concerning well-tried safety principles for the application of well-tried springs and the technical provisions for spring steels to ISO 4960 [8] are observed.

C.5.2 Examples of well-tried components in fluid power technology

EN ISO 13849-2 states no well-tried components for fluid power technology. The property of being well-tried is particularly dependent upon the application in question and upon observance of the requirements for well-tried components in Category 1 and the requirements of EN ISO 4413 [9] and EN ISO 4414 [10].

Examples of well-tried components for safety-related applications are:

- Directional control valves, stop valves and pressure valves

C.5.3 Examples of well-tried components in electrical technology

- Fuse

  Fuses and miniature circuit-breakers are equipment for protection against overcurrent. They interrupt an electrical circuit (de-energization principle) in the event of an excessively high current, caused for example by an insulation fault. A distinction must be drawn between fuses and circuit breakers. Lead fuses have for decades proved effective in protecting against overcurrent. Comprehensive provisions exist governing fuses [11; 12]. Provided they are used as intended and are correctly rated, failure of fuses can virtually be excluded.

- Emergency switching off device/emergency stop device

  Devices for emergency switching off and emergency stop in accordance with EN ISO 13850 [12] are employed for the initiation of action in an emergency. Both types of device feature direct opening auxiliary switches for interruption of the energy supply in accordance with Annex K of IEC 60947-5-1 [13]. A distinction is drawn between two types of auxiliary switch with direct opening action:

  – Type 1: with only one contact element, in the form of a direct opening contact

– Type 2: with one or more break contact elements and possibly with one or more make contact elements and/or one or more changeover contacts. All break contact elements, including the contact-breaking parts of the changeover contacts, must feature direct opening contact elements.

For further details, particularly concerning the modelling of emergency-stop devices, refer to subclause D.2.5.4.

- Switches with positive mode of actuation (direct opening action)

This particular type of switch is available commercially as a push-button, position switch, and selector switch with cam actuation, for example for the selection of operating modes. These switches have proved effective over many decades. They are based upon the well-tried safety principle of the positive mode of actuation by direct opening contacts. To be deemed a well-tried component, the switch must satisfy the requirements of IEC 60947-5-1, Annex K [13].

References

[1] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2012).

[2] IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (2016).

[3] IEC 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (2012).

[4] *Bömer, T.:* Fehlerlisten für sicherheitsbezogene Bauelemente – Bei der Prüfung unterstellte Fehlerarten. Code 340 220. In: IFA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. 2nd ed., Vol. 1/16, VI/2016. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany. Erich Schmidt, Berlin, Germany 2003 – loose-leaf ed. www.ifa-handbuchdigital.de/340220

[5] Measuring whisker growth on tin and tin alloy surface finishes, JESD22-A121A. Published by: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2008

[6] Environmental acceptance requirements for tin whisker susceptibility of tin and tin alloy surface finishes, JESD201A. Published by: JEDEC Solid State Technology Association, Arlington, Virginia, USA 2008

[7] *Mai, M.; Reuß, G.*: Self-tests for microprocessors incorporating safety functions or: "Quo vadis, fault?". BGIA-Report 7/2006e. Published by: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin, Germany 2006. www.dguv.de/ifa, Webcode: e91093

[8] ISO 4960: Cold-reduced carbon steel strip with a mass fraction of carbon over 0.25% (12.07).

[9] EN ISO 4413: Hydraulic fluid power – General rules and safety requirements for systems and their components (2010).

[10] EN ISO 4414: Pneumatic fluid power – General rules and safety requirements for systems and their components (2010).

[11] IEC 60269-1: Low-voltage fuses – Part 1: General requirements (2006) + A1 (2009) + A2 (2014).

[12] EN ISO 13850: Safety of machinery – Emergency stop function – Principles for design (2015).

[13] IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2016) + COR1 (2016).

Annex D:
Mean Time to Dangerous Failure ($MTTF_D$)

Changes with respect to the second edition (BGIA Report 2/2008e):

- Increase in the channel $MTTF_D$ cap to 2,500 years for Category 4 inserted
- Subclause D.2.4.2 and Figure D.3 revised to improve intelligibility
- In subclause D.2.3: increased $MTTF_D$ values for hydraulic values in accordance with good engineering practice inserted
- In subclause D.2.4: explanations inserted concerning the use of contactors and conversion of mechanical durability/electrical durability into B_{10D} values
- Figure D.3 revised
- In subclause D.2.5: Table D.2 (Good engineering practice methods) updated, including with higher $MTTF_D$ values for hydraulic valves operated only at long intervals; reduced B_{10D} value for "contactors with nominal load"; B_{10D} value instead of fault exclusion for emergency-stop devices and pushbuttons (e.g. enabling switches).
- In subclause D.2.5: comprehensive explanations inserted of the modelling of electromechanical components
- In subclause D.2.6: reference inserted to the deleted safety factor of 10 for typical electronic components

D.1 What does "$MTTF_D$" mean?

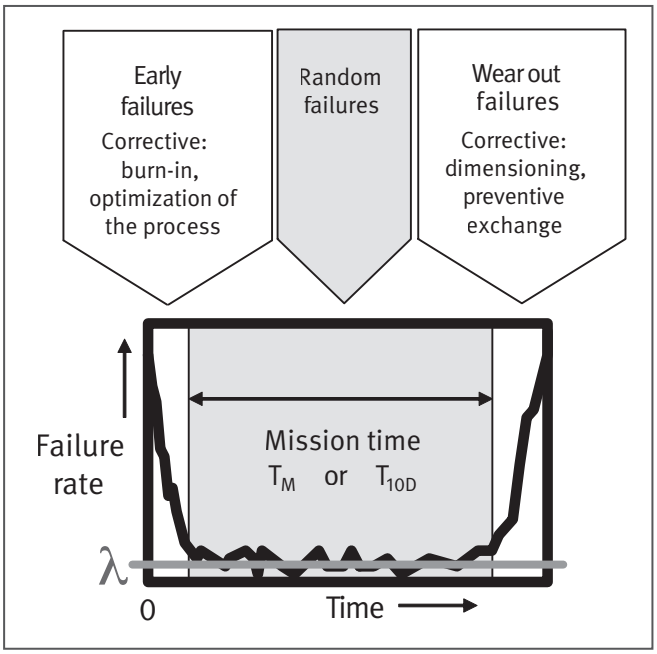
The mean time to dangerous failure $MTTF_D$ describes the reliability of the components used in a control system, and is one of several parameters that are used to determine the Performance Level. The $MTTF_D$ is defined in EN ISO 13849-1 as the "expectation of the mean time to dangerous failure". This emphasizes several aspects:

- The $MTTF_D$ is a statistical value, i.e. a value of empirical origin; in no way does it refer to a "guaranteed lifetime", "failure-free time", or the like.
- The $MTTF_D$ has the physical dimension of a period of time, and is generally stated in years.
- Only dangerous-mode failures are relevant, i.e. failures that impair performance of the safety function. Should the safety function be executed by several channels (redundancy), the term "dangerous failure" is used even if only one channel is affected.

D.1.1 Bath-tub life curve and constant failure rate

Component reliability is commonly described in terms of failure rates, abbreviated λ (and accordingly λ_D for dangerous failures only), the usual unit being FIT (failures in time, i.e. number of failures in 10^9 component hours, 1 FIT = 10^{-9} per hour). This failure rate describes the rate, at a particular point in time, at which functional components fail. In other words, the number of failures per unit time is divided by the number of components which at the point in time concerned have not yet suffered failure. The failure mode of many types of components (particularly electronic components) as a function of time takes the form, to a greater or lesser degree, of a "bath-tub life curve" [1] (see Figure D.1).

Figure D.1:
"Bath-tub life curve" of the failure rate



A greater number of components generally fail at the beginning of the mission time. These early failures dominate only for a short period. Once the recommended mission time has been exceeded, the failures begin to rise again. In the mid-range of the usual mission time, a plateau of a constant failure rate is often observed, particularly for electronic components. Random failures are typical for this phase. Even components which are affected more strongly by wear than by random failures, such as electromechanical or pneumatic components, can often be described over their mission time by the assumption of a constant failure rate estimated erring on the safe side. Early failures are generally disregarded, since com-

ponents exhibiting pronounced early failure patterns do not satisfy the availability requirements for a machine control system and are therefore not generally significant on the market. Suitable measures for the reduction of early failures are premature ageing (burn-in), selection, and optimization of the manufacturing process. In the interests of simplicity, constant failure rates within the mission time are therefore generally assumed in EN ISO 13849-1. The advantage of this assumption is that subsequent mathematical analysis is considerably simplified as a result, and forms the basis for the *Markov* modelling of the designated architectures upon which the bar chart/the simplified method of EN ISO 13849-1 are based. A constant failure rate results mathematically in a reliability curve which falls exponentially over the mission time, and in an anticipated value for the time to failure ($MTTF_D$) which corresponds to the reciprocal of the failure rate, i.e.:

$$MTTF_D = \frac{1}{\lambda_D} \qquad (D.1)$$

At a constant failure rate, the $MTTF_D$ is therefore equivalent to statement of a failure rate, whilst being much more illustrative. Whereas the practical significance of an FIT value is not very illustrative, statement of an anticipated time in years conveys the quality of components more graphically. Figure D.2 shows the statistically anticipated development of the proportion of dangerous failures over the mission time for four different $MTTF_D$ values. A further mathematical relationship can be observed here: at attainment of the $MTTF_D$ mark on the time axis, a statistical average of approximately 63% of all initially intact components have failed dangerously (not 50%, since although more components fail prior to attainment of the $MTTF_D$, the remaining, intact components with residual operation times in some cases of several times the $MTTF_D$ are of greater statistical influence).

D.1.2 Division into classes and capping

The assumption of an $MTTF_D$ for each component of relevance to safety (where reasons are not given for a fault exclusion) is a condition for the following steps, by which the $MTTF_D$ of each channel is produced, first at block and then at channel level. At channel level, EN ISO 13849-1 proposes division into three typical $MTTF_D$ classes (see Table D.1). These classes are intended to cancel out minor differences between the calculated $MTTF_D$ values, which in any case become irrelevant within the statistical uncertainty. They also serve to retain the equivalence to the other parameters (five Categories, four *DC* levels), and to provide the necessary simplification for presentation in the bar chart.

Table D.1:
Division into classes of the $MTTF_D$ for channels which execute the safety function

Description of the $MTTF_D$ for each channel	Range of the $MTTF_D$ for each channel
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years

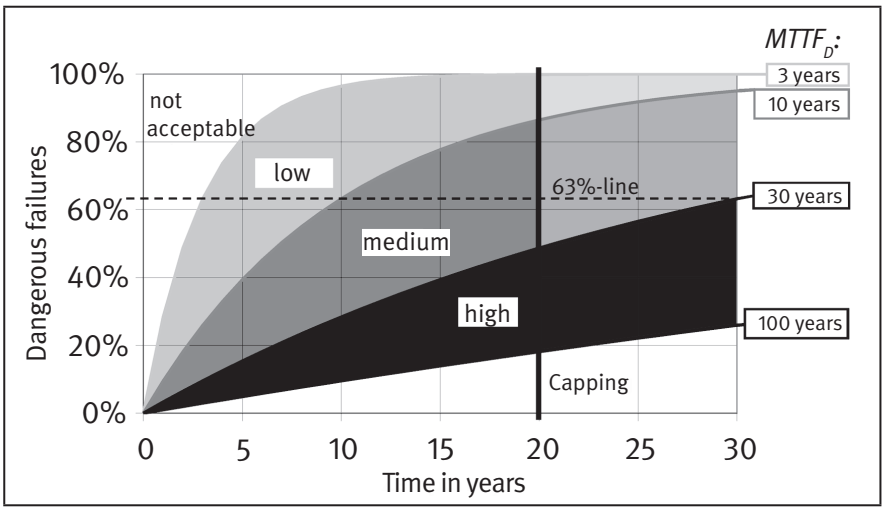


Figure D.2:
Illustration of the $MTTF_D$

The simplified quantification method to EN ISO 13849-1 assumes a usual mission time not exceeding 20 years for components in safety-related control systems in machine construction. Consequently, and with knowledge of the characteristic of the failure rate over time (Figure D.1), it becomes clear that a declared $MTTF_D$ value should be understood only as an illustrative indicator of the level of reliability within the mission time, and that it serves neither as a guarantee of a failure-free period before the $MTTF_D$ is reached, nor as a precise prediction of the point in time at which an individual component will fail. Once the wear phase is reached, the failure behaviour changes

fundamentally and can no longer be described realistically by a constant failure rate.

Desired side-effects of this classification are the rejection of $MTTF_D$ values of < 3 years from each channel, and the capping of higher $MTTF_D$ values for each channel to a maximum of 100 years (this capping is raised to 2,500 years for Category 4; these values are also to be assigned to the "high" class). Figure D.2 shows that with an $MTTF_D$ of three years, almost 30% dangerous failures can be expected after just one year, which would appear to be unacceptable for a safety-related control system. At the other end of the scale, statistical validation of reliabilities of > 100 years $MTTF_D$ appears highly questionable (this is acceptable in Category 4, since the other parameters determining the reliability, such as redundancy and fault detection, already have a high level). Furthermore, a residual probability of a dangerous failure within the mission time remains at $MTTF_D$ values of any magnitude, and may occur for other reasons (e.g. maloperation). It therefore appears inappropriate to validate high Performance Levels solely by the use of highly reliable components, without appropriate redundancy and fault detection.
In the bar chart to EN ISO 13849-1, this conclusion is expressed by the fact that no further $MTTF_D$ range is shown above the "high" $MTTF_D$ class, even though this would be possible according to the calculated probability. Higher $MTTF_D$ values are not capped to the maximum value of 100/2,500 years until the channel level, i.e. substantially higher $MTTF_D$ values may be substituted in the calculation for individual components.

D.1.3 What is the origin of the data?

A possible problem for users of the standard, particularly at the point at which the revised EN ISO 13849-1 was first published, was the lack of $MTTF_D$ data for components used in the SRP/CS [2]. In subclause 4.5.2, the standard proposes a hierarchy of data sources. The first of these are manufacturer's data [M], followed by typical values listed in the standard itself [S], and finally a very conservatively estimated substitutional value of ten years. Since this substitutional value relates to a component, and the lower limit of three years for the $MTTF_D$ value is soon reached where several components are employed in a channel, the $MTTF_D$ values listed in the standard itself were and are of particular importance. This will continue to be the case, at least until statement by the manufacturers of $MTTF_D$ values becomes the norm – including for components that were not developed from the outset for use in SRP/CS.

D.2 Differences between technologies

By its nature, the failure mode of components varies strongly according to the technology employed, since the "bath-tub characteristic" and the relevance of wear factors may differ. A very high $MTTF_D$ may be assumed for mechanical and hydraulic components, which are optimized in their design and use for high reliability and low wear. Random failures (in the constant failure rate phase) and wear failures are less significant for these components. Conversely, for the majority of electronic components, the failure behaviour over the typical mission time of comparatively "cheap" industrial components is generally well described by a constant failure rate, since the wear phase is reached only under exacerbated operating conditions. The failure behaviour of electromechanical or pneumatic components is very different again in its nature. The wear phase of these components can easily be reached within the usual mission time. For this reason, the attainable number of successful operation cycles is generally stated as the parameter, rather than a lifetime in terms of a time or failure rate per unit time. Consideration must be given to all these technology-specific aspects during calculation of the $MTTF_D$ value. For this reason, the standard proposes differentiated procedures.

D.2.1 $MTTF_D$ of mechanical control components

The approach employing constant failure rates is, unfortunately, not well suited to mechanical control components. At the same time, almost all safety functions involve mechanical control elements, at least where the sensors or actuators of mechanical control components are concerned that have the function for example of detecting movements or stopping hazardous movements. Although it would often be possible for an $MTTF_D$ estimated erring on the safe side to be stated for these components, fault exclusion is generally employed in this case. Provided the requirements for the fault exclusion are observed and documented, this is generally the most elegant means of considering the reliability of the mechanical components. These requirements include adequate resistance to the anticipated environmental influences, i.e. the validity of a fault exclusion depends upon the selected application. Another requirement is that of adequate overdimensioning, which ensures for example that the mechanical components are subjected to stress only within the fatigue limit. If fault exclusion is not possible, the good engineering practice procedure described below may provide a means by which an $MTTF_D$ value can be estimated.

D.2.2 BIA-Report 6/2004, "Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen" (study of the ageing process of hydraulic directional control valves)

On hydraulic systems, valves warrant special consideration as a "safety-related part of the control system"; valves that control hazardous movements or states, in particular, are extremely important for calculation of

the Performance Level. Experience has shown that the failure behaviour of hydraulic valves is characterized less by random failures than by failures due to wear. The causes of such failures are primarily systematic, such as excessive stress, unfavourable conditions of use, or lack of maintenance. In order for the lifetime of hydraulic valves to be estimated better, the IFA (at that time still the BGIA) launched a degree thesis on the subject, the results of which are available in the form of BIA-Report 6/2004, "Untersuchung des Alterungsprozesses von hydraulischen Wegeventilen" [3] (study of the ageing process of hydraulic directional control valves). Since valves that assume control tasks are generally piston-type directional control valves, the $MTTF_D$ values for "hydraulic components" were determined on valves of this type. The most important results of this study are presented briefly below.

Estimation of an $MTTF_D$ value is based in the first instance upon failure rates for hydraulic piston-type directional control valves that were determined in a study conducted in the maintenance departments of two large-scale users of hydraulic equipment (referred to below as users A and B). The failure rates were determined by the evaluation of computer data (quantities of re-ordered hydraulic piston-type directional control valves, repair reports) and involvement in maintenance work. In addition to the failure data for the valves, the operating conditions were also taken into account. The comparability of the $MTTF_D$ values determined for the different users of hydraulic systems is therefore assured. For validation and confirmation of these data, further failure data were collected by a survey of valve manufacturers. In the case of User A, the failure rates for the directional control valves were recorded in the maintenance department of a transmission production plant. Data were available for all failures of directional control valves over a period of 38 months, during which 143 directional control valves failed. Approximately 8,050 directional control valves of various ages were in use on the machines, for the most part machine tools, in the transmission production plant. If a constant failure rate is assumed during this period, an $MTTF_D$ of 178 years can be calculated as the reciprocal of the failure rate from the data for User A. At this user's plant, the operating conditions specified by the manufacturers were observed for the most part on the hydraulic systems. Since the facility primarily comprised new production lines, condition-based maintenance was performed.

The failure data for the directional control valves at User B's facility were likewise recorded in the maintenance department of a transmission production plant. Approximately 25,000 directional control valves varying in age were in use in this case. Data were available for all directional control valves that had failed over a period of four years (2000 to 2003). In contrast to User A's situation, the failure data for each year were available. It was therefore possible to calculate an $MTTF_D$ for each individual year. The $MTTF_D$ rose, from 195 years in 2000 to 300 in 2003. A significant relationship was observed between valve failures and operating/environmental conditions, since the maintenance measures and operating conditions in User B's facility had been improved continually over the years. In addition, the operating conditions were superior to those in User A's plant owing to further measures, such as monitoring of the fluid temperature; larger fluid reservoirs, generally located outside the machine; finer return line filters; and flue gas discharge systems for reducing the impurities in the ambient atmosphere. The study showed that, in conjunction with the type, quality, and level of contamination of the hydraulic fluid used and the design, material and type of the centering/return spring, the cylindrical guides of the components in valves, e.g. spool valves, had a substantial influence upon the anticipated lifetime of hydraulic piston-type directional control valves. A clear relationship was also established between the quality of the operating conditions and the attained lifetime to failure over a defined period of observation.

D.2.3 $MTTF_D$ of hydraulic control components

Based upon the results of the above study, an $MTTF_D$ of 150 to 1,200 years is proposed in EN ISO 13849-1 for hydraulic components, provided certain conditions are met. The valves studied were primarily of the piston type. Owing to the similarity in failure behaviour, however, the lifetime $MTTF_D$ determined for these valves serves as a good estimation for all safety-related hydraulic valves. This is however conditional upon observance during design and manufacture of the basic and well-tried safety principles described in EN ISO 13849-2 for hydraulic valves. The basic and well-tried safety principles for application, likewise described in EN ISO 13849-2, must also be stated by the valve manufacturer (in the manufacturer's data, operating conditions) and observed in practice.

Annex C.2, Table C.1 of EN ISO 13849-2 states the basic safety principles for hydraulic systems. The most important principles include the use of suitable materials and manufacturing procedures, and the principles of isolation, pressure limitation, protection against unexpected start-up, and a suitable temperature range (for further details, see Annex C).

Annex C.3, Table C.2 of EN ISO 13849-2 lists well-tried safety principles for hydraulic systems. The most important principles comprise overdimensioning/safety factors, speed limitation/reduction by means of a resistance for attainment of a defined volumetric flow, force limitation/reduction, an appropriate range for the operating conditions, monitoring of the condition of the pressure medium, the use of well-tried springs, and sufficient over-

lap in piston-type valves (for further details, refer again to Annex C).

Experience gained through application of the second edition of the standard has shown that for hydraulic valves, the frequency of actuation n_{op} (number of actuations per year, see subclause D.2.4) is also a relevant parameter for the reliability. For this reason, the third edition of the standard states graded $MTTF_D$ values of between 150 and 1,200 years for hydraulic valves (see Table D.2) as a function of n_{op} as part of the good engineering practice method (see subclause D.2.5).

Even though the standard states $MTTF_D$ values for hydraulic valves subject to these conditions, each valve manufacturer should, if at all possible, determine failure statistics for his own components and state an $MTTF_D$ value of his own.

D.2.4 $MTTF_D$ of pneumatic and electromechanical control components

In fluid power, mechanical and electromechanical technology, the lifetime and reliability of the components are generally determined by the wear characteristics of the moving elements.

In fluid power components such as valves, which generally constitute complex units with a large number of moving elements (such as pistons, plungers, springs in the pilot and main stages), the operational environmental conditions may also strongly influence the lifetime. These include, in particular:

- The quality and condition of the pressure medium (compressed air)
- Compatibility of seals with the lubricants
- Temperature influences
- Environmental influences such as dusts, gases, fluids

Observance of the requirements specified by the component manufacturer is crucial, since the parameters for the failure behaviour of the component from which the control system category is calculated are not otherwise valid.

A distinction is drawn between contactors and contactor relays. Contactor relays are used to implement logic and to drive contactors. Where higher power ratings must be switched, for example motors › 3 kW, contactors are generally used. Contactor relays are governed by the provisions of IEC 60947-5-1, contactors by those of IEC 60947-4-1.

Comprehensive criteria must be observed for their selection and use. These particularly include:

- System and operating conditions
- Operation functions and conditions
- Rate of operations and durability
- Protection against over-current and over-temperature
- Protection against over-voltage
- Special conditions of use

The manufacturers provide manuals containing comprehensive information on selection and engineering.

In the context of quantification in accordance with EN ISO 13849, the selection criteria for the lifetime will be considered briefly here. A distinction is drawn between the mechanical and electrical durability. The mechanical durability of a contactor is expressed by the number of operation cycles attained by the contactor without loading of the conducting paths. It is dependent upon the wear of the mechanical moving parts.

The electrical durability of switchgear is expressed by the number of operation cycles at the attainment of which the electrical contact elements are worn out. The electrical contact elements are stressed during operation under electrical load, during both the contact making and breaking processes. This causes wear of the contact members in the form of contact pitting. It varies as a function of the voltage, current, load type (e.g. inductive) and duration. Complete contact pitting generally leads to contact welding. In applications relevant to safety, this must be detected, in order for hazardous states caused by failure of the contacts to open to be detected. For detection to be assured, mechanically linked contacts must be used on contactor relays, or mirror contacts on contactors. The manufacturer's information must be observed here.

The mechanical durability and the electrical durability of the contact elements are determined by the manufacturers in test series. These values are however not independent of each other. The actual durability of the contactor may depend upon the power and operating mode of the electrical load, as well as upon the mechanical wear. The durability of the device is influenced by these values.

The B_{10D} values stated in Table D.2 of this report (see subclause D.2.4.1) for the durability of the device are for orientation only. Preference should be given to the values stated by the manufacturer. Should the manufacturer himself not state a B_{10D} value, but state values (number of operation cycles) for the mechanical and electrical durability, the lower of these values (generally dependent upon the load in the case of the electrical durability) can be used as an estimate of the B_{10} value. The B_{10D} can be obtained by doubling of this value (see subclause D.2.4.1).

Table D.2:
Typical reliability values that may be assumed to be reached when good engineering practice is followed

	Basic and well-tried safety principles to EN ISO 13849-2:2012	Other relevant standards	Typical values: $MTTF_D$ (years) B_{10D} (cycles)
Mechanical components	Tables A.1 and A.2	—	$MTTF_D$ = 150 years
Hydraulic components with $n_{op} \geq$ 1,000,000 cycles per year	Tables C.1 and C.2	EN ISO 4413	$MTTF_D$ = 150 years
Hydraulic components with 500,000 cycles per year ≤ n_{op} < 1,000,000 cycles per year	Tables C.1 and C.2	EN ISO 4413	$MTTF_D$ = 300 years
Hydraulic components with 250,000 cycles per year ≤ n_{op} < 500,000 cycles per year	Tables C.1 and C.2	EN ISO 4413	$MTTF_D$ = 600 years
Hydraulic components with n_{op} < 250,000 cycles per year	Tables C.1 and C.2	EN ISO 4413	$MTTF_D$ = 1,200 years
Pneumatic components	Tables B.1 and B.2	EN ISO 4414	B_{10D} = 20,000,000 cycles
Relays and contactor relays with small load	Tables D.1 and D.2	EN 61810-1/-2/-3 EN 60947-4-1 EN 60947-5-1	B_{10D}= 20,000,000 cycles
Relays and contactor relays with nominal load	Tables D.1 and D.2	EN 61810-1/-2/-3 EN 60947-4-1 EN 60947-5-1	B_{10D}= 400,000 cycles
Proximity switches with small load	Tables D.1 and D.2	EN 60947-5-3 EN ISO 14119	B_{10D}= 20,000,000 cycles
Proximity switches with nominal load	Tables D.1 and D.2	EN 60947-5-3 EN ISO 14119	B_{10D}= 400,000 cycles
Contactors with small load	Tables D.1 and D.2	EN 60947-4-1	B_{10D}= 20,000,000 cycles
Contactors with nominal load	Tables D.1 and D.2	EN 60947-4-1	B_{10D}= 1,300,000 cycles
Position switches [a]	Tables D.1 and D.2	EN 60947-5-1 EN ISO 14119	B_{10D}= 20,000,000 cycles
Position switches (with separate actuator, guard-locking) [a]	Tables D.1 and D.2	EN 60947-5-1 EN ISO 14119	B_{10D}= 2,000,000 cycles
Position switches [b] and push-buttons [b] under resistive load and with over-dimensioning (≤ 10% of the maximum load) of the electrical contacts	Tables D.1 and D.2	EN 60947-5-1 EN ISO 14119	B_{10D} = 1,000,000 cycles
Position switches [b] and push-buttons [b] with over-dimensioning in accordance with Table D.2, EN ISO 13849-1:2012 of the electrical contacts	Tables D.1 and D.2	EN 60947-5-1 EN ISO 14119	B_{10D} = 100,000 cycles
Emergency-stop devices [a]	Tables D.1 and D.2	EN 60947-5-5 EN ISO 13850	B_{10D}= 100,000 cycles
Enabling switches	Tables D.1 and D.2	EN 60947-5-8	B_{10D}= 100,000 cycles

[a] If fault exclusion is possible for direct opening action
[b] For make contacts and for break contacts, if fault exclusion is not possible for direct opening action

If the following characteristics are satisfied, the $MTTF_D$ value for a single pneumatic, electromechanical or mechanical component can be estimated by means of the formulae shown further below:

- The manufacturer of the component confirms that the basic safety principles to EN ISO 13849-1:2012, Table B.1 or Table D.1 were applied during design of the component (confirmation on the data sheet for the component).
- The manufacturer of a component for use in a Category 1, 2, 3 or 4 control system confirms that well-tried safety principles to EN ISO 13849-2:2012, Tables B.2 or D.2 were applied during design of the component (confirmation on the data sheet for the component).

- The manufacturer of the component specifies the suitable application and operating conditions for design of the SRP/CS and for the application. The designer of the SRP/CS satisfies the basic safety principles to EN ISO 13849-1:2012, Tables B.1 or D.1 for implementation and operation of the component and informs the user of his responsibility to satisfy the basic safety principles that he is required to implement. For the Categories 1, 2, 3 or 4, the same obligation applies with regard to satisfaction of the well-tried safety principles to EN ISO 13849-1:2012, Tables B.2 or D.2, and in turn during implementation and operation of the component.

The actual measures behind the basic and well-tried safety principles are similar to those described above in greater detail for hydraulic components.

The $MTTF_D$ value is defined as the mean time to dangerous failure. In order for this time to be determined for a component, corresponding lifetime characteristics must be defined. Such characteristics may be the distances travelled by pneumatic cylinders, the frequency of actuation of valves or electromechanical components, and stress reversal in the case of mechanical components. The reliability of pneumatic or electromechanical components is generally determined in the laboratory.

D.2.4.1 Determining of the lifetime value B_{10D}

The frequency of failure can be determined from values obtained in the laboratory or possibly in field studies, for example by means of *Weibull* statistics [4]. The two-parameter *Weibull* distribution function shown in Figure D.3 is more flexible than the exponential distribution, which it includes as a special case (b = 1).

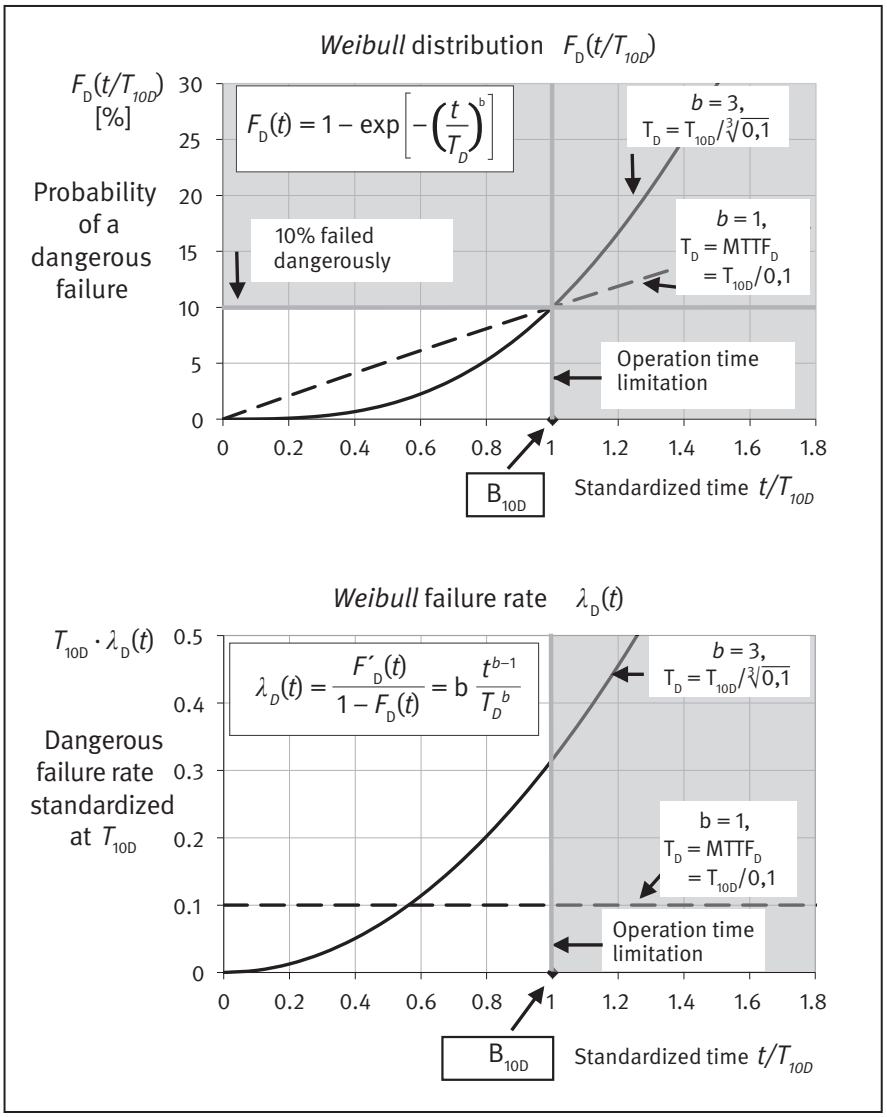


Figure D.3:
Illustration of the conversion from B_{10D} to $MTTF_D$

An increase in the failure rate following onset of the wear phase can be described well by b parameters › 1. The T parameter describes the characteristic life at which 63.2% of the components under consideration have failed.

If only dangerous failures are considered, this can be presented by the "D" suffix. Alternative methods can be used to determine the *Weibull* parameters, depending upon the test method. Such methods are also appropriate

when data are incomplete, for example when intact parts are to be considered. Results in the form of data for the parameters b and T can be read off from the diagrams. In turn, the nominal life T_{10}, at which 10% of the components studied have failed, can then be determined. The durabilities of pneumatic and electromechanical components are generally stated in the pseudo-unit of (operation) "cycles" rather than in the dimension of time. The mean number of operations per year n_{op} (in cycles per year, see subclause D.2.4.2) is used for conversion. The B_{10} value in cycles corresponds here to the time-based T_{10} value. The $MTTF_D$ value is determined as described below in subclause D.2.4.2 by the nominal life B_{10}. A reliability analysis employing *Weibull* statistics can be conducted by means of commercial software. The safety-related reliability values for fluid power and electromechanical components must be stated by the manufacturer of the components concerned. The reliability of pneumatic components can be determined with reference to ISO 19973, Pneumatic fluid power – Assessment of component reliability by testing. This standard currently comprises five parts:

- Part 1: General procedures
- Part 2: Directional control valves
- Part 3: Cylinders with piston rod
- Part 4: Pressure regulators
- Part 5: Non-return valves, shuttle valves, dual pressure valves (AND function), one-way adjustable flow control valves, quick-exhaust valves

Where the reliability of pneumatic valves is determined, the life (B_{10} value) is indicated in cycles before failure. The nominal life B_{10} (termed t_{10} in some references) is the average number of operation cycles by the attainment of which 10% of the units studied have failed. Since in the case of valves, the "availability" failure criterion also encompasses failures that are not relevant to safety (e.g. leakage above the defined threshold), it has been set out in the standard that the value determined for the nominal life (B_{10}) multiplied by two may be considered equal to the B_{10D} (dangerous) value (number of cycles until 10% of the components fail dangerously):

$$B_{10D} = 2 \cdot B_{10} \qquad \text{(D.2)}$$

The B_{10} value is generally determined in the laboratory. For this purpose, at least seven valves produced at different times are subjected to endurance testing. The maximum rate of operations for the endurance test is determined from the pressure build-up (attainment of 90% of the test pressure) and the pressure dissipation (attainment of 10% of the test pressure) in a connected volume that is defined according to the port cross-subclauses. At least five out of seven valves must fail for evaluation of the test results. The "maximum likelihood" and "rank regression" methods are stated in ISO 19973-1 as example methods for determining the *Weibull* parameters.

As an approximation, where testing is performed on a small number of test specimens, e.g. seven valves, the first failure determines the B_{10} value, i.e. the number of cycles attained by the time of the first failure corresponds approximately to the B_{10} value. Should the first failure be dangerous, the number of operation cycles performed up to this point approximates to the B_{10D} value.

Dangerous failures on pneumatic valves particularly include:

- Failure to switch (sticking at an end or zero position) or incomplete switching (sticking at a random intermediate position)
- Change in switching times
- Spontaneous change in initial switching position (in the absence of an input signal)

Analysis of the failures always refers to the entire modular unit, consisting for example of main valve and pilot valve.

D.2.4.2 Conversion of B_{10D} to $MTTF_D$

For the simplified method for estimation of a PL, the standard expects statement of an $MTTF_D$ value for consideration of random component failures. For electromechanical and pneumatic components however, B_{10D} are typically available, which must first be converted to $MTTF_D$ values. The standard provides an approximation formula for this purpose. This formula is subject to certain conditions:

$$MTTF_D = \frac{T_{10D}}{0{,}1} = \frac{B_{10D}}{0{,}1 \cdot n_{op}} \qquad \text{(D.3)}$$

This approximation is based upon reformulation in two steps. The B_{10D} value, stated in the pseudo unit of "cycles", is first converted to a T_{10D} value. This value is the elapsed time at which 10% of the components under analysis have failed dangerously:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \qquad \text{(D.4)}$$

The average number of actuations per year n_{op} (stated in cycles per year) serves as the conversion factor for this purpose. It is based upon the following parameters, which must be estimated for the anticipated application (if appropriate, the worst-case scenario):

- h_{op} → Mean operation in hours per day
- d_{op} → Mean operation in days per year
- t_{cycle} → Mean operation time between the beginning of two successive cycles of the component (e.g. switching of a valve) in seconds (s) per cycle.

The n_{op} (in cycles per year) can be determined from these parameters as follows:

$$n_{op} = \frac{d_{op} \cdot h_{op}}{t_{cycle}} \cdot 3{,}600 \frac{s}{h} \quad (D.5)$$

The second step in the approximation hidden in the formula (D.3) consists of the assumption of a "substitute failure rate" constant over time for the actual failure rate, of which wear is the dominant cause. This approximation, however, yields a result of adequate quality only up to attainment of the T_{10D} value (which equates in "cycles" to the B_{10D} value).

This part of the approximation is illustrated in Figure D.3. The unbroken curve represents the original *Weibull* distribution with an assumed shape factor of $b = 3$. In the particular case where $b = 1$, the *Weibull* distribution transitions to an exponential distribution that is characterized by a constant failure rate over time. The dashed line now refers to the exponential distribution corresponding to the "substitute failure rate", constant over time, which is equal to the reciprocal of the $MTTF_D$ value obtained by means of the formula (D.3). The $MTTF_D$ obtained by this means ensures that the exponential distribution shown by the dashed line intersects the original *Weibull* distribution at the point ($t = T_{10D}$; $F_D = 10\%$). The point at which 10% of the components under analysis have failed dangerously is therefore reached by both distributions following elapsing of T_{10D}. From Figure D.3, it can be seen that the actual failure rate prior to attainment of the wear phase is very low, and remains below the approximated exponential distribution up to point T_{10D}. This approximation is therefore conservative (on the safe side). The importance of limiting the mission time to T_{10D} is also evident: above this value, the proportion of dangerous failures which may actually be expected rises significantly over time when compared to the exponential substitute function. The validity of the approximation based upon the substitute failure rate constant over time can be extended by preventive replacement of the affected component when the T_{10D} value is reached.

In the lower part of Figure D.3, it can be seen clearly that the selected "substitute failure rate" $\lambda_D = 1/MTTF_D$ of the exponential approximation corresponds approximately to the arithmetic mean of the failure rate which may actually be expected up to the point in time T_{10D}. Beyond T_{10D} however, the onset of the wear phase results in strong variation.

Formula (D.3) is derived from the condition

$$F(T_{10D}) = 1 - \exp(-\lambda_D \cdot T_{10D}) = 10\%$$

for the exponential distribution forming the approximation, where λ_D represents the "substitute failure rate" referred to above. Reformulation produces $\lambda_D = -\ln(0.9)/T_{10D}$. Since $\ln(0.9)$ approximates closely to 0.1 and $MTTF_D = 1/\lambda_D$, the result is finally $MTTF_D \approx T_{10D}/0.1$.

D.2.5 Good engineering practice methods

Should no component reliability data be available from the manufacturer, the standard proposes the use of values listed within it as the first alternative. It provides support in the form of typical values for mechanical, hydraulic and pneumatic components and for electromechanical safety components frequently used in practice. These values are listed as $MTTF_D$ values or B_{10D} values in Table D.2. The B_{10D} value, which is obtained by the component manufacturer by testing, indicates the average number of cycles at which 10% of the components have failed dangerously. This value can be used to estimate the $MTTF_D$ value. A number of conditions must however be met when the values in Table D.2 are used:

- The manufacturer of the component confirms that basic safety principles to EN ISO 13849-1:2012 or the relevant standard (see Table D.2) were applied during design of the component (confirmation on the data sheet for the component).
- The manufacturer of a component that is to be used in a Category 1, 2, 3 or 4 control system confirms that well-tried safety principles to EN ISO 13849-1:2012 or the relevant standard (see Table D.2) were applied during the design of the component (confirmation on the data sheet for the component).
- The manufacturer of the component specifies the suitable application and operating conditions for the SRP/CS designer and the user and informs them of their responsibility to satisfy the basic safety principles to EN ISO 13849-1:2012 during implementation and operation of the component.
- The designer of the SRP/CS and the user satisfy the basic and/or well-tried safety principles to EN ISO 13849-1:2012 for implementation and operation of the component.

Compliance with these requirements is to ensure that the application of basic and/or well-tried safety principles is assured from manufacture, through implementation,

to routine operation of the component. The interface between the manufacturer, the designer of the SRP/CS and the user of the machine (operating party) is clearly defined: the manufacturer must provide binding confirmation that the safety principles were observed during design, and must make all relevant information available concerning the conditions of use and operation. The designer of the SRP/CS and the user of the machine (operating party) are in turn responsible for observing all safety principles concerning implementation and operation of the component. Provided these conditions are met, the typical values cited in Table D.2 can be used for calculation of the $MTTF_D$, if applicable via the B_{10D}. The $MTTF_D$ value of 150 years for hydraulic control components, the reasoning for which is stated above, is extended here to include mechanical components. This secondary value can be used when reasoning cannot be provided for a fault exclusion but when the use of basic/well-tried safety principles is assured. In addition, B_{10D} values for electromechanical components are stated that can be converted to an $MTTF_D$ value in accordance with the procedure also described above involving the average number of actuations per year n_{op}.

All values in the table relate to dangerous failures only, as expressed by the "D" suffix. It has generally been assumed here that only half of all failures are dangerous. The third edition of the standard however deviated from this rule for "contactors with nominal load", and the proportion of dangerous failures (75% break faults or short-circuits) stated in Table K.2 of the IEC 60947-4-1 product standard [5] was used for conversion. This leads to a reduced B_{10D} value compared to that in the second edition of the standard, namely 1,300,000 rather than 2,000,000 cycles. Consequently, the values stated here may well appear more optimistic than those indicated on manufacturers' data sheets, which relate to all fault types that could impair functionality in the sense of availability. On some electromechanical components, for example relays, contactor relays and contactors, the electrical load of the contacts is a major factor determining the B_{10D} value, as is frequently confirmed by observations in the field. At low electrical load (typically resistive load), described by EN ISO 13849-1 as up to 20% of the rated value, substantially better values are obtained. The mechanical rather than the electrical durability was assumed decisive in this case (see subclause D.2.4). Depending upon the type (resistive or inductive) and magnitude of the load, B_{10D} values lying between the extremes stated here may be derived. For the position switches, guard-locking devices, emergency stop devices and pushbuttons, such as enabling switches, listed in the table, the safety principle of direct opening action is generally a requirement for the electrical part. Between the second and third editions of the standard, certain changes took place for these components in the good engineering practice method as a result of experience gained with application in the field. This topic will therefore be discussed separately in detail in subclauses D.2.5.1 to D.2.5.6 below.

By their nature, these approaches constitute major simplifications of the actual, complex relationships. A very low load current in particular, combined with infrequent actuation, can for example lead to cold welding of electrical contacts. These effects should however be avoided by the required application of basic/well-tried safety principles. These principles include the suitability of both the mechanical and electrical component characteristics and their adaptation to the anticipated load.

D.2.5.1 Modelling of electromechanical components (position switches, guard-locking devices, emergency stop devices, enabling switches and pushbuttons)

It has been seen in practical application of the standard to date that considerable uncertainty exists regarding the modelling of electromechanical components. This can also be seen from the fact that the language between the two parts of the standard differs to some extent in this context: whereas the first part selects an approach involving B_{10D} within the good engineering practice method (see Table D.2), the second part addresses possible fault exclusions. This is exacerbated by the fact that for many of these components, a clear distinction cannot be made between their mechanical and electrical parts. Consequently, the requirements and information in both parts of the standard will first be presented below in general terms; a pragmatic modelling approach will then be proposed for the various electromechanical components that draws primarily upon Part 1 of the standard. Part 2 can also be applied as an alternative; implementation often fails in practice however owing to the fact that complete fault exclusion for the mechanical and electrical part requires confirmation by the manufacturer – for example in the data sheet – or precise knowledge of the conditions of use. In practice, the two conditions are often not met.

What is stated in the standard? – Electromechanical components in accordance with Part 1 of the standard

With the good engineering practice method introduced above, EN ISO 13849-1:2015 proposes that subject to satisfaction of the conditions set out below, the typical B_{10D} values [S] for position switches, guard-locking devices, emergency stop devices, enabling switches and pushbuttons stated in Table D.2 may be assumed:

- Use of basic and well-tried safety principles in design, application and operation of the component (see Tables D.1 and D.2 to EN ISO 13849-2), and

- The possibility of fault exclusion for direct opening action (contacts to IEC 60947-5-1, Annex K, characterized in the conceptual circuit diagrams by ⊖)

Manufacturer's data [M] should of course always be given preference over typical values stated in the standard. Regarding modelling, the standard states that the components "*can be estimated as a Category 1 or Category 3/4 subsystem depending on the number of electrical output contacts and on the fault detection in the subsequent SRP/CS. Each contact element (including the mechanical actuation) can be considered as one channel with a respective B_{10D} value.*"

Although this statement refers directly only to emergency stop devices and enabling switches, the principle can also be applied to other electromechanical components.

It appears at first glance inconsistent for single-channel or two-channel modelling to be determined by the number of electrical output contacts, despite the fact that fault exclusion for direct opening action can be assumed for mechanically linked contact elements. However, the statement that the B_{10D} value of each channel is to apply to the contact element including its mechanical actuation shows this to be a strategy intended to present, in the simplest way possible, the complex interrelationship of mechanical and electrical elements in the electromechanical components referred to. The focus lay here not upon the details of the electromechanical design, but upon a recipe that is as simple as possible:

- An electromechanical component employing **one** contact element with direct opening action that satisfies the above conditions can be modelled as part of a Category 1 subsystem. In the functional channel, the subsystem contains a block with the corresponding B_{10D} value.

- An electromechanical component employing (at least) **two** contact elements with direct opening action that satisfies the above conditions can be modelled as part of a Category 3 or 4 subsystem, depending upon fault detection in the downstream SRP/CS. In each of the two functional channels, the subsystem contains one block with the corresponding B_{10D} value.

Beyond the general case, EN ISO 13849-1 adds that "*in some cases it may be possible, that the machine builder can apply a fault exclusion according to EN ISO 13849-2, Table D.8 considering the specific application and environmental conditions of the device.*". The formulation of fault exclusion for an electromechanical component is therefore on the one hand an issue for the component manufacturer, who alone is familiar with the detail of its mechanical design. At the same time, it must be considered with respect to the application whether fault exclusion is permissible in consideration of ambient, operating and application aspects. These are special cases in which the machine manufacturer excludes certain faults on a case-by-case basis for specific applications in consultation with the component manufacturer.

What is stated in the standard? – Electromechanical components in accordance with Part 2 of the standard

Table D.8 of EN ISO 13849-2 applies to switches, such as electromechanical position switches and manually operated switches, and can therefore be applied to all the electromechanical components referred to above. The following conditions are stated for exclusion of the fault "failure of contacts to open":

- The switch must satisfy IEC 60947-5-1:2003, Annex K, i.e. it must possess contact elements with direct opening action.

- Fault exclusion applies only up to a maximum of PL d. PL e requires redundant components, i.e. a second (position) switch (exception: emergency-stop devices).

This yields, irrespective of the number of electrical contact elements, the following result for position switches (with and without separate actuator), guard-locking devices, enabling switches and pushbuttons:

- Up to PL d: fault exclusion is permissible and may also apply to the mechanical aspects, subject also to confirmation by the manufacturer. Modelling as a Category 3 encapsulated subsystem (with single-fault tolerance) and direct statement of PL d and PFH_D of zero. The coupling between PL and PFH_D must be cancelled for this purpose in SISTEMA (under Subsystem, "PL" tab).

- PL e: no fault exclusion (for mechanical and electrical aspects) is permissible

For emergency stop devices in accordance with IEC 60947-5-5, fault exclusion with respect to the "failure of contacts to open" is permissible for mechanical aspects up to PL e, provided a maximum number of actuations is considered. In the past, 6,050 actuations to IEC 60947-5-5 was employed in this context as the number of operation cycles over the lifetime.

As mentioned in the preceding subclause, the permissibility of fault exclusions in principle is of only limited relevance in practice.

The requirements stated in the standard are applied below to frequently used electromechanical components.

D.2.5.2 Position switches

Electromechanical position switches manufactured in accordance with IEC 60947-5-1 employing one or two electrical contact elements with direct opening action in accordance with IEC 60947-5-1, Annex K can be considered as described in Table D.3. The B_{10D} value that can be applied (to one or two channels) in accordance with the good engineering practice method is 2,000,000 cycles for position switches with separate actuator and 20,000,000 cycles for all other position switches.

Positive actuation of the switch (e.g. the actuating mechanism, attachment of the actuator) is important, as well as the switch itself. The relevant requirements of EN ISO 13849-2, Annex A must also be satisfied for the requisite fault analysis, including of possible fault exclusions. In accordance with EN ISO 13849-2, Table D.8, a maximum of PL d is attainable with a single position switch (even with two contact elements). The relevant Type C standards for machines may contain provisions deviating from this, such as the use of two position switches for Category 3.

Information on the selection and fitting of position switches can be found in DGUV Informative publication 203-079 [6] (in German).

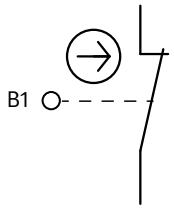
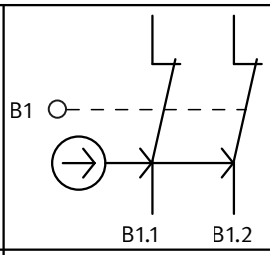
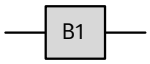
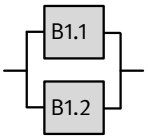
Conceptual schematic circuit diagram		
Safety-related block diagram		
Modelling	Block B1 B_{10D} = 2,000,000 or 20,000,000 cycles [N] or manufacturer's data [M]	Blocks B1.1 and B1.2 per block: B_{10D} = 2,000,000/ 20,000,000 cycles [S] or manufacturer's data [M]
Category and PL	Category 1 max. PL c	Category 3 max. PL d

Table D.3:
Modelling of position switches in the conceptual schematic diagram and in the safety-related block diagram, with Category and PL assignment

D.2.5.3 Guard-locking devices

Guard-locking devices in this context are equipment for the mechanical blocking of closed guards, with integrated position switch(es), considered as a modular unit, by means of which the safety functions of guard locking and interlocking (position monitoring of the safeguard) can be implemented. Of the "guard locking" safety function, only position monitoring of the locking element will be considered below. For discussion of the complete "guard locking" safety function, refer to subclause 8.2.19 (Example 19). Besides the arrangement for monitoring the position of a guard, an interlocking device with guard locking also possesses a facility for blocking the moving guard in the closed position. As long as this facility is active, the guard cannot be opened.

A product standard for guard-locking devices does not exist; basic safety requirements are however listed in EN ISO 14119. The GS-ET-19E test principles [7] also govern guard-locking devices as modular units. According to these principles, electromechanical guard-locking devices contain a position switch for position monitoring of the safeguard (guard door) and a position switch for position monitoring of the locking element (see Figure D.4).

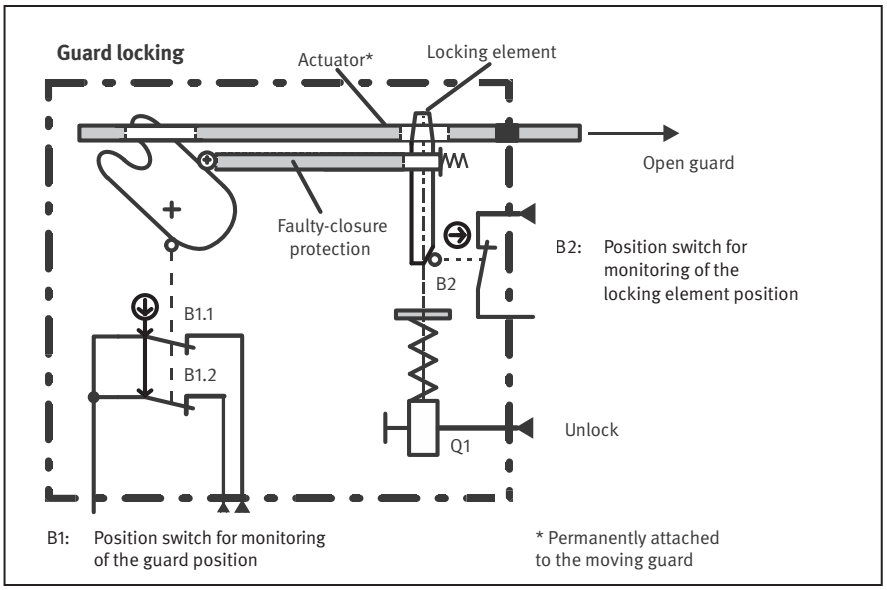


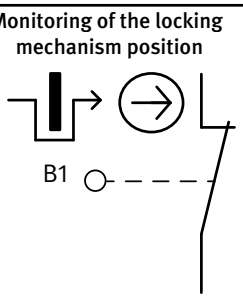
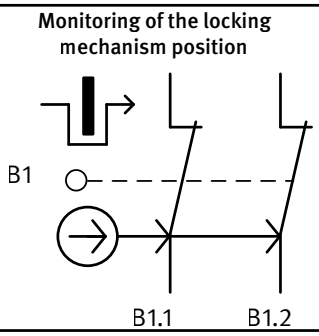
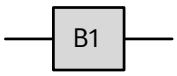
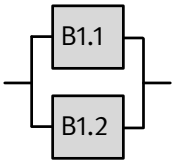
Figure D.4:
Conceptual presentation of a guard-locking device with faulty-closure protection and additional position monitoring of the safeguard (interlock)

If the guard-locking device uses the constructive element of a "faulty-closure protection", the position switch for position monitoring of the safeguard is not required: if the locking element is in the locked position, it can be assumed that the safeguard is closed. If the locking element is not in the locked position, no conclusion can be drawn regarding the position of the safeguard. Guard-locking devices can be considered as shown in Tables D.4 and D.5 in consideration of the requirements in EN ISO 14119 and the GS-ET-19E test principles.

Table D.4:
Modelling of guard-locking devices without faulty-closure protection in the conceptual schematic diagram and in the safety-related block diagram, with Category and PL assignment

Guard locking **without** faulty-closure protection				
Conceptual schematic circuit diagram	**Monitoring of the guard position** B1	**Monitoring of the locking mechanism position** B2	**Monitoring of the guard position** B1 B1.1 B1.2	**Monitoring of the locking mechanism position** B2 B2.1 B2.2
Safety-related block diagram	B1	B2	B1.1 B1.2	B2.1 B2.2
Modelling	Blocks B1 and B2 per block: B_{10D} = 2,000,000 cycles [S] or manufacturer's data [M]		Blocks B1.1, B1.2, B2.1 and B2.2 per block: B_{10D} = 2,000,000 cycles [S] or manufacturer's data [M]	
Category and PL	Category 1 max. PL c		Category 3 max. PL d	

Table D.5:
Modelling of guard-locking devices with faulty-closure protection in the conceptual schematic diagram and in the safety-related block diagram, with Category and PL assignment

Guard locking **with** faulty-closure protection		
Conceptual schematic circuit diagram	Monitoring of the locking mechanism position 	Monitoring of the locking mechanism position 
Safety-related block diagram		
Modelling	Block B1 B_{10D} = 2,000,000 cycles [S] or manufacturer's data [M]	Blocks B1.1 and 1.2 per block: B_{10D} = 2,000,000 cycles [S] or manufacturer's data [M]
Category and PL	Category 1 max. PL c	Category 3 max. PL d

The following can be summarized for guard-locking devices:

- The B_{10D} value that can be applied (to one or two channels) for guard-locking devices in accordance with the good engineering practice method is 2,000,000 cycles.
- The existence of the faulty-closure protection and the associated fault exclusion for the mechanical part must be confirmed by the manufacturer.
- A maximum of PL d can be attained by a single guard-locking device as a modular unit for the interlock function (even with two contact elements per position switch) in accordance with EN ISO 13849-2, Table D.8. If a PL of e is desired, it can be attained only by means of an external additional position switch for position monitoring of the safeguard.
- On guard-locking devices in the form of modular units, the guard-locking function is limited to PL d, since only one position switch exists for monitoring of the locking element and for the associated actuating mechanism.
- The restrictions stated in the relevant Type C standards for machines must be observed.

Guidance on the selection and fitting of guard-locking devices can be found in DGUV Informative publication 203-079 [6] (in German).

D.2.5.4 Emergency stop device

Emergency stop devices constructed in accordance with the IEC 60947-5-5 product standard can be considered as described in Table D.6 (see page 279).

D.2.5.5 Enabling switches

Three-position enabling switches constructed in accordance with the IEC 60947-5-8 product standard or the GS-ET-22E test principles [8] can be considered as described in Table D.7. Enabling switches are available with different contact sets (different numbers of make-/break-contact elements). The safety-related cancellation of the enabling function is attained on three-position enabling switches by releasing the switch or pressing it in fully. The two functions can be evaluated in the same way; with respect to release of the switch however, particular attention must also be paid to overdimensioning of the electrical (in this case make) contacts with regard to the load. The functions of "releasing" and "pressing in fully" are grouped below in a single safety function, since the direction of actuation is not predictable.

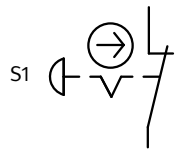
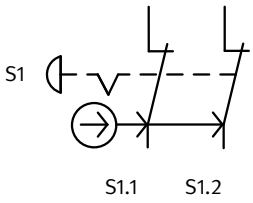
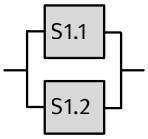
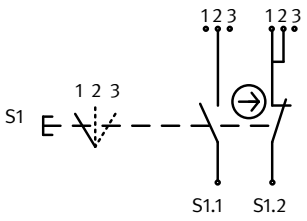
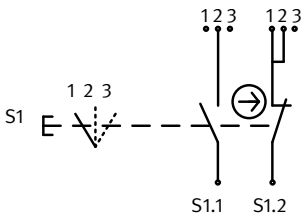
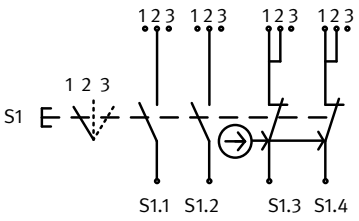
Conceptual schematic circuit diagram		
Safety-related block diagram		
Modelling	Block S1 B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M]	Blocks S1.1 and S1.2 per block: B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M]
Category and PL	Category 1 max. PL c	Category 3 or 4 max. PL e

Table D.6:
Modelling of emergency stop devices in the conceptual schematic diagram and in the safety-related block diagram, with Category and PL assignment

Table D.7:
Modelling of three-position enabling switches in the conceptual schematic diagram and in the safety-related block diagram, with Category and PL assignment

Conceptual schematic circuit diagram			
Condition	Break contact to EN 60947-5-1 Annex K	Enabling button to GS-ET-22E	Enabling button to GS-ET-22E
Safety-related block diagram			
Modelling	Block S1.1 B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M] Block S1.2 fault exclusion, PFH_D = 0	Block S1.1 B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M] Block S1.2 fault exclusion, PFH_D = 0	Blocks S1.1 and S1.2 per block: B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M] Blocks S1.3 and S1.4 per block: fault exclusion, PFH_D = 0
Category and PL	Category B max. PL b a)	Category 1 max. PL c	Category 3 max. PL d

a) Make contact S1 limits the attainable PL to b.
b) Adequate fault detection for the electrical contacts is implemented in the downstream SRP/CS.

The IEC 60947-5-8 product standard places no design requirements upon the opening function. This applies to both the make- and break-contact elements (releasing of the switch or pressing in fully). In particular, electrical contact elements with direct opening action to IEC 60947-5-1, Annex K are not required. They are not therefore well-tried components in this case, and Category 1 is consequently not possible.

The GS-ET-22E test principles set out particular design requirements, for example:

- For the “releasing” function: the use of well-tried springs, or a two-channel arrangement with contact monitoring
- For the “pressing in fully” function: electrical contact elements with direct opening action to IEC 60947-5-1, Annex K, or two-channel signal transmission with corresponding monitoring by the control system.

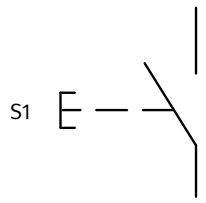
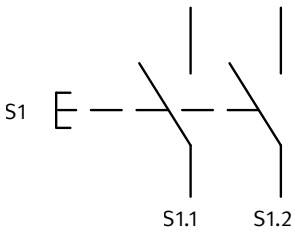
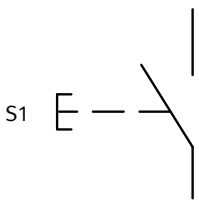
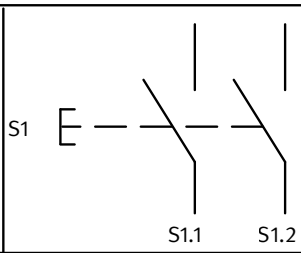
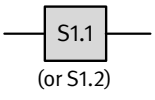
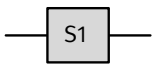
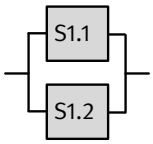
Design in accordance with GS-ET-22E provides safety comparable to that of a well-tried component.

Two-position enabling switches implement only the “releasing” safety function, and are not therefore contained in the IEC 60947-5-8 product standard. Where they satisfy the GS-ET-22E test principles, the same evaluation applies as in Table D.7 for make contacts of the three-position enabling switches: single-channel in Category 1 with a maximum PL of c, or two-channel in Category 3 with a maximum PL of d.

D.2.5.6 Pushbuttons

Pushbuttons to EN ISO 13849-2, Table D.8 are used for example for initiating a movement of limited duration or distance in inching mode. In this application scenario, they are always engineered as make-contact elements; the safety function is however dependent upon reliable opening of the make contact following actuation (comparable with the basic safety principle of de-energization (closed-circuit principle) to EN ISO 13849-2, Table D.1). The same analysis applies here as for the “releasing” function of a two-position enabling switch. Here too, particular attention must be paid to overdimensioning of the electrical contacts with respect to the load.

Table D.8:
Modelling of pushbuttons in the conceptual schematic diagram and in the safety-related block diagram, with Category and PL assignment

Conceptual schematic circiut diagram				
Condition	Pushbuttons to EN 60947-5-1	Pushbuttons to EN 60947-5-1	two-stage enabling button to GS-ET-22E	two-stage enabling button to GS-ET-22E
Safety-related block diagram				
Modelling	Block S1 B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M]	Block S1.1 or S1.2 per block B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M]	Block S1 B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M]	Blocks S1.1 and S1.2 per block B_{10D} = 100,000 cycles [S] or manufacturer‘s data [M]
Category and PL	Category B max. PL b	Category B max. PL b	Category 1 max. PL c	Category 3 max. PL d

For inching mode, Type C standards for machines often require an emergency-stop device in the vicinity of the pushbutton. Should the make contact fail to open following release of the pushbutton/inching button, the hazardous movement can be halted by actuation of the emergency-stop device. In addition, inching mode is often permitted only for a limited distance or duration, and/or with the SLS safety function (safely limited speed) activated. These measures cannot be quantified during determining of the PL (for example by means of SISTEMA), since they are dependent upon intentional action. It is therefore advisable for consideration to be given to the specific supplementary requirements for inching mode stated in a Type C standard when the PL_r is set.

Prevention of unintended start-up must also be considered: this leads to the need for control devices to EN 60947-5-1 to be used, even for the two PL b variants in Table D.8, for example in order to exclude the short-circuiting of adjacent contacts that are isolated from each as per Table D.8 of EN ISO 13849-2.

For higher risks (PL c or d), control devices to IEC 60947-5-1 are not sufficient, since they satisfy only Category B owing to their potential failure to open. “Safe” pushbuttons, such as two-stage enabling buttons to GS-ET-22E, are a suitable alternative. Versions of these pushbuttons with one make contact are suitable for use up to PL c, two-channel versions up to PL d.

D.2.6 $MTTF_D$ of electronic control components

As already mentioned, declaration of the failure rates λ and λ_D, for example in the form of FIT values (failures in time, i.e. failures in 10^9 component hours), has long been normal practice for electronic components. It is therefore very likely that reliability information can be obtained from the manufacturer. These data may possibly have to be converted to $MTTF_D$ values, for example with the aid of the simplifying assumption that only 50% of all failures are dangerous. If manufacturers' data are not available, reference can be made to a number of known databases. The following are cited by way of example in EN ISO 13849-1:

- Siemens Standard SN 29500, Ausfallraten Bauelemente, Erwartungswerte, published by: Siemens AG, Corporate Technology, Technology & Innovation Management, Munich, Germany 2004-2014 (updated at irregular intervals; order from michaela.pabst@siemens.com or thomas.haizmann@siemens.com)
- IEC/TR 62380, Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment. Published by: International Electrotechnical Commission (IEC), Geneva, Switzerland 2004
- Handbook of 217Plus Reliability Prediction Models, Quanterion Solutions Incorporated, Utica, New York, 2015, www.quanterion.com (further development of MIL-HDBK-217F)
- Telcordia SR-332, Reliability Prediction Procedure for Electronic Equipment, Issue 4, March 2016, telecom-info.telcordia.com
- EPRD-2014, Electronic Parts Reliability Data (RAC-STD-6100), Quanterion Solutions Incorporated, Utica, New York, 2015, www.quanterion.com
- NPRD-2016, Nonelectronic Parts Reliability Data (RAC-STD-6200), Quanterion Solutions Incorporated, Utica, New York, 2015, www.quanterion.com
- British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)
- Chinese Military Standard, GJB/z 299B & 299C

In addition to these collections of data, a number of software tools are available on the market that provide automated access to these or other databases. In the majority of databases, electronic components are catalogued by component type and other criteria (e.g. design, material, enclosure). Generally, base failure rates are stated in the first instance for reference conditions (e.g. for a component ambient temperature of 40 °C and nominal load). Where the actual conditions of use differ, these rates can be corrected by means of adjustment factors. Tables C.2 to C.7 of the standard even list values taken from the SN 29500 database for certain typical electronic components. In the third edition of the standard however, the columns present in the previous version, in which a safety margin of 10 (worst case) was implied, have been deleted. Provided the data sources are applied correctly, an additional safety factor is not generally required. Adjustment to stresses outside the reference conditions is not explicitly required by the standard, and should be applied with a sense of proportion in the interests of simplicity.

D.3 Integration of components and equipment that have already been certified

Manufacturers are increasingly stating an $MTTF_D$ for their components on the data sheet. For components intended for use as subsystems in an SRP/CS, the manufacturer states a PL to EN ISO 13849-1 or an SIL to IEC 61508, IEC 62061 or IEC 61800-5-2, combined with statement of an average probability of dangerous failure per hour PFH_D (PFH to IEC 61508). Should such components be employed in one channel of the SRP/CS only, the stated probability of failure per hour (PFH_D) may be considered as a substitute for the rate of dangerous failure (see formula D.6). Internal component characteristics such as redundancy and self-diagnostics are already considered in this case. More detailed information on this aspect can be found in Chapter 2 of SISTEMA Cookbook 4 [9].

$$MTTF_D = \frac{1}{\lambda_D} \approx \frac{1}{PFH_D} \quad \text{(“Black-Box” components with } PFH_D \text{ within one channel)} \qquad \text{(D.6)}$$

D.4 Parts count method

Once the $MTTF_D$ values of all safety-related components are known, the $MTTF_D$ of each block must first be calculated from them. This step can be performed in close detail by an FMEA (failure mode and effects analysis, Annex B); ideally, however, the different failure modes of each safety-related component and their effect upon the block must be analysed for this purpose. In consideration of the effort, this approach is therefore generally worthwhile only for components with a high failure rate, i.e. a low $MTTF_D$ value. An alternative that can be performed quickly and yields values that on average are not appreciably poorer is the parts count method stated in EN ISO 13849, Part 1. Essentially, this method is a summation with two chief assumptions:

- Irrespective of the failure mode of a component and its effects upon the block, all failures are divided into two halves, safe and dangerous. This means that half of the

failure rate λ of a component contributes to the dangerous failure rate λ_D of the associated block. If the proportion of dangerous failures, λ_D, within the failure rate as a whole has already been determined for the component, the same λ_D value is also allowed for the block.

- The dangerous failure rate λ_D of the block is then formed by summation of the λ_D contributions of all N safety-related components present in the block concerned (the contributions of identical components can simply be grouped):

$$\lambda_D = \frac{1}{2}\sum_{i=1}^{N}\lambda_i \quad \text{or} \quad \lambda_D = \sum_{i=1}^{N}\lambda_{Di} \tag{D.7}$$

Since, as described above, the standard assumes constant failure rates, the λ_D failure rates can be converted to $MTTF_D$ values simply by formation of the reciprocal. Based upon this relationship, the $MTTF_D$ value of a block can easily be derived from the $MTTF_D$ values of its components. An example of application of the parts count method can be found in Chapter 6.

D.5 Series arrangement of blocks in a channel and capping of the $MTTF_D$

If $MTTF_D$ values or λ_D failure rates are available for each block, the $MTTF_D$ for each channel can also be calculated in accordance with formula (D.7) by summation of the failure rates of all blocks involved in a channel. It is assumed in this case that the dangerous failure of any block in the chain of blocks constituting a channel is also to be treated as a dangerous failure of the channel. Since under certain circumstances however, downstream blocks are capable of detecting a dangerous failure of upstream blocks, this assumption constitutes an estimation erring on the safe side. The capping rule of the standard takes effect in this phase of determining the $MTTF_D$: with the exception of Category 4, each $MTTF_D$ of a channel that mathematically exceeds 100 years is routinely reduced to the maximum value of 100 years. In Category 4, the cap is 2,500 years. The purpose of this rule is to prevent the component reliabilities from being overstated in comparison with the other dimensions relevant to the PL, such as the architecture, tests and common cause failures.

D.6 Symmetrization of multiple channels

As soon as a control system involves two channels (as is generally the case for Categories 3 and 4) exhibiting different $MTTF_D$ values, the question arises as to which of the $MTTF_D$ values for each channel is to be used for determining the PL with the aid of the bar chart. For this issue, too, EN ISO 13849-1 has the answer in the form of a simple formula:

$$MTTF_D = \frac{2}{3}\left(MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right) \tag{D.8}$$

The average $MTTF_D$ per channel is thus produced from the $MTTF_D$ values of the two redundant channels C1 and C2 by means of an averaging formula (this formula can be derived mathematically by calculation of the $MTTF_D$ value for a two-channel system without diagnostics but with known $MTTF_D$ values of both channels – $MTTF_{DC1}$ and $MTTF_{DC2}$ [5]). This completes the successive grouping of the $MTTF_D$ values of all components involved in the control system. The result is a value for the typical reliability of the components present in the control system, without consideration of the redundancy, diagnostics or CCF (common cause failures, cf. Annex F). Given that the $MTTF_D$ is already capped to 100 years (2,500 years in the case of Category 4) for each channel involved, assignment of the $MTTF_D$ values to one of the three classes, “low”, “medium” or “high”, is expedient only after symmetrization. The symmetrized value is substituted in the numerical calculation of the PL as a parameter in addition to the Category, the average diagnostic coverage and the measures against common cause failure. Depending upon the Category to be attained, a minimum $MTTF_D$ value of three years (for Category B, 2 and 3) or 30 years (for Category 1 and 4) is also required.

References

[1] *Birolini, A.*: Qualität und Zuverlässigkeit technischer Systeme: Theorie, Praxis, Management. 3rd edition. Springer, Berlin, Germany 1991

[2] *Bork, T.; Schaefer, M.*: Aus Aktivität wird Vorsicht – Sinn und Unsinn der Quantifizierung. O + P Ölhydraulik und Pneumatik 51 (2007) No 3, pp. 78-85. www.dguv.de/medien/ifa/de/pub/grl/pdf/2007_016.pdf

[3] *Schuster, U.*: Untersuchung des Alterungsprozesses von hydraulischen Ventilen. BGIA-Report 6/2004. Published by: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin, Germany 2004. www.dguv.de/ifa, Webcode: d6362

[4] *Weibull, W.*: A statistical distribution function of wide applicability. J. Appl. Mech. 18 (1951), pp. 292-297

[5] IEC 60947-4-1: Low-voltage switchgear and control-gear – Part 4-1: Contactors and motor-starters – Electromechanical contactors and motor-starters (2009) + A1 (2012).

[6] DGUV Information 203-079: Auswahl und Anbringung von Verriegelungseinrichtungen. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin, Germany. August 2014 – updated edition December 2015. http://publikationen.dguv.de/dguv/udt_dguv_main.aspx?FDOCUID=26231

[7] Principles of testing and certification for interlocking devices with solenoid guard-locking, Principles of testing GS-ET-19E. Published by: DGUV Test, Prüf- und Zertifizierungsstelle Elektrotechnik, May 2015. www.bgetem.de, Webcode: 12700341

[8] Principles of testing and certification for electro-mechanical enabling switches and enabling devices with and without start-up controllers, Principles of testing GS-ET-22E. Published by: DGUV Test, Prüf- und Zertifizierungsstelle Elektrotechnik, July 2016. www.bgetem.de, Webcode: 12700341

[9] SISTEMA Cookbook 4: When the designated architectures don't match. Published by: Deutsche Gesetzliche Unfallversicherung e.V. (DGUV), Berlin, Germany 2015. www.dguv.de/ifa, Webcode: e109249

[10] *Goble, W. M.*: Control systems safety evaluation and reliability. 3rd ed. Published by: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010, www.isa.org

Annex E:
Determining of the diagnostic coverage (*DC*)

Changes with respect to the second edition (BGIA Report 2/2008e):

- Reference inserted to possible reduction of the *DC* by cascading, e.g. of electromechanical position switches
- Two *DC* measures deleted from Table E.2: redundant shut-off path without monitoring of the actuator, and redundant shut-off path with monitoring of one of the actuators by either logic or the test equipment
- Figure E.3 amended
- Conditions amended for the simplified method in Category 2 (testing upon demand as an alternative to testing 100 times as frequently as demand; test channel at least half as reliable as the functional channel, instead of $MTTF_{D,L} \geq 0.5 \cdot MTTF_{D,TE}$)
- Examples inserted from the standard concerning fault detection in the process

The diagnostic coverage *DC* is a measure of the effectiveness of a control system's self-test and monitoring measures. It may relate to individual components, blocks, or entire subsystems (DC_{avg}). The precise definition of the *DC* is based upon the division of failures into three groups (see Figure E.1):

- Safe (S) failures: these failures automatically result in a safe state being assumed that does not give rise to any hazards (example: a contactor remaining open or a valve remaining closed, resulting in interruption of energy and consequently stopping of potentially hazardous movements).

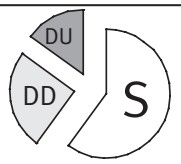
- Dangerous detectable (DD) failures: these potentially dangerous failures are detected by test or monitoring measures and transferred to a safe state (example: failure of a contactor to open or of a valve to close, which is detected by a readback contact or position monitor, and handled safely).

- Dangerous undetectable (DU) failures: these potentially dangerous failures are not detected (example: undetected failure of a contactor to open or of a valve to close, as a result of which a demand for a safe torque off does not result in stopping of a hazardous movement).

On multi-channel systems, the term “dangerous failure” is used with regard to a single channel, although a dangerous system failure need not necessarily yet have occurred. The failures “DD” and “DU” can be combined to form the group of dangerous failures (D). The safe failures may also be detectable or undetectable; the distinction is irrelevant, however, since the safe state is assumed in both cases.

Figure E.1:
Illustration of the diagnostic coverage

$$DC = \frac{\sum \lambda_{DD}}{\sum (\lambda_{DD} + \lambda_{DU})}$$



The diagnostic coverage (*DC*) is determined by the proportion of detectable dangerous failures (DD) among all dangerous failures (D), and is generally stated as a percentage. For calculation of the *DC*, for example in conjunction with an FMEA (failure mode and effects analysis, see Annex B), the ratio is calculated of the totals of the failure rates λ_{DD} and λ_{D} of the unit under consideration. The *DC* is seen here to be a value relating to the tested unit (e.g. the block) and not to the test equipment. In order to simplify calculation of the *DC*, EN ISO 13849-1 offers an alternative solution to the FMEA: it proposes *DC* key values for typical diagnostics measures, the attainment of which may be assumed when the relevant measure is implemented correctly. In this way, evaluation from tables of the diagnostics measures implemented per unit is sufficient. A similar procedure is frequently used by test bodies as standard and economic practice.

Since the proportion of dangerous undetectable failures (i.e. 1 – *DC*) is the relevant value for the probability of failure for evaluation of the implemented test and monitoring measures, selection of the key values (60, 90 and 99%) for formation of the four *DC* quality stages (Table E.1) is self-explanatory.

Table E.1:
The four levels of diagnostic coverage in accordance with the simplified approach of EN ISO 13849-1

DC (level of diagnostic coverage)	
Description	**Range**
None	$DC < 60\%$
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

A fundamental distinction must be drawn between the *DC* of an individual test for a certain component or block, and the average diagnostic coverage DC_{avg} for the entire subsystem under analysis of a safety-related control system (SRP/CS). The formation of groups by means of the key values is applied here both for qualification of the individual tests, and for definition of the DC_{avg}. Since DC_{avg} is one of the input variables for the simplified bar-chart method for quantification of the probability of failure, the calculated DC_{avg} value is rounded down to the next lowest of the four key values (0, 60, 90 and 99%) from Table E.1, and thereby placed in one of the four *DC* classes (None, Low, Medium and High). For example, a DC_{avg} value of 80% is reduced in the simplified approach to a value of 60% (in contrast to the procedure in the IFA SISTEMA software utility, which employs intermediate DC_{avg} values in its default setting; see Annex H). The *DC* of individual tests will first be discussed below, followed by calculation of the DC_{avg}.

Table E.2 shows typical test and monitoring measures for components (usually elements or blocks), and evaluation of their *DC* to EN ISO 13849-1. Different measures are usual for each function (I, L, O, i.e. input, logic, output), Category and technology. Their evaluation may vary as a function of the design or external factors, such as the application in which the control system is operated. In some applications, indirect monitoring by displacement transducers or position switches on the actuators rather than on the control system elements may for example not provide any indication of whether the safety function can still be executed independently by each of two redundant control channels. In general, evaluation as a numerical *DC* value makes no distinction between automatic tests (e.g. program routines that are performed regularly) or deliberate tests (e.g. tests initiated manually by the operator at regular intervals); refer here also to subclause 6.2.14.

Table E.2:
DC key values for typical test and monitoring measures at component and block level, to EN ISO 13849-1

Measure	Primarily relevant for			*DC* (%)	Description of measure
	I	L	O		
Cyclic test stimulus by dynamic change	X			90	Periodic generation of a signal change with monitoring of the results
Plausibility check/readback/ (cross-)monitoring					
• Without dynamic test	X		X	0 to 99	The attained *DC* value depends on how often a signal change is done by the application
• With dynamic test, without high quality fault detection	X		X	90	
• With dynamic test, with high quality fault detection	X		X	99	
Indirect monitoring	X	X	X	90 to 99	The attained *DC* value depends on the application
Direct monitoring	X	X	X	99	
Fault detection by the process	X	X	X	0 to 99[1]	The attained *DC* value depends on the application; this measure alone is not sufficient for the required Performance Level e[2]
Monitoring some characteristics	X			60	

Which unit performs a test is in principle also irrelevant, for example in the case of self-tests. Only where appropriate independence is assured (single-fault tolerance, resistance to common cause failures) between the testing and tested units, however, is a test actually effective. It is also important that the safe state is actually assumed following detection of a dangerous failure. If, for example, contact welding on a main contactor is detected, but no means exist for timely stopping of a hazardous movement, the detection is useless and must be rated with a *DC* of 0%.

With regard to the *DC* measure of "fault detection by the process", the third edition of the standard provides information in the form of examples: "*The DC measure 'fault detection by the process' may only be applied if the safety-related component is involved in the production process, e.g. a standard PLC or standard sensors are used for workpiece processing and as part of one or two redundant functional channels executing the safety function. The appropriate DC level depends on the overlap of the commonly used resources (logic, inputs/outputs etc.). E.g. when all faults of a rotary encoder on a printing machine lead to highly visible interruption of the printing process, the DC for this sensor used to monitor a safely limited speed may be estimated as 90% up to 99%.*" For PL_r = e, this measure is not sufficient on its own (see Table E.2), and produces a red warning message when SISTEMA is used. Where adequately justified however, for example by means of further *DC* measures acting upon the same block, or when the complementary block of the redundant channel implements a different *DC* measure with a *DC* at least as great as the assumed *DC* provided by the process, this measure may still be included in the analysis. In SISTEMA, this can be achieved by direct input of the *DC* with manual selection of the percentage step, accompanied by documentation of the justification.

<table>
<tr><th colspan="5">Typical realisation in different technologies</th></tr>
<tr><th>Mechanics</th><th>Pneumatics</th><th>Hydraulics</th><th>Electrical systems</th><th>(Programmable) electronics</th></tr>
<tr><td colspan="5">See description of measure</td></tr>
<tr><td colspan="5">Manual initiation of the test function</td></tr>
<tr><td colspan="3"></td><td colspan="2">Comparision of inputs or outputs without detection of short circuits</td></tr>
<tr><td colspan="2">Position monitoring of the valving element, value of DC depends on concrete realisation</td><td>Cross monitoring of inputs or outputs with detection of short circuits and static faults, e.g. using safety modules</td><td>Cross monitoring of signals and intermediate results with detection of short circuits and static faults and temporal and logical program sequence monitoring; dynamic cross monitoring of independently attained position of velocity information</td></tr>
<tr><td>Position measuring systems or limit switches at the actuators instead of the control elements</td><td colspan="2">Position measuring systems or limit switches at the actuators instead of the control elements; monitoring of valves by pressure switches</td><td colspan="2">Position measuring systems or limit switches at the actuators instead of the control elements</td></tr>
<tr><td>Position monitoring directly at the control element</td><td colspan="2">Position monitoring directly at the valving element over the whole stroke</td><td>Position monitoring by mechanically linked readback contacts (non-equivalent break contacts)</td><td>Signal monitoring by readback e.g. using optocouplers</td></tr>
<tr><td colspan="5">Failure of the process control, becoming obvious through malfunction, damage of workpiece or parts of the machine, interrupts or delay of the functional process, without producing a hazard immediately</td></tr>
<tr><td colspan="2">Monitoring of response time, range of analogue signals</td><td colspan="3">Monitoring of response time, range of analogue systems (e.g. electrical resistance, capacitance)</td></tr>
</table>

Measure	Primarily relevant for			*DC* (%)	Description of measure
	I	L	O		
Program sequence monitoring					
• Simple temporal		X		60	Time monitoring
• Temporal and logical		X		90	
Start-up self-tests		X	(X)	90	To detect latent faults, *DC* depends on the testing technique
Checking the monitoring device		X		90	Checking the monitoring device reaction capability by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demands it, through an input facility
Dynamic principle		X		99	All components of the logic are required to change the state ON-OFF-ON when the safety function is demanded
Test of memory and CPU					
• Invariable memory: signature of one word (8 bit)		X		90	
• Invariable memory: signature of double word (16 bit)		X		99	
• Variable memory: RAM-test by use of redundant date e.g. flags, markers, constants, timers and cross comparison of these data		X		60	
• Variable memory: check for readability and write ability of used data memory cells		X		60	
• Variable memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. “galpat” or “Abraham”)		X		99	
• Processing unit: self-test by software		X		60 to 90	
• Processing unit: coded processing		X		90 to 99	
Redundant shut-off path					
• With monitoring of the actuators by logic or test equipment			X	99	

[1] For example to be determined by FMEA calculating the ratio of detected dangerous failures to all dangerous failures

[2] PL e normally requires two channels. Therefore as a minimum the complementary block of the redundant channel should implement a different *DC* measure, with a *DC* value at least as high as the assumed *DC* by the process

Typical realisation in different technologies				
Mechanics	**Pneumatics**	**Hydraulics**	**Electrical systems**	**(Programmable) electronics**
	not relevant			Timer as watchdog, where trigger points are within the program of the logic
	not relevant			By the watchdog, where the test equipment does plausability checks of the behaviour of the logic
			Detection of e.g. welded contacts by triggering and readback	Detection of latent faults in program- and data memories, input/output ports, interfaces
				Checking the watchdog reaction capability
	Interlocking circuits implemented by pneumatics		Interlocking circuits implemented by relays	
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure
	not relevant			see description of measure

The following requirement applies, in addition to the test and monitoring measures stated in Table E.2: should a *DC* of "medium" or "high" be required for the logic, at least one measure with at least 60% must be selected in each case for variant memory, invariant memory and processing unit. Measures other than those stated in Table E.2 may also be employed.

Further information on determining the *DC* for typical test measures can be found for example in Tables A.2 to A.14 of IEC 61508-2 [1]. These tables contain the key values of 60, 90 and 99% as the maximum *DC* to be attained by the relevant measure. With suitable unrestricted implementation of the measures stated, this maximum value can however generally be employed for estimation. Annex E of EN ISO 13849-2 [2] describes a comprehensive example of validation of the failure behaviour and the diagnostic measures on an automatic assembly machine.

Following determining of the *DC* for individual test measures and prior to calculation of the DC_{avg}, the *DC* value per block must be determined. An individual test measure generally acts upon an entire block (e.g. cross monitoring): the discrete value can then simply be adopted for the block. Further permutations exist, however:

- If a block is monitored by a number of individual measures (see Figure E.2), the block *DC* is at least as good as the best individual *DC*. Should the measures mutually complement each other, a higher block *DC* may even be possible; this *DC* however must then be determined by analysis of the failures covered by each test, similar to an FMEA.

- A block consists of several units, each of which is tested by different measures, for example programmable electronics with separate tests for the memory and the processing unit (see Figure E.3). The block *DC* is then at least as good as the poorest individual *DC*. (Whether the occurrence of units without testing is permissible must be determined with reference to the relevant Category definition, see subclauses 6.2.5 to 6.2.7; the *DC* for the logic is subject to further requirements, see above.) A better and more precise value for the block *DC* can be attained by weighting the individual *DC* value with the associated failure rate λ_D (= $1/MTTF_D$). Formula (E.1) can also be used for this purpose as an averaging formula at block level. Depending upon the accuracy, such an analysis also ultimately leads to an FMEA, however.

- Where components are cascaded, such as electromechanical position switches connected to a safety module by a common conductor, it may lead to a reduction in the *DC*. An electrically two-channel arrangement enables certain faults of a position switch to be detected by the safety module from logically implausible signals from the two electrical contacts. Starting of the machine for example is prevented following closing of the door on which the switch is defective. If, in addition to the door on which the position switch has failed dangerously, a further door is opened, fault detection is (depending upon the sequence) not possible. Cascading thus leads to a reduction in the *DC*; this is dependent upon factors including the number of guard doors and the frequency with which they are opened. Details of such constellations and of estimation of the *DC* for them can be found in ISO/TR 24119 [3]. Subclause 6.1 of this standard excludes PL e for cascading. If, as shown in Example 28 (see subclause 8.2.28), an additional contact is employed for fault detection for each position switch, fault detection is also not restricted for cascading, and PL e is attainable.

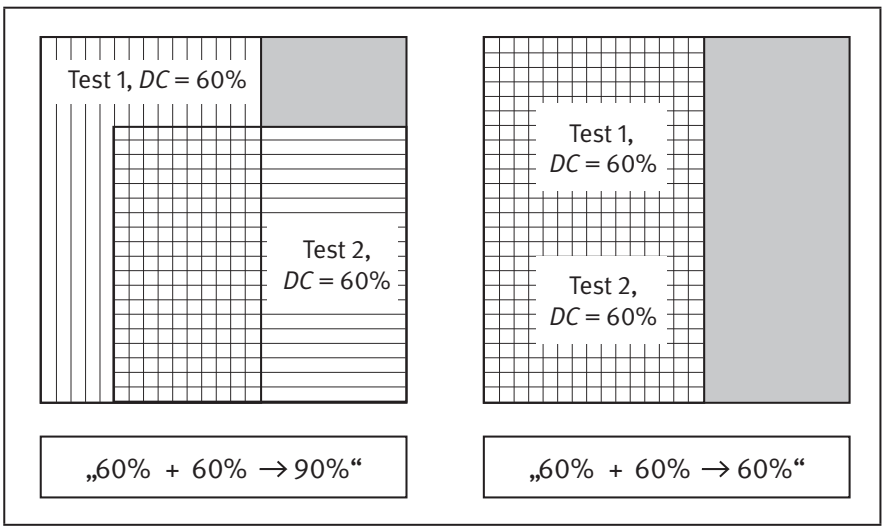


Figure E.2:
Where several tests act upon the same block, their overlap may lead to a higher overall *DC* (left), or it may not (right); the hatched areas represent the proportion of the detected dangerous failures; the square overall area represents all dangerous failures (100%)

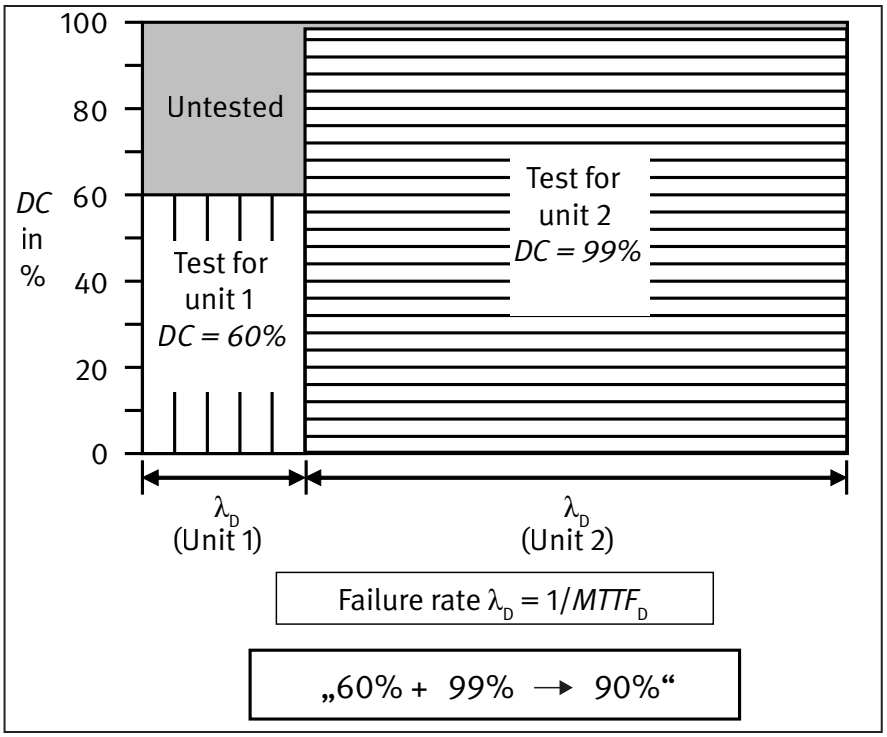


Figure E.3:
Where the *DC* is averaged for several units of one block, weighting of the individual *DC* values of 60% and 99% with λ_D leads to a different value (90%) than for example the unweighted arithmetic mean (79.5%)

The average *DC* for an SRP/CS (at subsystem level) is termed DC_{avg} and is calculated from the *DC* values for all blocks in functional channels. In contrast to the $MTTF_D$ per channel, no distinction is drawn between the control channels; rather, an overall value is determined directly. The averaging formula weights the individual *DC* values with the associated failure rate λ_D (= $1/MTTF_D$) of each block. This ensures that blocks with a high failure rate, i.e. a low $MTTF_D$, are given greater consideration than blocks the dangerous failure of which is comparatively unlikely. The averaging formula is as follows:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}} \qquad \text{(E.1)}$$

The summation extends over all relevant blocks with the following provision:

- For blocks with no *DC*, a *DC* of 0% is substituted. These blocks thus contribute only to the denominator of the fraction. Whether the absence of diagnostics for blocks is consistent with the requirements of the Category concerned must be determined on a case-by-case basis. Category 2 imposes the generic requirement of “check of the safety function(s)”, Category 3 fault detection “whenever reasonably practicable”, Category 4 also requires detection of an individual fault and only “if this detection is not possible” that the safety function is also to be performed in the event of an accumulation of undetected faults.
- For blocks with fault exclusion for the dangerous failure mode (an imperceptibly low failure rate λ_D or infinitely high $MTTF_D$), the corresponding value is omitted from the numerator and the denominator.
- All blocks that execute safety functions in the various functional channels are considered. Blocks that have the function of testing only are not considered. For Category 2 structures, this means that blocks of the test channel (“TE” and “OTE”) are not counted. In Category 3 and 4, the average value is formed directly across both channels; symmetrization is not performed separately per channel as it is for the $MTTF_D$.

For a detailed analysis of the influence of the tests upon the probability of failure of the overall system, further variables must be considered in addition to the *DC*. These include, in addition to the test rate, the failure rate of the test equipment itself, for example. In multi-channel systems however, the frequency of a test is of lesser consequence, since the relevant intervals are generally considerably smaller than the $MTTF_D$ values of the channels. Consequently, several channels must fail before the impairment of a test becomes relevant to the system, which is very unlikely as long as the test cycles continue to be much smaller than the $MTTF_D$ of a channel. Subclause 6.2.14 provides more comprehensive explanations concerning the required test rate. In Category 2 structures however, failure of the test equipment turns a single-channel tested system into a single-channel untested system. The next dangerous failure in the functional channel can then no longer be detected and leads directly to performance of the safety function no longer being possible. In addition to requirements for the *DC*, further

conditions therefore apply for the simplified assessment of the probability of failure of Category 2 systems:

- All test rates must be at least 100 times (in exceptional cases, at least 25 times) greater than the demand rate upon the safety function; alternatively, in the event of testing immediately upon demand of the safety function, testing should be performed so quickly that the safe state is reached before a hazard arises. This is to ensure that a failure can be detected by a test before a demand of the safety function cannot be met (see also Annex G).

- The $MTTF_D$ of the test channel (TE and OTE) must be at least half as high as the $MTTF_D$ of the functional channel (I, L and O). This assumption ensures that the probability of failure of the test channel is not unacceptably high. Should this condition be violated (even after capping of the $MTTF_D$ of the functional channel to 100 years), it is of course permissible to calculate the probability of failure using an $MTTF_D$ of the functional channel that is reduced mathematically to double the $MTTF_D$ of the implemented test channel.

References

[1] IEC 61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (2010)

[2] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2012)

[3] ISO/TR 24119: Safety of machinery – Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts (11/15)

Annex F:
Common cause failure (CCF)

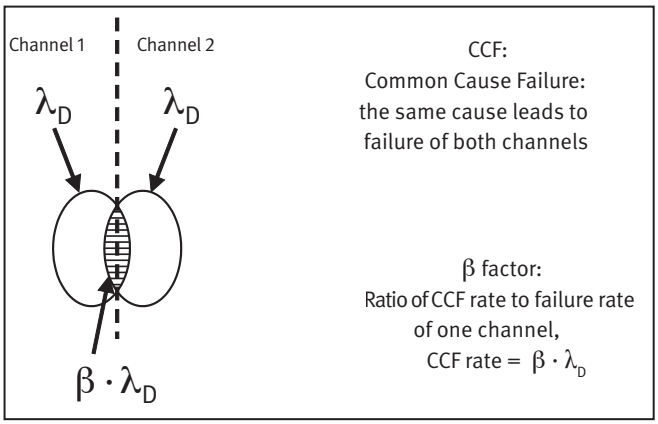
Changes with respect to the second edition (BGIA Report 2/2008e):

Text of the descriptions of the measures brought into line with the third edition of the standard

The term common cause failure (CCF) describes the fact that in a redundant system or a single-channel system with separate test channel, several channels may be disabled by one and the same cause. The desired single-fault tolerance of a redundant structure is thus negated. It is therefore important that this source of faults be eliminated as far as possible. The triggers of CCFs may be physical in nature, such as overtemperature or strong electromagnetic interference, or systematic, such as defective circuit design or programming errors where identical software is employed for both channels.

A common strategy for quantification of a control system's susceptibility to CCF is the beta-factor model. This strategy assumes that a certain proportion of the dangerous failures in one channel share the same cause as dangerous failures in the second channel. This concept is illustrated in Figure F.1: the dangerous failure rates for the two channels (shown symbolically as elliptical areas) have a CCF overlap, which is shown by the hatching. The proportionality factor between the CCF rate and the dangerous failure rate of the single channel λ_D is normally termed β (common cause factor or beta factor).

Figure F.1:
Illustration of common cause failure (CCF) by means of the beta-factor model



It is virtually impossible to calculate the beta factor precisely for a specific control system, particularly since this should be done at the beginning of the actual design process. IEC 61508-6 [1] employs a points system for this purpose by which β values of between 0.5 and 10% can be determined. Points are assigned in a long list of measures sorted according to different causes; when certain rules are applied, the sum of these points results in an estimated β value. EN ISO 13849-1 takes up this method, both in simplified form and with adaptation to machine safety. Simplification is based upon technical measures that experts have considered particularly useful for the avoidance of CCF. This is, however, a compromise that can be justified empirically, but not scientifically:

- The list of measures against CCF was focused upon the relevant solutions, primarily technical in nature, in machine safety.
- A single target value with a maximum of 2% was selected instead of several possible β values. The target value can only be either attained or not attained. The simplified method to EN ISO 13849-1 for determining the Performance Level is based upon an assumed beta factor of 2%.
- The mathematical rules for the points system were summarized in two steps: each measure can only be either satisfied completely (full number of points) or not satisfied (zero points); no provision is made for proportional numbers of points for measures that are not completely satisfied. If measures (such as diversity, use of well-tried components) are satisfied completely only in individual SRP/CS in the form of subsystems, different packages of measures may act against CCF at subsystem level. The minimum number of 65 points must be reached for the Categories 2, 3 and 4 in order for use of the simplified method for determining the Performance level to be permissible. A maximum of 100 points can be reached.

The following points must be observed during evaluation of the measures:

- The measures must be evaluated with particular consideration for their effectiveness against CCF. For example, the product standards already require immunity to environmental influences and electromagnetic interference. Supplementary evaluation must be performed of whether these influences have been effectively minimized as sources of common cause failures.
- The physical counter-measures differ according to the control technology employed: of the environmental influences, for example, electromagnetic interference is more relevant in the case of electrical control systems,

whereas contamination of the fluid is more relevant in the case of fluid control systems. Counter-measures must therefore be evaluated with consideration for the technology employed.

- The tested structure of Category 2 systems constitutes a special case. In this case, CCF concerns common failure of both the functional channel and the test channel. A common cause failure results in the structural benefit being negated. The evaluation of the measures must be adjusted accordingly to the particular aspects of the Category 2 structure.

- The full number of points may be credited for a measure against common cause failures that cannot occur owing to the inherent characteristics of the control system.

The measures against common cause failures and the associated numbers of points from EN ISO 13849-1 are as follows:

- Separation/segregation (15 points): physical separation between the signal paths, e.g.:

  – Separation in wiring/piping

  – Detection of short-circuits and open circuits by dynamic testing

  – Separate shielding for the signal path of each channel

  – Sufficient clearances and creepage distances on printed-circuit boards

- Diversity (20 points): different technologies/design or physical principles are used. Examples include:

  – One channel electronic or programmable electronic, the other electromechanical hard-wired

  – Different initiation of the safety function for each channel, for example by means of position, pressure or temperature

  – Digital and analogue measurement of variables (e.g. distance, pressure or temperature)

  – Sourcing of components from different manufacturers

- Design/application/experience: protection against overvoltage, overpressure, overcurrent, overtemperature, etc. (15 points) and the use of well-tried components (5 points)

- Assessment/analysis (5 points): a failure mode and effects analysis has been performed for each part of the SRP/CS, and its results taken into account during design for the avoidance of CCF

- Competence/training (5 points): training of designers in understanding the causes and consequences of CCF

- Environmental conditions concerning protection against adverse influences upon electrical/electronic and fluid power systems (25 points):

  – Electrical/electronic systems: prevention of contamination and electromagnetic disturbances (EMC) in accordance with appropriate standards

  – Fluid power systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, for example in compliance with the component manufacturer's requirements for purity of the pressure medium

On combined fluid power and electrical systems, both aspects should be considered.

- Environmental conditions with regard to other influences (10 points): consideration of the requirements for immunity to all relevant environmental conditions, such as temperature, shock, vibration, humidity (for example as specified in the relevant standards)

Reference

[1] IEC 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (2010)

Annex G:
What is the significance of the bar chart in Figure 5 of EN ISO 13849-1?

Changes with respect to the second edition (BGIA Report 2/2008e):

- Reference to Note 1 in Annex K of the new standard
- Explanations from subclause 4.5.4 of the standard of the time aspects during testing brought into line with the new standard
- Explanations inserted concerning extension of the mission time beyond 20 years
- "Reference" subclause updated
- Sequence of the images brought into line with the text

Unlike its predecessor, EN 954-1 [1], EN ISO 13849-1 makes provision for demonstration of a Performance Level (PL) in addition to examination of the Category. The Performance Level is determined numerically, as shown in Table 6.1 of this report, from the average probability of a dangerous failure per hour (PFH_D) of the system (cf. Footnote 4 in Chapter 3, Page 15). This value must be determined from the system structure, the failure rates of the components, the level of diagnostic coverage provided by automatic testing, the mission time of the system, and in the case of relevant system structures, the sensitivity of the system to CCF (common cause failure).

Mathematical models are employed for this purpose that take account of the combined effect of the stated factors and return the result in the form of the PFH_D (as an average value over the mission time). In theory, a custom model should be created for each system under analysis when the standard is applied. For some common structural variants, the "designated architectures" of EN ISO 13849-1, subclause 6.2, (cf. subclauses 6.2.1 to 6.2.7 of this report), *Markov* models have been developed at the IFA the numerical results of which are compiled in the form of a bar chart in subclause 4.5.4, Figure 5 of the standard (Figures 6.10 and G.1 of this report). This dispenses with the need for development of a dedicated mathematical model and for complex calculations, provided the system essentially shares the form of one of the designated architectures, or can be broken down into system parts that do so (cf. in this context subclause 6.3 and Annex H of EN ISO 13849-1, or subclause 6.4 of this report). A basic introduction to the *Markov* modelling technique can be found for example in [2].

For a comprehensible diagram to be obtained, certain restrictions and simplifications are necessary. Firstly, the standard limits the number of designated architectures and therefore also the number of necessary models. Secondly, the large number of input parameters has been reduced by intelligent grouping. For this purpose, the values $MTTF_D$ and DC_{avg} were introduced, each of which groups several input parameters.

The $MTTF_D$ used in the diagram represents a mean time to failure of each channel in its dangerous failure mode. The $MTTF_D$ values of several function blocks are grouped here to form a single channel $MTTF_D$ (Chapter 6 and Annex D). All $MTTF_D$ values are based upon the assumption of constant component failure rates λ_D, hence $MTTF_D = 1/\lambda_D$. In a two-channel structure with different $MTTF_D$ values between channels, an averaged substitute $MTTF_D$ value is employed. Conversely, the DC_{avg} represents the weighted average value of the diagnostic coverage for the entire system; this value is used for assignment to one of the four DC_{avg} levels (see Table 6.4).

The meaningfulness and permissibility of this grouping within the required quantification accuracy have been demonstrated by comprehensive test calculations. The same applies to the relationship, permitted in subclause 4.5.4 of the standard, between the $MTTF_D$ values of the test and functional channels in the Category 2 architecture: the $MTTF_D$ of the test channel must be at least half the $MTTF_D$ of the functional channel. Finally, a requirement is imposed for redundant structures that common cause failures be reduced to an appropriate level: no more than 2% of the dangerous failures may have a common cause. This must be demonstrated in each case during application of the standard by means of a simple estimation method (Annex F).

The *Markov* models upon which the bar chart in EN ISO 13849-1 (and Figure G.1 of this report) is based take account of operation of the systems under underlying conditions that are realistic for machinery. They assume that the systems:

- Are subject to at least to one demand of the safety function per year
- Assume the safe "Operating inhibition" state in response to automatic detection of an internal fault, and are then generally switched off manually shortly afterwards (and at the latest after a few hours)

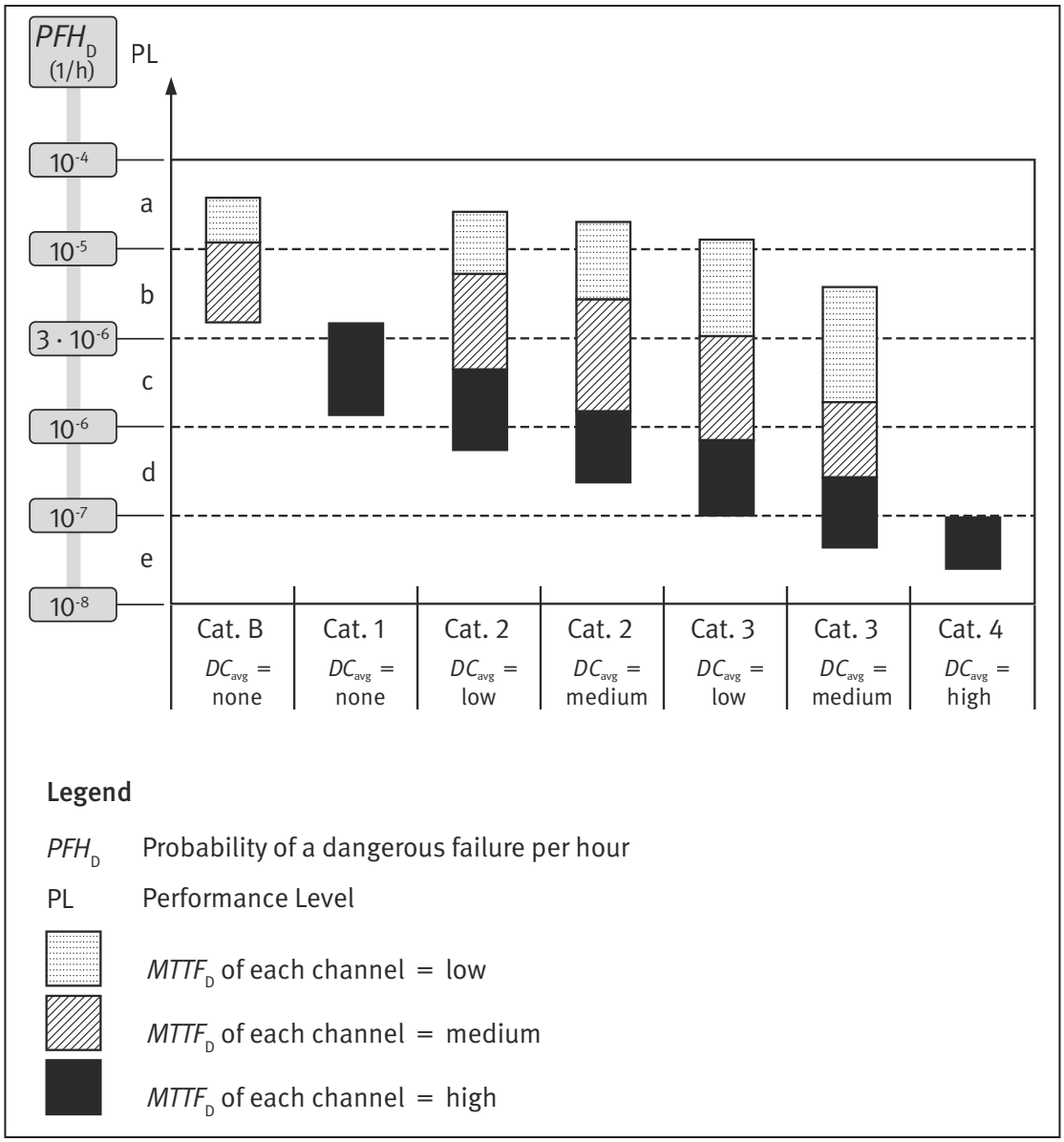


Figure G.1: PFH_D and Performance Level as a function of the Category, DC_{avg} and $MTTF_D$

- Are repaired or replaced and restored to service following assumption of the operating inhibition state, an accident or detected dangerous failure

Under these underlying conditions, the quantitative target value for modelling, the PFH_D, represents the average number per hour of demands upon the safety function that are not met owing to failure. Where demands are made continually upon the safety function (continuous mode of operation), it indicates the number of dangerous system failures per hour. For Category 2, a requirement is that testing is fully effective. This can be attained by an adequate relationship between the test and demand rate or by an adequately fast response to a fault (cf. subclause 6.2.14). Since the PFH_D determined in this way considers only random failures and not systematic failures and other negative effects, it must be regarded as a theoretical performance value that denotes the safety quality of a design but does not permit conclusions for example regarding the frequency of accidents. This PFH_D is the mathematical quantity indicated on the vertical axis of the bar chart (cf. Figure G.1).

Despite consideration being given in principle to demands upon the safety function and to repair, the absolute values for the demand rate and the repair rate (the reciprocal of the repair time) have only a negligibly small influence upon the PFH_D in this sense. Only for the designated architecture for Category 2 must testing at a frequency substantially higher than that of the demand of the safety function be made a requirement (alternatively: testing takes place immediately upon demand and the times for fault detection and safe response are together shorter than the specified system response time; cf. EN ISO 13849-1, subclause 4.5.4). The standard proposes a test rate that is at least 100 times that of the demand rate. Even down to a ratio of 25 : 1, however, the PFH_D increases only by approximately 10%, which can be allowed for by a correction factor of 1.1 (cf. Note 1 in Annex K of the standard). This ratio in the rates avoids an unacceptably high impairment of diagnostics caused

by insufficiently frequent performance of the test. For the Categories B, 1, 3 and 4, the influence of the demand rate upon the PFH_D is negligibly low. The PFH_D values determined from the diagram for the Categories B, 1, 3 and 4 therefore apply to any demand rates and any (mean) repair times. For values of less than one demand per year, the bar chart provides an estimation erring on the safe side. For Categories 3 and 4, the PFH_D values are valid for adequately high test frequencies (see explanations in subclause 6.2.14).

Should the mission time of an SRP/CS exceed 20 years, the PFH_D values determined by means of the simplified method (Annex K of the standard) are generally no longer valid. Under certain circumstances, this situation can however be addressed within the simplified procedure with a few improvements. Two possible scenarios exist:

- In the first scenario, the SRP/CS is specified from the outset for a mission time exceeding 20 years. The influence of the longer mission time can then be estimated erring on the safe side from the *Markov* models upon which Annex K of the standard is based, as follows: for every five years' extension of the mission time beyond 20 years, a further 15% is added to the PFH_D for Categories 2, 3 and 4 (Categories B and 1 require no adjustment of the PFH_D). The simplified method and SISTEMA can therefore still be used. This is conditional upon constant failure rates, irrespective of the mission time. For parts subject to wear, this means that the parts must be designed for the specified longer mission time T_M ($T_{10D} \geq T_M$), or each part must be replaced preventively upon expiration of T_{10D}.

- In the second case, the SRP/CS was originally designed for a mission time of 20 years, but is now to be used beyond this duration. The deterioration in the PFH_D anticipated from the *Markov* modelling can then be estimated as described in the first case with addition of an allowance. The situation is critical where the SRP/CS contains wearing parts or components that deteriorate over age; these typically include “chemical” components (e.g. “wet” electrolytic capacitors, batteries, electrochemical sensors), mechanical components (such as brakes, clutches), electromechanical components (such as switches, relays, contactors), fluid power components (such as valves), and certain optical components (such as optocouplers). In this case, the user of the machine (operating party) is generally unable to assess whether all its components are also designed for an extended mission time, or what measures, such as preventive replacement of individual parts, proof testing, etc., must be performed. Extension of the mission time – with addition of the allowance stated above to the PFH_D – is possible only when manufacturer's information is available on the measures to be taken when the mission time is extended, and only conditional upon these measures being implemented by the user (operating party).

The columns for Category B and 1 in Figure G.1 were calculated by means of a model that considers the demand of the safety function, and the repair. The PFH_D values for these Categories can however be approximated very well by the simple relationship $PFH_D \approx \lambda_D = 1/MTTF_D$. This means simply that the PFH_D of the single-channel untested system ($DC_{avg} = 0$) corresponds practically to its dangerous failure rate.

For the other Categories, however, a more complex method of calculation is required. The essential modelling method is explained below with reference to the example of the "designated architecture" for Category 2. This structure is shown again in Figure G.2.

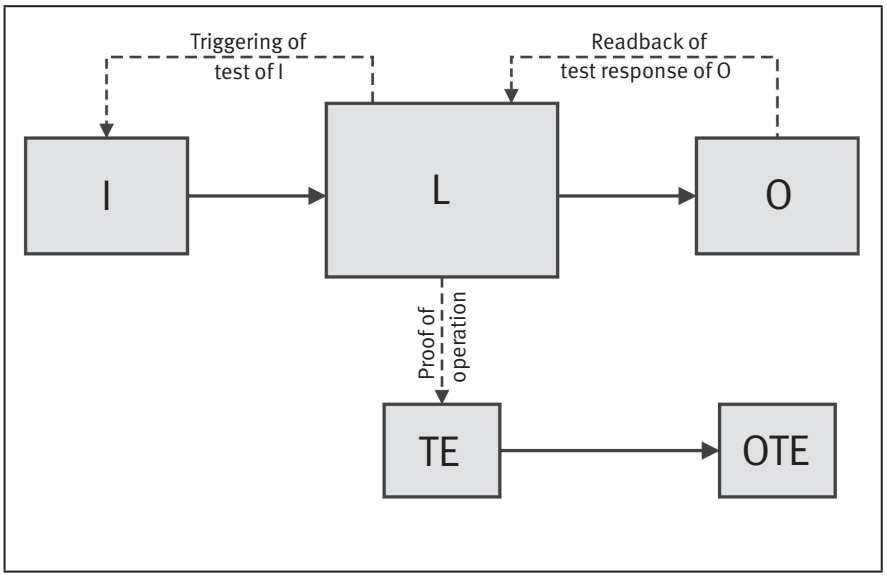


Figure G.2:
Designated architecture for Category 2 to EN ISO 13849-1, subclause 6.2.5

Five function blocks are present, of which the blocks I (input), L (logic) and O (output) execute the safety function proper in a logical series arrangement. Block L tests blocks I, O and itself in conjunction with the function block TE (test equipment). The function block OTE (output of TE) is capable of initiating a safe state in the event of failure of the main I-L-O channel. The additional function blocks TE and OTE, which are not directly essential to the function, thus constitute a form of substitute channel for the fault case. Unlike a "true" second channel, this substitute channel becomes active only when faults are detected in the main channel.

The state graph in Figure G.3 can be derived from the safety-related block diagram in Figure G.2. To this end, all $2^5 = 32$ failure combinations of the five function blocks are first formed. The state without failure is the OK state shown above. It is followed by a series of states in which only one function block has failed, then by a series in which two blocks have failed, and so on. The denotation of the states consists of the names of each failed function block followed by "D", indicating that the block concerned has failed dangerously (i.e. unfavourably in safety terms). Failures of function blocks cause consequential states to be reached, indicated here by arrows. States in which the system is no longer capable of performing the safety function are shown in grey. In cases where the failure can be detected and a safe response is therefore possible, a transition exists to the "Operating inhibition" state shown on the left-hand side. Of the 32 failure combinations, those in which the system has failed dangerously and undetectably (to itself) are grouped together for simplification of the model. This collective state, denoted "System DU" (dangerous undetectable), is shown on the right. It can be attained from several states as a consequence of the failure of function blocks. The "Hazardous situation/harm" state can be seen at the bottom of Figure G.3. This state is attained if and only if a demand is made upon the safety function from within dangerous previous states (shown in grey). Like the "Operating inhibition" state, this state is also transitioned to the OK state by repair. Further transition arrows, for example from "OK" to "System DU", are the result of simultaneous, common cause failure (CCF) of multiple function blocks. It is assumed in 2% of the dangerous failures of either of the function blocks L and TE, the other of the two blocks fails dangerously for the same reason. The same is assumed for the function blocks O and OTE.

All arrows are assigned to transition rates the dimension of which is determined by the transition processes concerned (failures, tests, demands, repairs). Consideration of common cause failures (CCFs) at different points also results in a change in the original transition rate. For the purpose of calculation of the bar chart, the worse case is assumed in which the test equipment employed in the system is itself not tested. For this reason, a rate of zero is assigned to some transitions in Figure G.3.

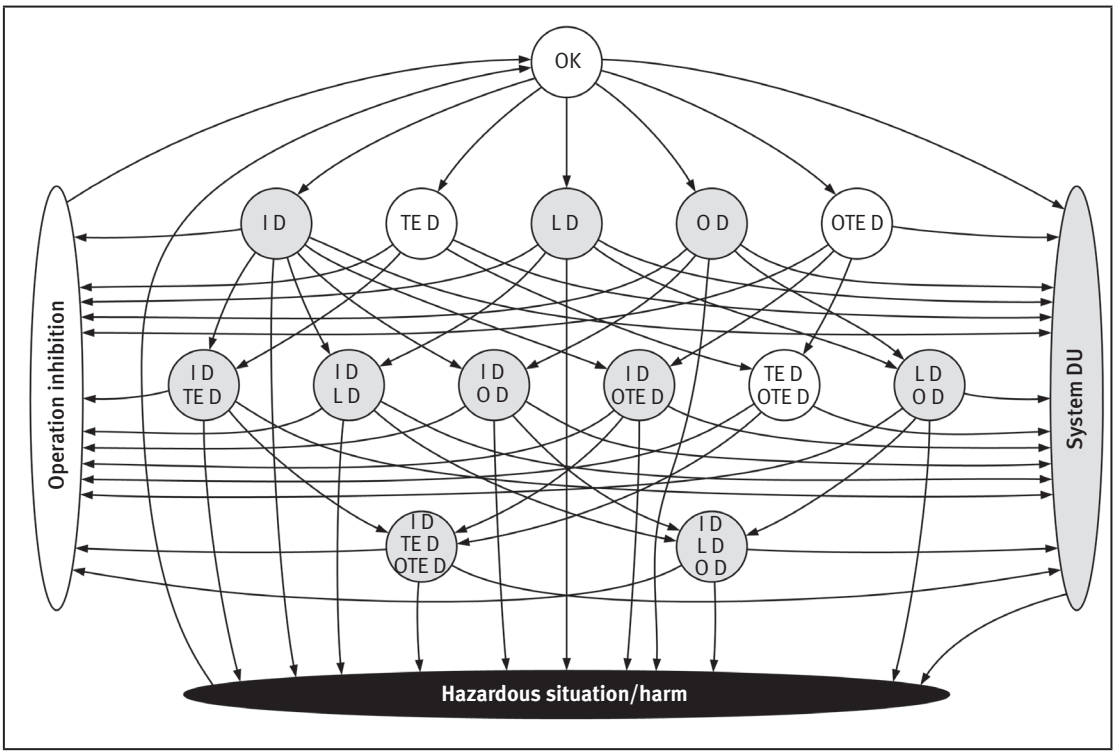


Figure G.3: State graph of the *Markov* model for the Category 2 designated architecture for determining of the PFH_D

Systems that do test their test equipment are therefore estimated erring on the safe side. For the purpose of simplified calculation by means of the *Markov* method, it is assumed that all transition processes are characterized by state residence periods that are distributed exponentially, even though this holds true, strictly speaking, only for the constant-rate random failures. Separate considerations justify this simplification.

It is assumed that at the beginning of the mission time, the probability of the system being in the OK state is 1 and the probability of all other possible system states is 0. During the assumed mission time of 20 years, all state probabilities gradually change: beginning at the OK state, they are redistributed along the transition arrows. The sum of the state probabilities remains constant at 1. This also results in a migration over time to the "Hazardous situation/Harm" state, of which the average value with respect to time over the 20-year mission time is represented by the PFH_D, i.e. the average probability of a dangerous failure of the system per hour.

This PFH_D value is shown on the vertical axis of the bar chart for the different "designated architectures" in accordance with subclause 6.2 of the standard (cf. subclauses 6.2.3 to 6.2.7 of this report); Categories 2 and 3 are subdivided further according to the average diagnostic coverage (DC_{avg}). The columns are created by variation of the $MTTF_D$, i.e. the mean time to dangerous failure of the (or a) functional channel, for a combination of the architecture (or the associated *Markov* model) and the DC_{avg}. The *Markov* model in Figure G.3 can for example be used to calculate the two columns for the designated Category 2 architecture. (For mathematical reasons, an equivalent substitute model differing from this model was used in practice. This model is not presented here, since its relationship to the block diagram in Figure G.2 is less transparent. The substitute model delivers virtually identical results.) The other columns are based upon further *Markov* models that were also developed in accordance with the principles described above for the corresponding designated architectures.

The PFH_D intervals were assigned the Performance Levels a to e on the logarithmic PFH_D scale in accordance with Table 6.1. This is shown in Figure G.1, in which an additional PFH_D scale has been added to Figure 5 of EN ISO 13849-1.

The PFH_D interval from 10^{-6} per hour to 10^{-5} per hour has a particular peculiarity: it is mapped to the two adjacent Performance Levels b and c. Division of the logarithmic scale in the middle places the boundary between Performance Levels b and c at the geometric mean of 10^{-6} per hour and 10^{-5} per hour, specifically at $\sqrt{10} \cdot 10^{-6}$ per hour $\approx 3 \cdot 10^{-6}$ per hour. The assignment of PFH_D intervals and Performance Levels is largely consistent with IEC 61508-1, Table 3, and IEC 61508-5, Figure E.2 (see [3; 4]).

Annex K of the standard contains the content of Figure G.1 in numerical form in Table K.1. Table K.1 can be used to determine the Performance Level more precisely than is possible by means of the figure; this is particularly useful when the PFH_D contributions of several cascaded subsystems require summation. Conversely, the bar chart provides, above all, a swift overview of the suitability of various technical solutions for the PL, and can therefore be used to make a preliminary selection. The information in Table K.1 of the standard is also contained in the "Performance Level Calculator" (PLC), a convenient card disc available from the IFA that can be used to determine the PL [5].

Occasionally, the DC_{avg} value determined for a system may lie only marginally below one of the thresholds "low" (60%), "medium" (90%) or "high" (99%). If the simplified quantification method in EN ISO 13849-1 is then applied, purely formal constraints require that the next-lower DC_{avg} level, i.e. "none", "low" or "medium", be used. This procedure constitutes an estimation of the system erring on the safe side. Owing to the small number of graduations on the DC_{avg} scale, however, a minor change to the system that has the effect of causing the DC_{avg} value to dip just below one of the thresholds may result in a substantially poorer assessment of the system. This can even occur when components with high-quality testing (a high *DC*) in a channel are replaced by superior components (with a higher $MTTF_D$) (cf. the DC_{avg} formula for example in subclause 6.2.14). The minor improvement in the channel $MTTF_D$ is then over-compensated for by the formal downgrading of the DC_{avg} to the next lower level, as a result of which a poorer (i.e. greater) PFH_D value is determined. This effect, which appears paradoxical, is a consequence of the coarse division of the DC_{avg} scale, i.e. ultimately of the simplicity of Figure 5 (Table K.1) of the standard (cf. Figure G.1 of this report).

This effect can be prevented or ameliorated by use of a graph with a finer scale for the DC_{avg} values (Figure G.4) in place of Figure G.1. In consideration of the limited accuracy of DC_{avg} values (cf. EN ISO 13849-1, Table 6, Note 2), the minimum possible DC_{avg} values were also considered for all Categories. The IFA "SISTEMA" software utility (see Annex H) can be used to determine the PFH_D. SISTEMA even interpolates between the columns shown in Figure G.4. Generally, a major downgrading of the DC_{avg} can thereby be avoided, and a PFH_D value often obtained that is both more precise and superior.

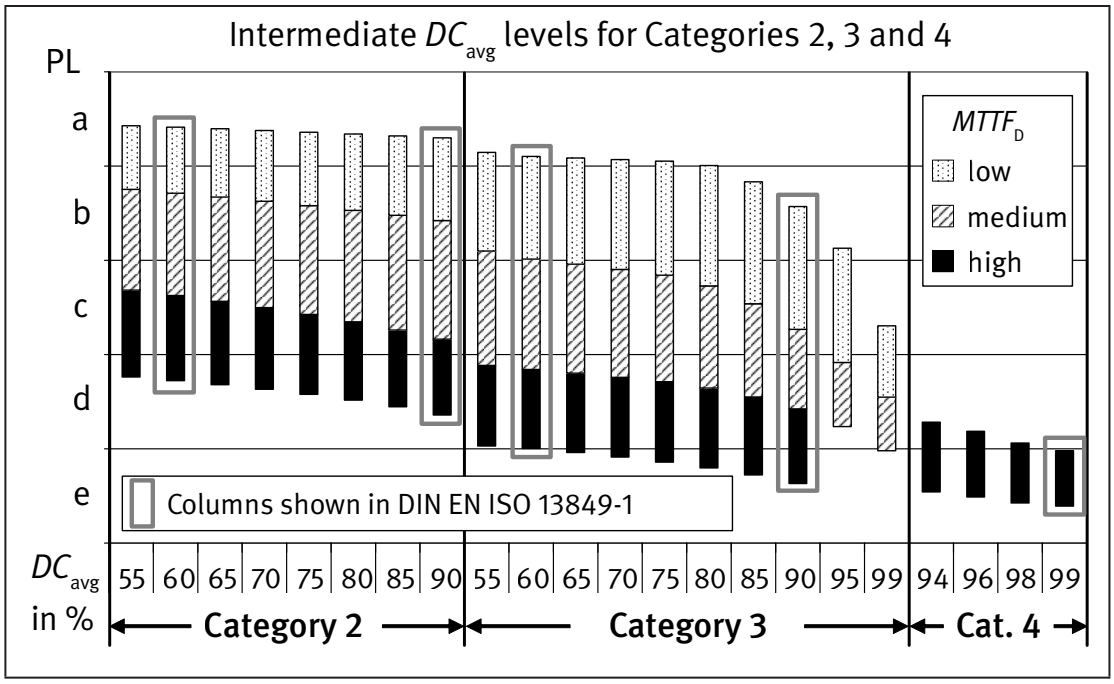


Figure G.4: Performance Level with finer resolution of the DC_{avg} scale (extended modification of Figure 5 from EN ISO 13849-1)

References

[1] EN 954-1: Safety-related parts of control systems. Part 1: General principles for design (12.96)

[2] *Goble, W. M.*: Control systems safety evaluation and reliability. 3rd ed. Published by: The International Society of Automation (ISA), Research Triangle Park, North Carolina 2010

[3] IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (2010)

[4] IEC 61508-5: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (2010)

[5] *Schaefer, M.; Hauke, M.*: Performance Level Calculator – PLC. 5th edition. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin; Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V. – Fachverband Automation, Frankfurt am Main, and Verband Deutscher Maschinen- und Anlagenbau e. V. – VDMA, Frankfurt am Main, Germany 2015. www.dguv.de/ifa, Webcode: e20892

Annex H:
SISTEMA: the software utility for evaluation of SRP/CS

H.1 What is SISTEMA capable of?

The SISTEMA software utility (SISTEMA is the German acronym for safety of control systems on machines) provides developers and testers of safety-related machine controls with comprehensive support in the evaluation of safety in the context of EN ISO 13849-1. The tool, which runs on Windows, enables the structure of the SRP/CS to be modelled based upon "designated architectures", and ultimately permits automated calculation of the reliability values at various levels of detail, including that of the attained Performance Level (PL) and the probability of failure (PFH_D).

Relevant parameters, such as the risk parameters for determining the required PÜerformance Level (PL_r), the Category of the SRP/CS, the measures against common cause failure (CCF) on multi-channel systems, the mean time to dangerous failure ($MTTF_D$) and the diagnostic coverage (DC) of components and blocks, are entered step by step in input dialogs. Once the required data have been entered into SISTEMA, the results are calculated and displayed virtually instantly: each parameter change is reflected immediately on the user interface with its impact upon the entire system. Users are for the most part spared time-consuming consultation of tables and calculation using formulae (calculation of the $MTTF_D$ by means of the parts count method, symmetrization of the $MTTF_D$ for each channel, estimation of the DC_{avg}, calculation of the PFH_D and PL, etc.), since these tasks are performed by the software. This enables parameter values to be varied and effects of the changes assessed with little effort. The final results are summarized in a report, which can be printed out.

H.2 How is SISTEMA used?

SISTEMA processes basic elements from a total of six hierarchical levels: the project (PR), the safety function (SF), the subsystem (SB), the channel (CH)/test channel (TE), the block (BL) and the element (EL). The relationship between them is shown briefly below (Figure H.1).

The user first opens a project, in which the machine or hazard zone that is to be analysed in greater detail can be defined. Safety functions are then assigned to the project. The safety functions can be defined and documented, and a PL_r assigned to them. The PL actually attained by the parameterized SRP/CS is determined automatically from the subsystems which – in a series arrangement – execute the safety function. Each subsystem is based upon a "designated architecture" from the standard, as a function of the selected Category. The architecture determines, among other things, whether the control system is of single-channel, single-channel tested or redundant design, and whether a special test channel must be considered during evaluation. Each channel can be subdivided in turn into any desired number of blocks, for which either an $MTTF_D$ value and a DC value are entered directly, or – on the lowest level in the hierarchy – the values for the individual elements of which the block is composed.

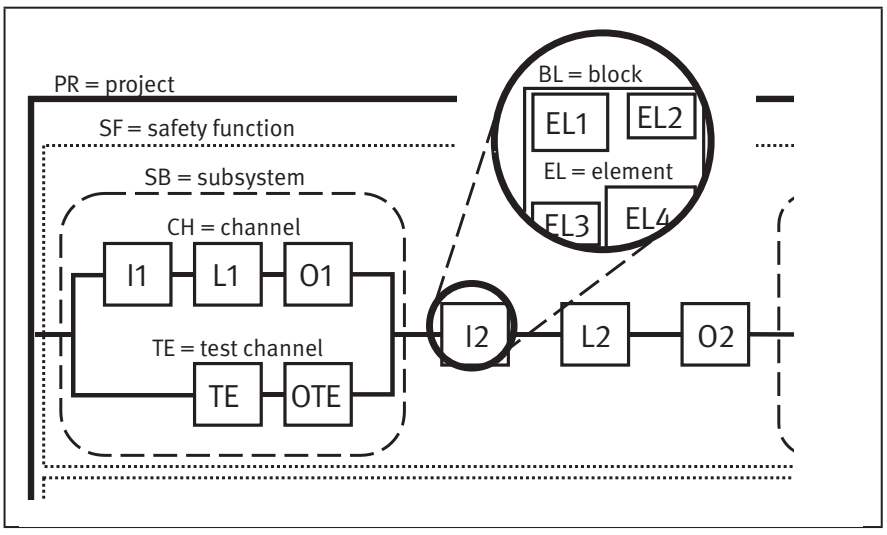


Figure H.1:
Hierarchy levels considered in SISTEMA

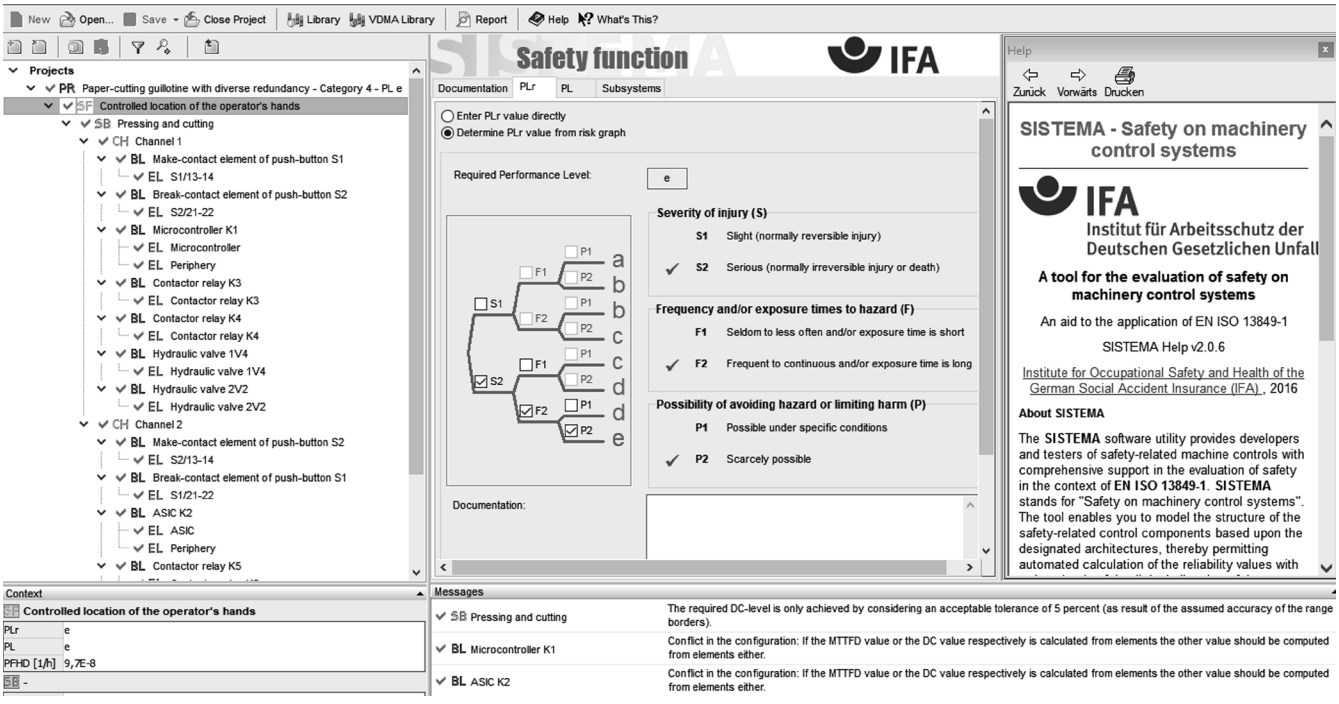
User-friendly library functions complete SISTEMA's range of features. Many manufacturers of components provide libraries of their products' data. Links to these libraries can be found on the IFA's website (www.dguv.de/ifa, Webcode: e92603). Users can however create libraries of their own, in which they can store subsystems that they have developed themselves, or frequently used components. Libraries can be stored either locally, or centrally on servers.

H.3 The SISTEMA user interface

The SISTEMA user interface is divided into four areas (see Figure H.2). The greatest part of the user interface is occupied by the workspace in the centre. Depending upon which view is active, the workspace contains an editable input dialog or a partial view of the overview document. The content of the active view is determined by the basic element selected from the hierarchy described above, which is selected from a tree view on the left-hand side. Each branch in the tree view represents one basic element. Basic elements can be created, deleted, moved or copied on different levels in the tree view. The details of the selected basic element are entered in the input dialog in the editing view. Each input dialog is further subdivided into different areas by tabs. The final tab in each input dialog contains a table summarizing all lower-level branches and listing the main information. If, for example, a block in the tree view is marked, this table shows all elements contained within the block, together with their $MTTF_D$ and *DC* values.

The tree view also shows status information for each basic element. The status information takes the form of a coloured marker adjacent to the branch. A red cross indicates that a condition of the standard is not satisfied, a limit value is exceeded, or that a required value cannot be calculated owing to a general inconsistency. A warning is output in this case. A yellow dot indicates the presence of a message (as for example when a basic element has not yet been assigned a name). All other basic elements are marked with a green tick. The colour marking is also always inherited by the branches higher up in the hierarchy, red having the highest and green the lowest priority. All warnings and information concerning the active basic element are displayed in the message window below the workspace.

Figure H.2:
SISTEMA user interface



The area below the tree view shows the main context information for the selected basic element. This information comprises the PL, PFH_D, $MTTF_D$, DC_{avg} and number of CCF points of the higher-level subsystem, and the PL_r, PL and PFH_D of the higher-level safety function (this applies, of course, only to basic elements on lower hierarchy levels). The consequences of changes in the displayed parameters are thus displayed immediately.

In addition to its flexibility, the SISTEMA user interface is notable for its ease of use and intuitiveness. Context help on the right-hand side is intended to facilitate the learning process.

H.4 Where can SISTEMA be obtained from?

After registering, you can download the SISTEMA software free of charge from www.dguv.de/ifa, Webcode e34183. SISTEMA may be shared with third parties. Modification of SISTEMA is however not permitted. SISTEMA is supplied in the following language versions: English, German, French, Italian, Spanish, Japanese and Finnish. Instructions on the use of SISTEMA can be found in the Getting Started (Webcode m1221153), the SISTEMA cookbooks (Webcode e109249) and the help file installed with SISTEMA. Information and guidance on EN ISO 13849-1 can be found under Webcode e89507 and at www.dguv.de/ifa/13849e.

Annex I:
Operating mode selection safety function

I.1 Introduction

Work on a machine generally entails manual intervention in the danger zone, in addition to automatic operation. Since such intervention, required for example for setup, troubleshooting or cleaning, is generally associated with an elevated risk, different operating modes are employed depending upon the task to be performed.

Selection of an operating mode activates safety functions on the machine that reduce the respective prevailing risk to an acceptable level. From a safety perspective, an operating mode is thus defined in terms of the safety functions that are activated and those that are deactivated when the operating mode is selected. Errors in selection of the operating mode may lead to the required safety functions not being activated: if a different operating mode is activated to that selected, other safety functions are activated rather than those required for the planned task. In the worst-case scenario, an error in operating mode selection may even lead to no safety functions at all being active. The increase in the risk associated with the two cases necessitates a safety analysis of the operating mode selection.

Operating mode selection is normally implemented by electromechanical selector switches. The Machinery Directive [1] sets out a number of requirements for this purpose. For example:

- A selector switch that can be locked in each position must be provided for operating mode selection
- Activation of an operating mode must be unambiguous (i.e. each position of the selector switch must correspond to only one operating mode)
- The selected operating mode must be clearly identifiable by the operator (for example evident from the position of the selector switch)

The Machinery Directive permits substitution of the selector switch in the application by a different item of equipment for selection that is able to restrict the use of certain machine functions to selected groups of persons. The use of electronic equipment for this purpose is not excluded; the circuits and components used that are relevant to safety, and any software that may be used, must however attain a level of safety comparable to that of an electromechanical operating mode selector switch.

Since an error in selection of the operating mode may lead to a direct increase in the risk, selection of the operating mode must be regarded as a safety-related function. It is also listed as such in Table 8 of the standard. This raises the question whether the control aspect of operating mode selection is part of each safety function implemented on the machine, or whether operating mode selection can be regarded as a safety function in its own right. As in the procedure described in subclause 5.3.2, in which overlapping hazards within a given danger zone can be divided into hazards presented by individual parts of the machine, it is expedient for operating mode selection to be treated as a safety function in its own right. This also prevents the components used for operating mode selection from further increasing the average probability of a dangerous failure per hour (PFH_D) in each individual safety function.

As stated in the introduction, an operating mode is characterized in safety terms by the safety functions that are activated by its selection. Accordingly, the safety function of operating mode selection can be defined as follows: activation of the safety functions required for the selected operating mode.

It must now be determined how the required Performance Level PL_r of the operating mode selection function is to be set. In some cases, the PL_r of operating mode selection is already stated in the product standard used. Where this is not the case, it is logical for the highest PL_r of all safety functions that can be activated on the machine to be applied. This rule is based upon the fact that failure of the operating mode selection function can result in the required safety functions not being activated, or – in a worst-case scenario, when operating mode selection fails altogether – the machine being operated unnoticed with no safety functions whatsoever. When a machine tool is changed from the “setup” to the “process monitoring” operating mode, for example, this could lead to an unacceptable increase in the risk.

When operating mode selection is treated as a safety function in the sense of EN ISO 13849-1, the standard also becomes relevant for evaluation of the control technology employed. Depending upon the components used and the scenario, fault exclusions could be asserted. This procedure will be described below for common control elements used for operating mode selection. Further information on operating mode selection as a safety function can be found in subclause 4.1 of [2].

I.2 Cam-operated selector switches

On switches with direct opening contact elements to IEC 60947-5-1 [3], Annex K, fault exclusion for failure of the contacts to open can be applied in accordance with Table D.8 of EN ISO 13849-2 [4]. These switches also have the status of well-tried components; the safety function can therefore be classified as Category 1 in accordance with the standard when they are used.

If, on switches with direct opening contact elements, the fault exclusions are also possible for short circuit between adjacent isolated contacts and for simultaneous short circuit between the three terminals of changeover contacts in accordance with Table D.8 of EN ISO 13849-2, these component faults need not be assumed. For example, on a two-channel electrical circuit, fault exclusion permits modelling as a Category 3 subsystem and implementation up to Performance Level PL d in the single-channel mechanical components (refer in this context also in IFA Report 4/2018e, Annex A, Example 8 [2]).

Fault exclusions cannot be asserted for PL e; additional measures are required in this case. It is possible for example for the operator of the machine to be required to confirm the selected operating mode following display on a user interface. At the same time, an activation system (see subclause I.3) in the safety-related control in PL e is to ensure that at any given time, no more and no less than one operating mode is selected on the machine.

I.3 Electronic equipment

Fault exclusion is not possible on electronic equipment. A further analysis is therefore required for fault analysis of operating mode selection by means of electronic equipment.

For this purpose, it must first be established which operating mode selection functions must be modelled by the selection equipment. Analysis reveals the following sub-functions:

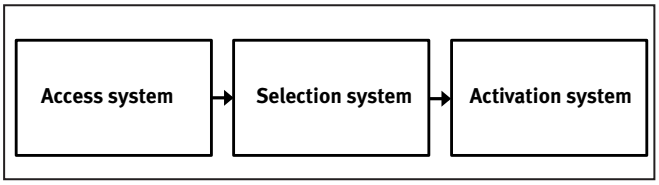
1) Access to the operating mode selection function

2) Selection of the operating mode

3) Activation of the operating mode

On an operating mode selection arrangement engineered by means of electronic equipment, the sub-functions stated can be implemented in three subsystems (Figure I.1) [5]:

Figure I.1:
Structure of the operating mode selection function



Access system

The access system is the part of the operating mode selection function that restricts the facility to select the operating mode to certain groups of persons and prevents actuation of the selection system inadvertently or improperly. Since selection of each operating mode is associated with the activation of different safety functions, the access system is considered relevant to safety.

On electromechanical selection equipment, access is implemented by means of a key. Mechanical coding of the key can be used to limit the selection to specific operating modes. This measure is accompanied by organizational measures that have the purpose of limiting access to the key(s) to certain groups of persons.

On electronic selection equipment, access can be implemented for example by means of an RFID (radio-frequency identification) key or by passwords and corresponding organizational measures. For analysis of the safety, assessment is necessary of whether the access restrictions exhibit safety comparable to that provided by a key on electromechanical selection equipment (integrity of the access data, coding, copy protection, organizational measures, etc.). The access system does not therefore need to be considered during determining of the probability of failure of the safety function.

Selection system

The selection system determines the operating mode that is to be activated by the activation system in the control system (see below).

On electromechanical selection equipment, the selection system corresponds to the manually actuated switch knob, the position of which is transmitted mechanically, for example via a shaft and cams, to the electrical contact elements. As described above, fault exclusion permits safety implementation up to PL d and with the application of additional measures up to PL e on such equipment.

On electronic selection equipment, the selection system is generally implemented by means of a user interface (human-machine interface, HMI), for example employing a touchpad or membrane keyboard. The operator specifies the operating mode to be activated in the machine control

through the user interface and where applicable further electronic components. Since standard components are generally employed for this purpose, classification of a selection system engineered in this way as PL c or higher is not generally possible in the first instance. One means by which the required safety can nevertheless be attained is described in subclause 4.6.4 of the standard, which states provisions concerning software-based parameterization. Since selection of the operating mode by an electronic selection system is equivalent to software-based parameterization, the safety of this selection system can be assessed against this subclause of the standard. The method described in subclause 4.6.4 encompasses selection of the operating mode by the operator, checking of the selected operating mode in the safe control system, and confirmation of the selected operating mode by the operator. This ensures that the integrity of the data used for parameterization is maintained along the entire communication chain and that corruption is detected. In particular, should a fault occur in one of the components of the selection equipment, it is prevented from selecting or confirming an incorrect operating mode.

Activation system

The actual safety function of operating mode selection, i.e. activation of the safety functions required for the selected operating mode, is performed on the activation system. Where electronic selection equipment is used, only the activation system is considered in quantification of the operating mode selection when the selection system – as described above – is evaluated against the requirements of software-based parameterization.

For the activation system, a PFH_D is determined according to the control components used for this purpose that must yield at least the Performance Level PL_r required for the operating mode selection function.

Operating mode selection by means of electronic selection equipment is described below in further detail with reference to an example (Figure I.2).

I.4 Operating mode selection with use of an electronic key system as the access system – PL e

I.4.1 Safety function

Activation of the safety functions required for the selected operating mode.

I.4.2 Structure

The access system in the example takes the form of an electronic key system. The personal authorization level for access is stored on the electronic key.

The selection system comprises three components: an HMI with touchscreen for displaying and selecting the operating modes available in the applicable authorization level, a safety PLC for checking the authorization level and the selected operating mode, and a standard PLC for communication between the components.

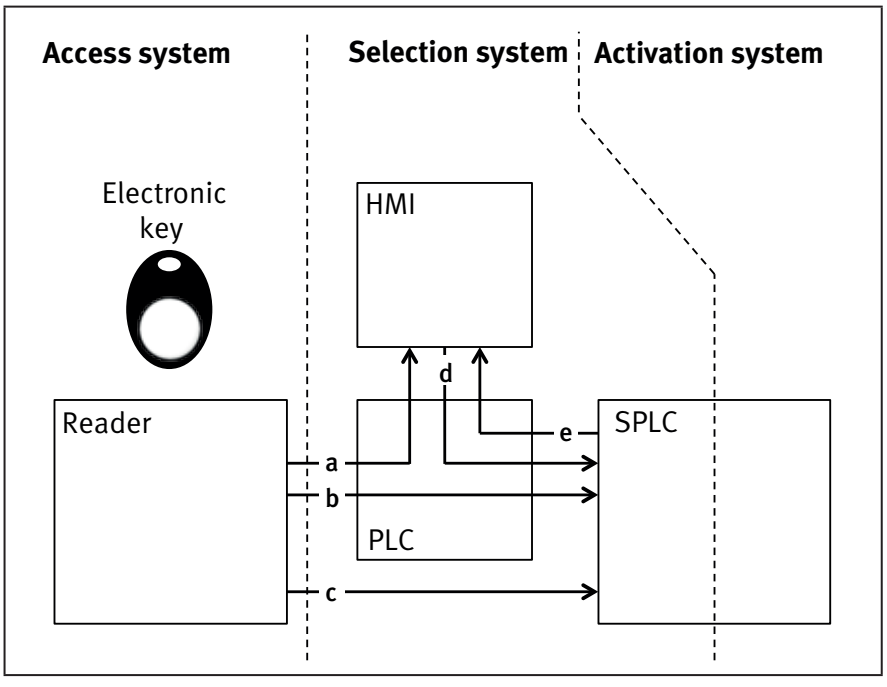


Figure I.2:
Example of operating mode selection with use of an electronic key system as the access system; HMI: human-machine interface; PLC: programmable logic controller (standard); SPLC: safety PLC; a to e: information flow (see functional description)

The safety PLC forms the activation system. It is responsible for changing the operating mode and thus for activating the safety functions required for the operating mode. The safety PLC also ensures that one operating mode and the associated safety functions are active at any given time.

I.4.3 Functional description

Key system/standard PLC

Insertion of a key into the reader causes the authorization level to be read out. The authorization level defines, as a function of the technical qualifications of the operator, which operating modes the operator is to be entitled to select. The reader is connected to the standard PLC through a data interface. Once the key data have been read out, the authorization level is transmitted to the HMI (a) and the safety PLC (b).

In addition to the data interface, the reader features a relay output that is switched off as long as no key is inserted or the key data cannot be read out. The relay output is connected to a safe input on the safety PLC (c).

HMI

The operating modes to which the key provides entitlement by virtue of the authorization level are displayed on the HMI. Following selection of an operating mode, it is transmitted via the standard PLC to the safety PLC (d). The safety PLC sends a feedback message regarding the saved operating mode over the same path back to the HMI, where it must be acknowledged by the operator.

Safety PLC

As soon as a signal change takes place on the safe input of the safety PLC following insertion of the key, a process is launched in the safety PLC at the end of which the selected operating mode is activated. The process comprises the following discrete steps:

1. The authorization level stored on the key is checked for its validity.

2. The operating mode selected on the HMI is then checked for whether it constitutes a valid operating mode and the operator is authorized to select it based upon the authorization level.

3. The operating mode is signalled back to the HMI for acknowledgement (e).

4. Following acknowledgement of the operating mode, it is checked for its consistency with the operating mode actually selected.

5. The safety functions required for the operating mode are activated.

I4.4 Safety analysis

The reader in this example satisfies the structural requirements for Category 3. This means that a single fault cannot lead simultaneously to an incorrect output on the data interface and the relay output. Single faults are detected by high-quality coding of the authorization level, cross monitoring in the reader, and anticipation in the safety PLC. The reader combined with the electronic key serving as an access system thereby attains a level of safety comparable to that of the key of electromechanical selection equipment.

The process described for selection, checking and confirmation of the operating mode and programming of this process satisfy the requirements for software-based parameterization in accordance with subclause 4.6.4 of the standard.

The SRASW software of the safety PLC is programmed in accordance with the requirements for PL e and the guidance in subclause 6.3.

The safety PLC is a safety component for use in PL e.

The average probability of a dangerous failure of the operating mode selection safety function is derived from the PFH_D for the activation system, which in the example is the safety PLC.

More detailed references

[1] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) OJ EU (2006) L 157, pp. 24-86

[2] *Werner, C.; Zilligen, H.; Köhler, B.; Apfeld, R.*: Safe drive controls with frequency converters. IFA Report 4/2018e. 3rd ed. Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin, Germany 2019 (will be published in Summer 2019). www.dguv.de/ifa, Webcode: e635980

[3] IEC 60947-4-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (2009) + A1 (2012)

[4] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2012)

[5] DGUV-Information: Sicherheitsbezogene Betriebsarten an spanenden Werkzeugmaschinen der Metallbearbeitung (FB HM-073). Date of publication: 2/2016. Published by: Fachbereich Holz und Metall der Deutschen Gesetzlichen Unfallversicherung e. V. (DGUV), Mainz, Germany 2016. www.dguv.de/ifa, Webcode: d545286

Annex J:
Overlapping hazards

Changes with respect to the second edition (BGIA Report 2/2008e):

The content below is taken from DGUV expert committee information sheet No 47. Following publication of the third edition of the standard, this information sheet was withdrawn, as its regulatory content was adopted in the standard. It has been included here for the purpose of illustrating the handling of overlapping hazards.

Safety functions to EN ISO 13849-1 where multiple overlapping hazards are present

On complex manufacturing systems and machine tools, overlapping hazards may arise in working areas as a result of hazardous movements caused for example by multiple feed axis drives with closed-loop control. This information sheet describes a procedure, agreed with OSH experts and the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), by which safety functions with overlapping hazards can be modelled and analysed by application of EN ISO 13849-1 [1] or IEC 62061 [2].

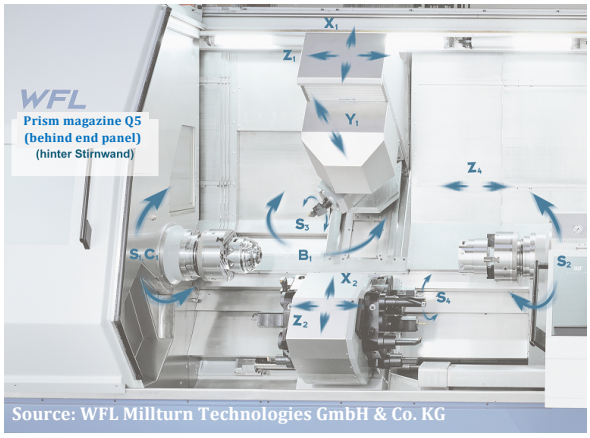


Figure 1: Diagram showing the axes of a machine tool

Overlapping hazards are characterized by the simultaneous action of multiple discrete hazards upon one or more persons (or their limbs or parts of the body) requiring protection and present at a hazardous location or able to reach hazardous areas (see Figure 1).

Discrete hazards include both the movement of an individual axis, and hazards resulting for example from the movement of an entire machine part. Where the movement of a machine part is the result of kinematic interaction between one or more spindle and feed axis drives (such as a milling tool on the saddle of a machining centre), it may therefore be regarded as a discrete hazard.

Contents

1 Current situation

The analysis of discrete hazards is proven good practice in safety technology. Probabilistic analysis in accordance with EN ISO 13849-1 or IEC 61508 [3, 4] and IEC 62061 and the risk assessment for a hazard situation show however that consideration must also be given to the overlap of hazards. The paper [5] provides a basis for discussion of the consequences of a probabilistic approach to the analysis of overlapping hazards. The present information sheet details and elaborates upon this paper.

Owing to the wide range of hazardous situations encountered at the human-machine interfaces referred to above, this information sheet cannot be considered universally valid for their analysis. Standards developers are free to describe appropriate machine-specific provisions in the relevant product or Type C standards and have the remit to do so.

Problematic in this context is that where a large number of overlapping hazards arise at a human-machine interface, a sufficiently low probability of failure of all safety-related control components involved (sensors, logic, multiple actuators) can be demonstrated only with very high analytical effort (e.g. Markov modelling), if at all.

Furthermore, overlapping hazards of differing risk (differing in their PL_r or SIL) make determining the probability of failure of safety functions more complex, which in turn drastically increases the required analytical effort.

Safety functions to EN ISO 13849-1 where multiple overlapping hazards are present

2 Handling of overlapping hazards in practice

Precise examination of which hazards actually overlap within a specific hazard zone is absolutely essential. The dimensions of the parts of the body at risk and the proper actions on the part of the machine operators must be considered, as must the possible movements of the machinery parts presenting a hazard (such as vectorial movements caused by the kinematics of multiple axes or translational movements of single axes).

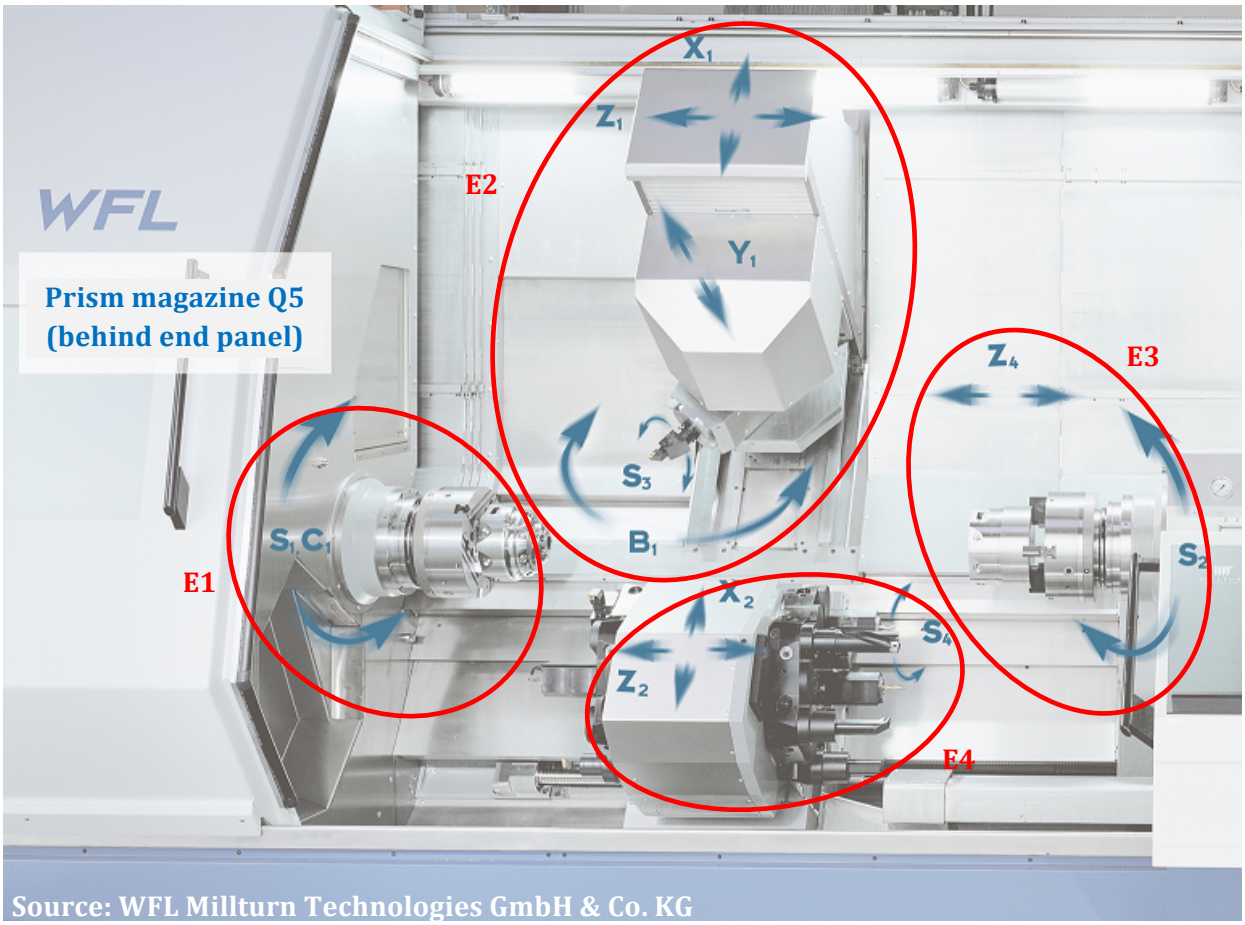


Fig 2: Different discrete hazards, with reference to the example of a machine tool

Depending upon the specific risk assessment, it is permissible in practice to model safety functions based upon an analysis of their discrete hazards, even though they are formed by overlapping hazards.

However, where several actuators (e.g. contactors, valves, closed-loop drive controls) contribute to reducing the risk of the same discrete hazard, they must all be considered together in a safety function. In other words, all actuators capable of causing hazardous movements on one and the same machine part must be considered together in a safety function.

When the individual risk assessment on the machine leads to a differentiated risk assessment with differing PL_r or SIL, it is permissible in practice to model safety functions based upon the analysis of discrete hazards.

Examples:

1. If the movement of a milling tool is derived from the kinematic interaction between multiple movements of discrete axes, all actuators triggering this movement must be grouped in a safety function. The resulting movement may for example be comprised of five discrete movements: three translational movements in the axes X_1, Y_1, Z_1, one swivel movement B_1 and one rotational movement S_3 (see Figure 2, discrete hazard E2).

2. Movements of a single multi-axis robot must be grouped in a safety function for analysis (multiple robots side by side are considered separately).

3. Multiple chucks that together hold an item (where a failure of one of the chucks results in the item no longer being held) must be grouped in a safety function.

With reference to Example 1, formulation of safety functions from the discrete analysis can result in the analysis of the hazards presented by the drive axes as shown in Figure 2. The image shows, by way of example, four discrete hazards E1 to E4, marked by red circles, in the machining zone of a machine tool:

E1: Rotational (S_1) and translational (C_1, for off-centre machining) movement of the left-hand workpiece spindle

E2: Rotational (S_3), translational (X_1, Y_1, Z_1) and swivel (B_1) movement of the milling spindle

E3: Rotational (S_2) and translational (Z_4) movement of the right-hand workpiece spindle

E4: Rotational (S_4) and translational (X_2, Z_2) movement of a tool spindle (the turret toolholder is indexed; its rotational movement need not therefore be considered here)

These four discrete hazards thus yield the four safety functions SF1 to SF4. The safety function SF1 for E1 for example comprises one feed axis and one spindle drive (C_1, S_1). The safety function SF2 for E2 for example comprises the feed axis drives X_1, Y_1, Z_1, the swivel drive (B_1) and the spindle drive (S_3).

References

[1] EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, 2015-12

[2] IEC 62061: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems, 2015-06

[3] IEC 61508-1: Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1: General requirements, 1998-12 (replacement planned by 65A/548/FDIS, 2009-12)

[4] IEC 61508-5 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels, 1998-12 (replacement planned by IEC 65A/552/FDIS, 2009-12)

[5] *Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schäfer, M.:* Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) No 6, pp. 34-37

Annex K:
Index

D

E

F

G

H

R

S

T

U

V

W