DGUV Test
Prüf- und Zertifizierungssystem der
Deutschen Gesetzlichen Unfallversicherung

Can PL c be achieved with a standard PLC?

Are electronic components suitable as an alternative to well-tried components in category 1?

06
06/2022

DGUV Test Information

Question

In standard EN ISO 13849-1 for safe control systems on machinery, control system architectures are assigned to five categories that can achieve one of five Performance Levels (PL). Performance Levels with higher reliability values enable use in applications where a higher risk is present.

In accordance with the current version of the standard, single-channel electronic control systems without testing and redundancy only achieve the lowest category (category B), and a maximum PL b. If only well-tried components are used, the higher category 1 and PL c can be achieved.

However, the standard limits this possibility to certain technologies: Complex electronic components, e.g. programmable logic controllers (PLCs), microprocessors and application-specific integrated circuits (ASICs) cannot be considered well-tried components.

There have been continuous initiatives from machine users to remove this limitation after over two decades of experience using electronic components for safety-related control systems. In 2017, the German Machine Tool Builders' Association (VDW) published a study on the field-evidenced reliability of automatic multi-spindle lathes with a workpiece clamping safety function that is actuated by means of a standard PLC (https://vdw.de/en/safety-of-standard-plc-control-validated-yet-again-2/).

This argument is also being discussed in standards committees. Although the example of a standard PLC is mentioned primarily, the fundamental question also affects all other devices with complex electronic control system components, e.g. microprocessors and integrated circuits.

Against this backdrop and with a view to the upcoming revision of the second part of EN ISO 13849, in which typical well-tried components for various technologies are listed, a working group made up of various DGUV Test testing and certification bodies tackled this topic. The collective position of the group is presented in this paper.

Position of DGUV Test

Some arguments are made again and again to prove the **reliability of complex electronic components**. These justifications can be refuted as follows:

- Statistics-based arguments, which, for example, point to low numbers of failures or claim there is no relevant incidence of accidents

  ► Statistical records often have systematic inadequacies. Sporadic, non-reproducible failures (e.g. caused by soft errors) and software errors do not appear in statistics about replaced components. Near-accidents are usually either not documented or documented in a way that is not meaningful.

- Because complex electronics have been used for functional safety for multiple decades, it is claimed that these now offer a similar level of reliability as electromechanics and fluid technology, for example.

  ► Complex electronics and their software often have much shorter innovation cycles than electromechanics and fluid technology. In the hardware, for example, components on the PCB (printed circuit board) are replaced by more modern versions, components are procured from other suppliers, the design is modified/miniaturised or the production technology is modernised. The embedded software is updated regularly for the purpose of eliminating faults or adding new functionality. This means that reliability is rarely achieved despite the high level of development efforts (see Pentium bug, for example: https://en.wikipedia.org/wiki/Pentium_FDIV_bug).

  - In some applications (e.g. machine tools or earth-moving machinery), single-channel complex electronics (standard PLCs or standard sensors) in category B for PL b have already been used for a long time for safety functions that could lead to serious injuries (fatal or irreversible) if the safety function were to fail in the event of a fault. However, in contrast, if you use the risk graph from EN ISO 13849-1 to determine the required Performance Level (PL_r), in the event of serious injuries a PL_r of c or higher would be the result. However, solutions to achieve PL c or higher (tested single-channel systems or two-channel systems) are too technically complicated, the costs are too high or the performance is insufficient.

  ► Product standards can define the requirements individually in their own area of application, which means that they can deviate from the principles set out in generic safety standards, such as EN ISO 13849-1, in order to adequately account for application-specific features, the state of the art and the incidence and severity of accidents (e.g. if only minor, reversible injuries occur). In this context, in justified individual cases, high-rated requirements in relation to the reliability of the machine control system can be downgraded and supplemented by means of equipment-related measures or organisational measures, provided that a comparable level of safety is achieved through other means. Furthermore, since the third edition of the standard from 2015, there is the option of downgrading the PL_r by one level by accounting for a lower probability of occurrence of a hazard. The definition of requirements that are as concrete, practicable and effective as possible is in the interests of both users and occupational safety and health.

In order to assess the reliability of complex electronics, especially programmable components such as a standard PLC, the **following error sources and vulnerabilities** require special attention:

- Accident investigations show failures of complex electronics as causes for failures of control systems. Examples include the failure of output cards, which leads to stuck-at faults (static signals, short circuit or interruption), or the non-resetting of an interrupt. It was also observed that the power supply was not completely switched off and a low voltage level of 5 V was sufficient to keep out-put switching elements (e.g. contactors, relays, electromechanically actuated valves) in a held state (ON state).

  ► Can suitable fault detection and fault reaction measures be taken here that lead to a safe state in the event of a dangerous failure?

- Fluctuations in the power supply (especially overvoltages), ageing of components, signal drift, electromagnetic interference and other environmental influences (e.g. temperature, humidity, application-specific features) can lead to undefined and dangerous states.

  ► Can a sufficient ability to resist faults be ensured, e.g. oriented towards SIL 1 environmental requirements in Table A.16 and B.5 of IEC 61508-2, the environmental requirements in Section 4.3 of IEC 61496-1 and the increased requirements in relation to the ability to resist electromagnetic interference in Section 12.5 of IEC 61131-6 (functional safety), which go beyond the requirements in Section 8.3 IEC 61131-2 (equipment requirements and tests)? DGUV Test Information 15 and a new Annex L in the upcoming fourth edition of EN ISO 13849-1 provide further information regarding the practical implementation of the requirements for sufficient electromagnetic compatibility.

- In contrast to application software, the embedded software (operating system) of programmable standard components is not accessible to the integrator or user. It has not been designed by the manufacturer with safety requirements in mind and it is also difficult for the user to do this at a later stage. It is also not possible in practice to verify the reliability of the embedded software due to systematic difficulties in the recording of statistical data (see "Statistical arguments" above).

  ► This issue is addressed in EN ISO 13849-1 as such that this case is tolerated for PL a and b when category B, 2 or 3 is used. For PL c and d with category 2 or 3, the use of redundant technologies is required. A single-channel implementation (category B or 1) in PL c is not envisaged for category 1 due to the exclusion of complex electronic components as well-tried components.

Taken together, the previously mentioned arguments, error sources and vulnerabilities lead to the following **arguments, which continue to justify the exclusion of complex electronic components from the list of well-tried components**:

- Standard PLCs and other complex electronic components, such as sensors, are available in countless varieties (e.g. compact controller, laptop, microcontroller systems) with short innovations cycles, and are therefore very inexpensive.

- Complex electronic components have a varied, partly unpredictable failure behaviour, e.g. triggered by electromagnetic interference. In practice, software errors or soft errors can no longer be controlled fully. Consequently, these cannot be viewed as a black box with simple, defined failure behaviour.

- The rate of change of complex electronic components (modification of hardware and software) is significantly higher than that seen in electromechanics or fluidics, and therefore, there is an increased probability for systematic failures. These result from errors during the development or production process.

- For category 1 and PL c, the standard requires the use of well-tried safety principles in addition to the basic safety principles. Therefore, reliable verification is required to show that the following requirements in particular have been satisfied: Over-dimensioning, balance between complexity and simplification, separation of safety-related functions and other functions; and for software: Integrity and reliability, avoidance of undefined states. This verification is not feasible for single-channel complex electronics in accordance with the relevant requirements.

Position of DGUV Test

Taking into account the arguments, error sources and vulnerabilities, the current exclusion of complex electronic components from the list of well-tried components remains correct.

Alternative ways to achieve PL ≥ c with the use of a standard PLC

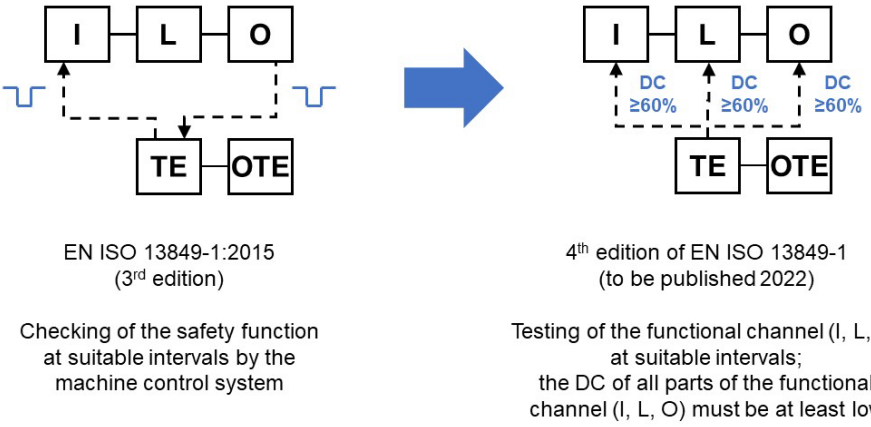
According to EN ISO 13849-1, as an alternative to single-channel control systems using well-tried components (category 1), PL c can be achieved with single-channel tested control systems (category 2) or two-channel tested control systems (category 3). Depending on the task of the control system, these two alternative possibilities can be implemented with a manageable amount of additional effort.

However, as is the case for category 1, well-tried safety principles shall be implemented in addition to the basic safety principles for categories 2 and 3, and all requirements for the relevant category set out in the standard shall be fulfilled. Special attention shall be paid to an effective test rate and resistance against common cause failures, which includes independent operation of the test equipment and functional channel.

Implementation in category 2

- With the upcoming fourth edition of EN ISO 13849-1, checking the fault-free execution of the entire safety function at suitable intervals will no longer be required for control systems in category 2. Instead, testing of the functional channel with at least low diagnostic coverage (DC) is sufficient, i.e., 60 percent of dangerous failures shall be detected. However, this minimum requirement for test coverage shall be satisfied individually for the input (I), logic (L) and output (O) blocks in the functional channel. Since this means that the failure of the safety function no longer needs to be recognised, but instead – specifically for PL c – only the majority of dangerous failures need to be detected through tests, it is worth checking the feasibility of implementation as a category 2 in accordance with the requirements of the standard.

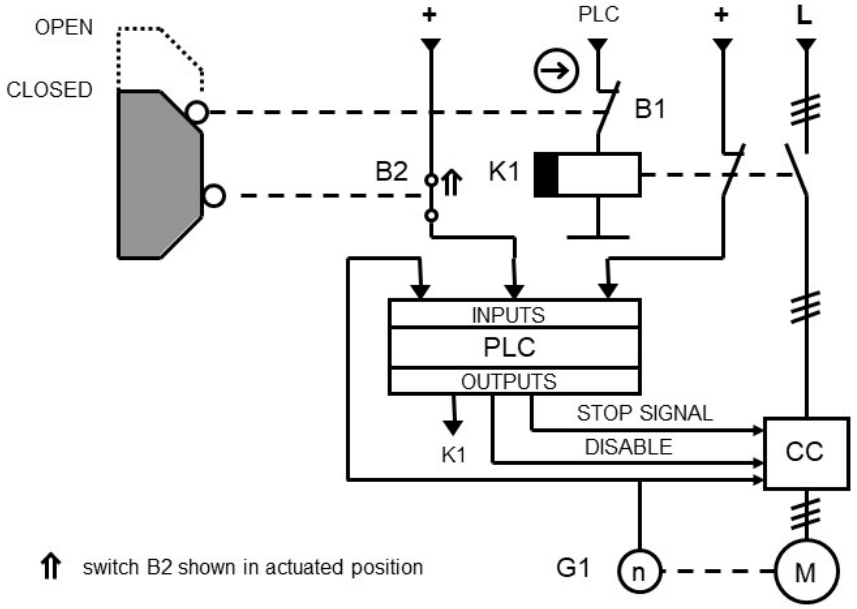
Figure 1: Example implementation of a control system in accordance with category 2 in the upcoming fourth edition of EN ISO 13849-1; source: DGUV Test



- The addition of a second functional channel with a small number of components that is limited to the straight execution of the safety function transforms the control system into category 3. Since one (programmable) electronic component is already present with the standard PLC, the minimum required low diagnostic coverage can often also be upgraded with a limited amount of effort.

  Control system example B in Annex I of EN ISO 13849-1 shows such a configuration, which can even achieve PL d under certain conditions provided all requirements set out in the standard are satisfied. Here, the existing functional channel consisting of position switch B2, standard PLC and current converter CC is expanded with a second electromechanical functional channel featuring an additional position switch B1 and a contactor relay K1. The required fault detection is mainly implemented in the existing standard PLC:

Figure 2: Example implementation of a control system in accordance with category 3 based on Section I.4 of EN ISO 13849-1; source: DGUV Test



B1	Position switch (normally closed switch with direct opening action)
B2	Position switch (normally open switch, shown in actuated position)
K1	Contactor relay (contact with drop-out delay)
PLC	Programmable logic controller without integrated safety
CC	Current converter
G1	Rotation sensor
M	Motor

Further information

- EN ISO 13849-1:2015-12, Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
  The revised fourth edition of EN ISO 13849-1 is scheduled to be published at the end of 2022.
- EN ISO 13849-2:2012-10, Safety of machinery - Safety-related parts of control systems - Part 2: Validation
- Safety of machine controls to EN ISO 13849: www.dguv.de/ifa/13849e
- IEC 61508-2:2010-04, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- IEC 61496-1:2020-07, Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests
- IEC 61131-2:2017-08, Industrial-process measurement and control – Programmable controllers - Part 2: Equipment requirements and tests
- IEC 61131-6:2012-10, Programmable controllers - Part 6: Functional safety
- EMC and functional safety in the field of machinery, Increased immunity as required by DIN EN 13849-1 for integration of SRP/CS, DGUV Test Information 15 (12/2016), Webcode: e24251

DGUV Test Office
Alte Heerstrasse 111
53757 Sankt Augustin, Germany
Tel.: +49 30 13001 4566
Fax: +49 30 13001 864566
Email: dguv-test@dguv.de