IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

0340

Aus der Arbeit des IFA

Ausgabe 7/2012 617.0-IFA:638.22

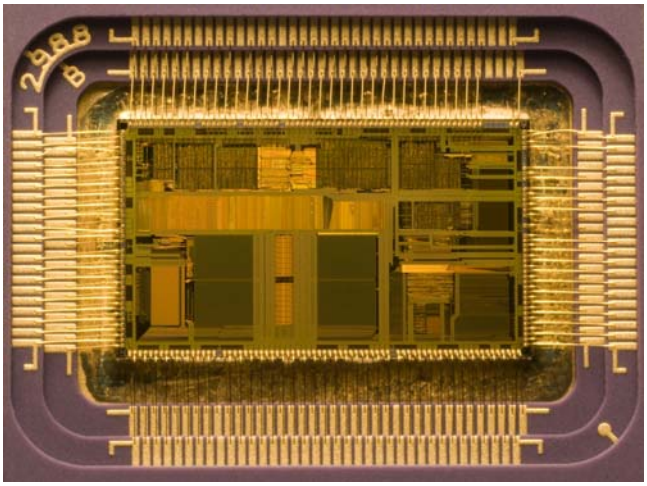
Sicherheits-Mikrokontroller auf dem Vormarsch

Problem

Der Einsatz von Mikroelektronik kann in der Sicherheitstechnik von Maschinen und Industrieanlagen als etabliert gelten. Der Hang zu immer kleineren, oft sogar komplexeren Systemen stellt auch die Sicherheitstechnik vor neue Herausforderungen. Eine häufig verwendete Methode sind redundante Schaltungen: Sicherheitsfunktionen werden damit doppelt ausgeführt. Diese Technik wird seit Jahrzehnten genutzt, wobei genauestens auf die Unabhängigkeit der beiden Schaltungsteile (Kanäle) geachtet werden muss. Sonst könnten Ausfälle in einem Kanal den anderen Kanal in Mitleidenschaft ziehen, mit negativen Folgen für die Sicherheit.

Anlass für eine weitere Miniaturisierung war vor gut zehn Jahren der Wunsch aus der Industrie, die redundanten Kanäle innerhalb eines einzelnen Mikrochips zu realisieren: Er sollte die gesamte Schaltungsstruktur doppelt bereithalten und gleichzeitig die sicherheitstechnischen Anforderungen erfüllen. Hierzu boten sich anfangs kundenspezifische Chips (ASICs = Application Specific Integrated Circuits) an. Die Serienreife der ASIC-Technologie liegt zwar schon gut 30 Jahre zurück, ihr Einsatz in der Sicherheitstechnik ließ dennoch einige Jahre auf sich warten.

Gesucht waren jetzt eine Methode und Anforderungen, um die Sicherheit dieser Bauteile zu beurteilen.



Innenleben eines Mikrochips, Quelle Wikipedia (Chip von Matt Britt präpariert, Foto Matt Gibbs).

Aktivitäten

Das IFA führte zu Beginn der Arbeiten Recherchen zum Aufbau von Mikrochips und ASICs durch und erörterte die Thematik mit Experten aus der Halbleiterindustrie. Innerhalb eines Expertenarbeitskreises entstand ein sicherheitsbezogenes Maßnahmenbündel, anhand dessen solche mehrkanaligen ASICs sicher gestaltet werden können. Diese Maßnahmen gingen als deutscher Vorschlag, begleitet durch das IFA, in die internationale Normung zur zweiten Ausgabe der IEC 61508 ein. Gleichzeitig wurden die Maßnahmen bei mehreren Industrieprüfungen auf ihre Wirksamkeit und Machbarkeit überprüft. In der Normung wurde der Ansatz nach langwierigen Grundsatzdiskussionen sogar von ASICs auf integrierte Schaltkreise (ICs) allgemein ausgeweitet.

Ergebnisse und Verwendung

Bei der Zusammenführung redundanter Kanäle auf einem Chip (Substrat) muss die primäre Frage lauten: Sind Ausfälle gemeinsamer Ursache (common cause failure, CCF) mit ausreichender Wahrscheinlichkeit verhindert? Wegen des naturgemäß konservativen Ansatzes in der Sicherheitstechnik wird diese von der Normung als On-Chip-Redundanz bezeichnete Technologie bei besonders hohen Risiken ausgeschlossen. Generell ist ein möglicher Einsatz vorab im Rahmen einer CCF-Analyse zu beurteilen. Ein Chipdesign mit On-Chip-Redundanz in Übereinstimmung mit Anhang E der IEC 61508-2, der nach aktuellem Stand nur digitale Schaltungstechnik betrachtet, muss eine Reihe fundamentaler Anforderungen einhalten.

Wichtige Maßnahmen zur Realisierung sind z. B.:

- Blockbildung durch strenge physikalische Trennung redundanter Kanäle auf dem Substrat
- Maßnahmen gegen Einflüsse der Spannungsversorgung, z. B. eine eigene Versorgung für jeden Block (Kanal)
- für jeden einzelnen Kanal Realisierung einer minimalen Diagnose/Fehlererkennung von 60 %, die besonders auf eine mögliche Temperaturerhöhung durch Chipdefekte reagieren muss
- Einhaltung eines Minimalabstands zwischen Blöcken
- symmetrische Leitungsführung der Versorgungsleitungen und kreuzungsfreie Führung der Schnittstellen.

Quasi zeitgleich mit Abschluss der Normungsarbeiten brachten namhafte Mikrochip-Hersteller sogenannte Sicherheits-Mikrokontroller auf den Markt, die das On-Chip-Redundanz-Konzept verfolgen.

Nutzerkreis

Hersteller von elektronischen Sicherheitsbauteilen in den Bereichen Maschinen, Automobil und Medizintechnik; Hersteller von Mikrochips

Weiterführende Informationen

- DIN EN 61508 Teil 1-7: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (02.2011). Beuth, Berlin 2011
- Merchant, K.; Bömer, T.: Requirements for On-Chip Redundancy in Safety Technology (Anforderungen an On-Chip-Redundanz in der Sicherheitstechnik). 9. Internationales Symposium Funktionale Sicherheit in industriellen Anwendungen. 4.-5. Mai 2010, Köln
- Hercules™ ARM® Sicherheits-Mikrocontroller, http://www.ti.com/ww/de/prod_mcu_hercules.html (Texas Instruments, aufgerufen 26.06.2012)
- Safety mit zwei Kernen, http://www.elektroniknet.de/automation/news/article/30528/0 (WEKA-Fachmedien, aufgerufen 26.06.2012)

Fachliche Anfragen

IFA, Fachbereich 5: Unfallverhütung − Produktsicherheit

Literaturanfragen

IFA, Zentralbereich

Herausgeber und Druck:
Deutsche Gesetzliche Unfallversicherung e. V.
(DGUV), Mittelstraße 51, 10117 Berlin

ISSN (Internet): 2190-006X
ISSN (Druckversion): 2190-0051

Bearbeitet von: Dr. Michael Schaefer,
Dipl.-Ing. Thomas Bömer
Institut für Arbeitsschutz der Deutschen
Gesetzlichen Unfallversicherung (IFA)
Alte Heerstraße 111, 53757 Sankt Augustin
Tel. 02241 231-01/Fax: -2234
E-Mail: ifa@dguv.de, Internet: www.dguv.de/ifa