IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

0340

Focus on IFA's work

Edition 7/2012

617.0-IFA:638.22

Safety microcontrollers growing in popularity

Problem

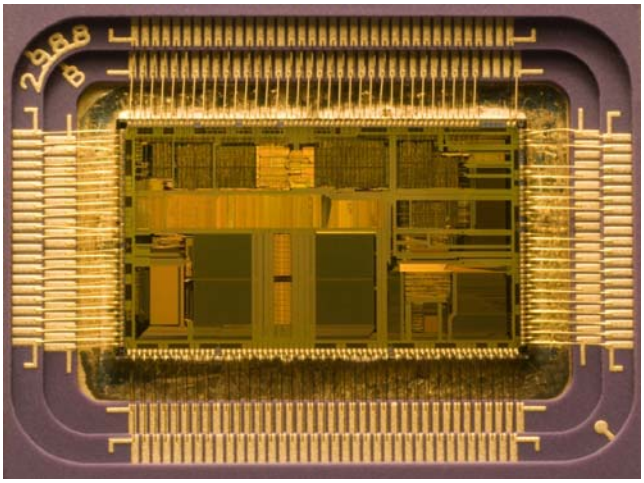
The use of microelectronics in the safety systems of machinery and industrial plant may now be regarded as established. The trend towards increasingly miniaturized and often more complex systems also presents new challenges for safety engineering. One method frequently applied is that of redundant circuits, in which safety functions are implemented in duplicated form. This technology has been in use for decades. Close attention must however be paid to the independence of the two circuits (channels) from each other, since failures in one channel may otherwise impact upon the other channel, to the detriment of safety.

A reason for further miniaturization over ten years ago was the desire of industry to implement the redundant channels on a single microchip. The chip was to provide the entire circuitry in duplicated form, whilst at the same time satisfying the safety requirements. Application-specific integrated circuits (ASICs) were initially used for this purpose. ASICs reached production maturity over 30 years ago; it was some years however before they came to be used in safety technology.

Methods and specifications were then required by which the safety of these components could be evaluated.

Activities

At the beginning of the work, the IFA researched the structure of microchips and ASICs, and discussed the issue with experts in the semiconductor industry. A group of experts drew up a package of safety-related measures by reference to which such multi-channel ASICs could be designed so as to be safe. These measures were submitted to the process of international standardization, specifically for the second edition of IEC 61508, in the form of a German proposal supported by the IFA. At the same time, the measures were reviewed for their effectiveness and feasibility in a number of type approvals of industrial devices. Following protracted discussions of principles, the approach was even extended during standards development to include not just ASICs but integrated circuits in general.



The inside of a microchip. Source: Wikipedia (chip prepared by Matt Britt; photograph: Matt Gibbs)

Results and Application

When redundant channels are grouped on a single chip (substrate), the principal question must be: are common cause failures (CCFs) prevented with adequate probability? The inherently conservative approach in safety engineering rules out this technology, described in the standards as on-chip redundancy, in applications involving particularly high risks. A possible application must generally be evaluated beforehand by means of a CCF analysis. A chip design involving on-chip redundancy in compliance with Annex E of IEC 61508-2, which at present considers only digital ICs, must satisfy a number of fundamental requirements.

Important measures for implementation include:

- The formation of blocks by strict physical separation of redundant channels on the substrate
- Measures to prevent the power supply from exerting an influence, such as a dedicated supply for each block (channel)
- Implementation for each individual channel of a minimum diagnostic coverage of 60%, which in particular must respond to any temperature increase caused by chip defects
- Observance of a minimum clearance distance between blocks
- Symmetrical routing of power supply conductors, and non-crossing interfaces

Virtually at the same time as the standardization work was completed, leading microchip manufacturers introduced safety microcontrollers to the market that implemented the on-chip redundancy concept.

Area of Application

Manufacturers of electronic safety components in the areas of machinery, cars and medical devices; microchip manufacturers

Additional Information

- IEC 61508 Parts 1-7: Functional safety of electrical/electronic/programmable electronic safety-related systems (2010-04). IEC, Geneva 2010
- Merchant, K.; Bömer, T.: Requirements for On Chip Redundancy in Safety Technology. 9th International Symposium. Functional Safety in Industrial Applications. 4-5 May 2010, Cologne
- Hercules™ ARM® Safety MCUs, http://www.ti.com/mcu/docs/mcuprodoverview.tsp?sectionId=95&tabId=2835&familyId=1931&DCMP=hercules&HQS=hercules-bthp (Texas Instruments, accessed 27 September 2012)
- Safety mit zwei Kernen http://www.elektroniknet.de/automation/news/article/30528/0 (WEKA-Fachmedien, accessed 26 June 2012)

Expert Assistance

IFA, Division 5: Accident prevention – Product safety

Literature Requests

IFA, Central Division

Published and printed by:
Deutsche Gesetzliche Unfallversicherung e. V.
(DGUV), Mittelstraße 51, 10117 Berlin, Germany

ISSN (online): 2190-006X
ISSN (print): 2190-0051

Edited by: Dr Michael Schaefer, Thomas Bömer
Institut für Arbeitsschutz der Deutschen
Gesetzlichen Unfallversicherung (IFA)
Alte Heerstraße 111, 53757 Sankt Augustin, Germany
Phone: +49 2241 231-01/Fax: -2234
E-mail: ifa@dguv.de, Internet: www.dguv.de/ifa