

Focus on IFA's work

Edition 1/2015

617.0-IFA:638.22

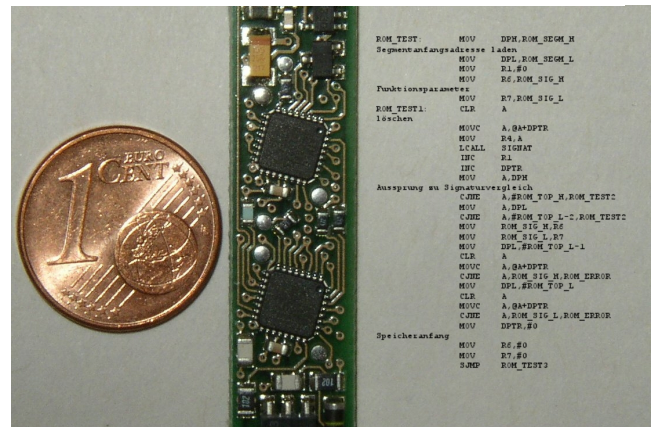
Self-tests for microprocessors incorporating safety functions

Problem

Machines with microprocessor control systems have become an accepted part of modern working life. Such controls are also increasingly assuming safety functions, and many complex safety functions are in fact inconceivable without them.

The progress of technical development has been accompanied by adaptation of the relevant standards. This adaptation is continual, in order for safety provisions to remain in step with the rapid pace of innovation. In contrast to everyday products (the development from the cassette recorder to the MP3 player will be familiar to all), stricter requirements must be defined for industrial machinery and equipment in the interests of safe, accident-free work. This fact is also taken into account by the standards governing the new microprocessors. The standards contain requirements concerning organization and specific provisions governing the design of software, as well as those concerning the structure of a machine control system.

Despite this description of the measures which are to be taken in the software, implementation in practice is not easy. In the view of the IFA, a small example is often sufficient for software developers to find an adequate solution of their own for their application.



Safe software is not a function of the microprocessor size

Activities

The IFA has developed routines for a type 80C537 microcontroller, programmed them in a modular fashion, and supplemented them with comments. This allows to offer consultancy and to respond to requests for suitable examples of automatic microprocessor self-tests. Attention was paid here to absolute independence from existing solutions, and the software was developed solely against the relevant standards. Testing of the software modules produced in this way was also conducted in accordance with the provisions of the standards.

Results and Application

The explanatory description of the software modules has been published in a BGIA report, which can be downloaded from the Internet.

The software modules have been compiled in an archive file and can also be downloaded free of charge.

The particular hardware features of the microprocessor were deliberately not exploited during programming. Transfer of the tests to other microprocessors should not therefore present difficulties. Should this not be possible in certain cases, however, the examples provide at least a starting-point for implementation of the requirements of the standards in practice.

Area of Application

Software developers for safety-related systems

Additional Information

- Self-tests for microprocessors with safety functions, or: "Quo vadis, fault?" BGIA Report 7/2006e. Published by: Deutsche Gesetzliche Unfallversicherung (DGUV), Sankt Augustin 2009, www.dguv.de/webcode/e91093
- DIN EN 61508 Parts 1-7: Functional safety of electrical/electronic/programmable electronic safety-related systems. Beuth, Berlin 2011
- EN ISO 13849: Safety of machinery – Safety-related parts of control systems. Part 1: General principles for design (12.08). Beuth, Berlin 2008

Expert Assistance

IFA, Division 5: Accident prevention – Product safety

Literature Requests

IFA, Central Division