Design of safety-related architectures based on asic and microprocessors

Jean-Luc Durka, D. Reinert

DESIGN OF SAFETY-RELATED ARCHITECTURES BASED ON ASIC AND MICROPROCESSORS

Authors

Durka, J.-L., Institut National de l'Environnement Industriel et des Risques*, Reinert, D., Berufsgenossenschaftliches Institut für Arbeitssicherheit, Germany. *INERIS, Parc Technologique ALATA, B.P. 2, 60550 Verneuil-en-Halatte, France

Résumé

L'INERIS et le BIA collaborent dans un projet européen sur la conception et la validation de technologies innovantes tels que l'utilisation des ASIC pour les parties des systèmes de commande relatifs à la sécurité, ainsi que sur la conception d'une architecture, à base de microprocesseurs, configurable de la catégorie 2 à la catégorie 4 selon la norme EN 954[1]. Cette étude s'intègre dans le cadre de la Directive Machines[2]. Elle présente, d'une part, les spécifications nécessaires à la conception de tels dispositifs relatifs à la sécurité, et d'autre part, leurs méthodes de validation.

1. Introduction

The STSARCES project is divided into five research work packages. A specific work-package, joining INERIS and BIA as test-houses, SICK and JAY as manufacturers, takes into account the foreseeable evolutions in design of safety related systems owing to continuing progress in the electronic technologies. The work programme is divided in two main parts :

- BIA and SICK defined a dual channeled microprocessor controlled device which can be configured for the categories 2, 3 or 4. BIA developed a Markov-Model for the chosen architecture. Different diagnostic coverages and on-line test intervals can be simulated.
- INERIS and JAY work on ASIC's development for a single-way safety light barrier with a dual ASICs designed for a category 4. The first part deals of techniques and requirements for ASICs design. The second part is based on methods and techniques for ASICs validation.

2. New topics in research

Under the term ASIC (Application Specific Integrated Circuit) we can found a partial list of the following components :

- Analogue functions or mixed functions (amplifiers, analog gates, phase-locked loops, triggers, etc.). These circuits are issued from standard cells or full-custom components.
- Digital functions (PAL, FPGA, EPLD, etc.).
- Microprocessors and their peripherals («Von Neumann» or «Harvard» structures).

DESIGN OF SAFETY-RELATED ARCHITECTURES BASED ON ASIC AND MICROPROCESSORS

For ASIC components the input document is the technical specification, and software design and simulation give the layers. The usually generated schema is only a thinking aid but it is not the viewing of the exact chip result (integrity of compilers).

For microprocessor Von Neumann structure some rules are well known (as RAM and ROM testing). These rules are not applicable for Harvard structure. This component is impossible to use for safety related purposes, and other strategies for testing need to be imagined.

3. System configurable for category 2 to category 4

Today, the designs are always specific for the different safety categories. So manufacturers build specific type 2 to type 4 systems in accordance to the IEC 61496[3]. The different categories are only unit cost driven. The R&D costs and times are high. Typically they use microprocessor-based technologies in their products, but also custom specific ASIC solutions are implemented.

Tomorrow, the time to market will become shorter and shorter. So it will be necessary to reduce the R&D time to a minimum and make a project mix between the unit costs and the R&D efforts. An interesting issue consists to build a type 2 up to type 4 configurable system with an identical hardware. The only difference is the software running in the microprocessors. The safety categories shall be selected in the final test. The main questions are :

- Which quality level of testing is necessary in which safety categories ?
- What is the minimum test repeat time in the system ?
- How long could the system continue to run after a fault detection ?

The prototype is based on two microprocessors with a 8051 core. Additionally the processor has EEPROM, a SPI interface for interprocessor communications and it allows incircuit programming. The prototypes have only safety-related digital inputs and outputs for evaluation.

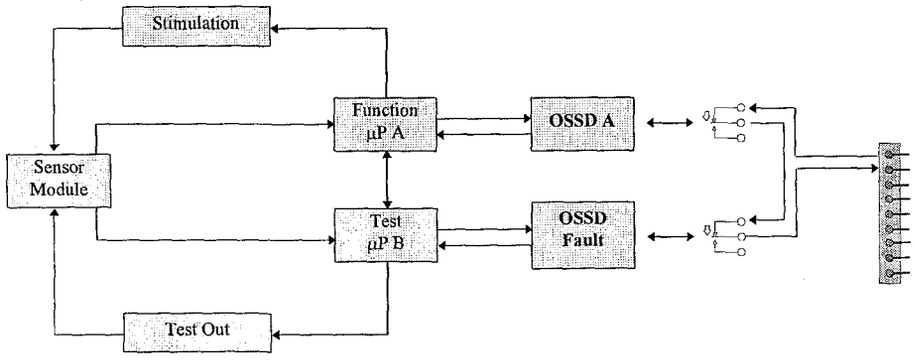

Figure 1 : Category 2 architecture

DESIGN OF SAFETY-RELATED ARCHITECTURES BASED ON ASIC AND MICROPROCESSORS

In this architecture, the microprocessor B makes a periodic test to reveal a failure to danger (e.g. loss of detection capability, response time exceeding, failure of microprocessor A, failure of the output signal switching device "OSSD", etc). The test signal simulates the actuation of the sensing device. A single fault affecting normal operation is detected by the periodic test.

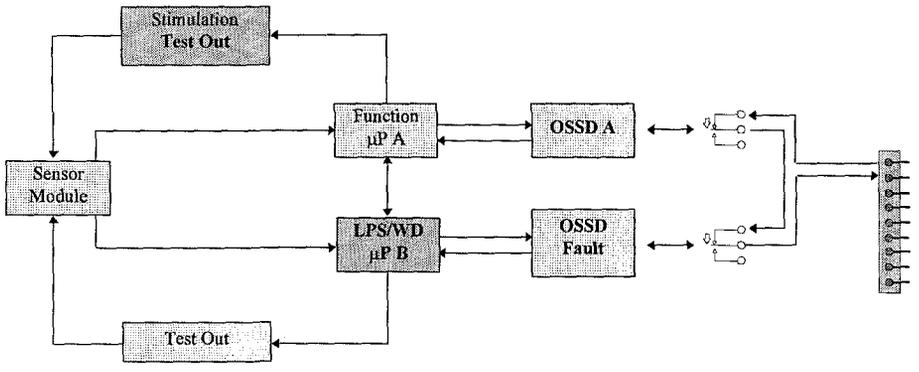

Figure 2 : Category 3 architecture

In this architecture, a single fault in the control does not lead to the loss of the safety function. Some but not all faults will be detected and an accumulation of undetected faults can lead to the loss of the safety function.

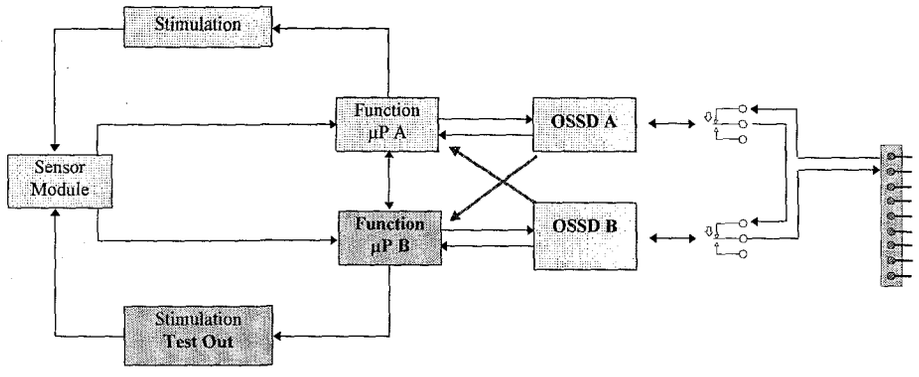

Figure 3 : Category 4 architecture

In this architecture, a single fault in the control does not lead to the loss of the safety function, and the single fault is detected at or before the next demand upon the safety function. When the faults occur, the safety function is always performed and the faults will be detected in time to prevent the loss of the safety functions.

4. Behaviour under failure

To avoid any unsafe behaviour the following rationale could be used, after choosing the relevant category :

- For external signals we can use the catalogue of single faults which is the annex B of EN 61496-1.
- For internal signals the followings topics need to be analysed :
  - Rules of design, including fault simulation (e.g. IEC 61508[4], DIN V VDE 801 Appendix A2[5]), where some failures are described : signal stucked, loss of a function, loss of time synchronism, components drift, signal unwanted oscillations, intermittent failures.
  - Tools of design-compilers integrity, certified versions. Low or high level langage.
  - Suggested safety strutures.
  - Process stability and known technology.

5. Validation for complex electronics circuits

For complex application specific integrated circuits a new approach in validation seems to be necessary because this type of complex components cannot be completely validated through testing. The validation procedures should be included in early stages of the design to be more effective.

For complex application specific integrated circuits (ASICs), the term „proven in use" should be clarified and related to the different inputs for the design process :

- process technology,
- design rules for cell placement, interconnect and layout,
- pre-layouted or generated macro cores,
- cell libraries, including layout information and simulation models,
- soft macros,
- design tools: layout, synthesis, simulation.

The validation plan is shared in six main phases :

- Functional Testing

Functional testing is used to reveal failures during the specification and design phases. During the functional tests, reviews are carried out to see whether the specified characteristics of the system have been achieved.

- Functional testing under environmental conditions

This method provides that the safety-related system is protected against typical environmental influences. The system is put under various environmental conditions during which the safety functions are assessed.

- Fault insertion testing

Fault insertion testing is used to introduce or simulate faults in the system hardware. However, it is difficult, by influencing inputs and outputs of a complex component, to reach all relevant internal states and nodes. Therefore this method is not sufficient for validation of safety functions. The theoretical base of fault insertion testing is a Failure Mode and Effects Analysis.

- Worst case testing

The operational capacity of the system and the component dimensioning is tested under worst case conditions. The environmental conditions are changed to their highest permissible marginal values. The most essential responses of the system are inspected and compared with the specification. The equipment under test is usually damaged when the worst case test was done successfully.

- Expanded functional testing

Further to normal functional testing, it is useful to check the behaviour of the safety-related system in the event of rare or unspecified inputs. This method is implemented for testing the limits of normal use and to define the system reactions in case of unknown stress and unknown fault combinations.

- Testing of Complex Components

First, the design flow is given and described in an introductory paragraph. Second, all state of the art verification and validation steps are listed, based on the presented design flow. Third, possible hazards, e.g. reasons for common cause failures or single faults resulting in erroneous results will be identified. This will help to define a set of validation tests required for safety validation and reveal the eventual needs for additional tests.

6. Footnotes

[1] EN 954-1. Safety of machinery : Safety related parts of control systems. Part 1 : General principles for design

[2] Directive Machines 89/392 CEE modifiée 91/368 CEE, 93/44 CEE et 93/68 CEE.

[3] IEC 61496-1. Safety of machinery : Electro-sensitive protective equipment. Part 1 : General requirements and tests.

[4] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1 to Part 7.

[5] DIN V VDE 801 Appendix A2. Principles for computers in safety-related systems.