

# Implementing Functional Safety Requirements and Expectations in the Automotive Industry

Peter Löw, Roland Pabst and Dr Erwin Petry, KUGLER MAAG CIE

Innovations in the automotive industry are increasingly driven by electrical, electronic or programmable electronic systems. According to German car manufacturers, 80 to 90 per cent of them are implemented in electronics and software, hence the number and complexity of electronic control units (ECUs) in a car continue to increase.

As many of these control units include safety related functions, their development becomes more challenging, requiring additional process steps to meet safety goals and to provide evidence that these goals have been achieved. In a globally competitive environment, it is essential to implement the safety requirements in an efficient and effective way while maintaining the speed of innovation. In such an environment a process performance improvement program based on process reference models like CMMI® or Automotive SPICE™ can help improve both safety and efficiency of development.

## Freedom from unacceptable risk

Safety is freedom from unacceptable risk. Functional safety is part of the overall safety that depends on product functions operating correctly. Society, customers and govern-

ments have high expectations regarding the prevention of accidents and the reduction of risk to a tolerable level.

The December 2001 Directive 2001/95/EC of the European Parliament and Council on general product safety has by now been implemented in national laws, for example, the Equipment and Product Safety Act – GPSG in Germany<sup>1</sup>. This act says that a product satisfies safety requirements if it has been manufactured according to a released safety standard, like IEC 61508. The burden of proof is with the distributor or manufacturer, as he is liable for damages caused by non-safe products. The IEC 61508 safety standard is generic. Area specific standards like the ISO WD 26262<sup>2</sup> for Automotive, are derived from it.

## Derived standards

Both standards, IEC 61508 and ISO WD 26262:

- Define requirements regarding all phases of the safety lifecycle from concept definition and realisation to decommissioning
- Use safety integrity levels (SIL/ Automotive SIL) to specify the safety requirements.

SIL is a discrete level (one out of a possible four) where Level 4 consti-

tutes the highest level of safety integrity, and Level 1 the lowest. In the automotive industry SIL 1-3 are used.

## Steps in the safety lifecycle

Safety lifecycles, as defined by IEC 61508 and ISO WD 26262, start with a concept phase that includes a hazard and risk analysis regarding the new functions to be developed. The result of this analysis is a safety integrity level (SIL) assigned to each new function.

Development of functions with associated safety requirements (SIL ≥ 1) will be managed according to the requirements imposed by the applicable safety standard. Other, non-safety related functions (SIL = 0) will be implemented according to the established "standard" process of the company.

## Requirements imposed by the safety standard

IEC 61508 defines requirements with respect to:

- Planning and management of activities related to functional safety
- Hardware and software architecture of the safety related system depending on the SIL (eg, redundant processors, fault handling)

- Processes for risk analysis design, development, verification and validation
- Methods and techniques to be applied depending on the SIL level (eg, walkthroughs, inspections, diverse programming, error detecting codes, black box testing, error seeding)
- Functional safety assessment (providing evidence).

Other than CMMI or Automotive SPICE, the safety standards specify both "what to do" (processes to be applied) and "how to do it" (methods and techniques to be applied). Some of the processes required by the safety standard are not covered by the process models CMMI or Automotive SPICE.

All safety requirements mentioned above are to be satisfied for each safety function. Descoping can result in non-safe products leading to damage to the health of people, a high commercial risk for the company, and even penalties for persons responsible.

#### Efficient implementation

Adequate analysis, design and planning in the early phases of the safety lifecycle are prerequisites for an efficient and effective implementation of safety requirements.

Proper hazard and risk analysis, as well as adequate design of the hardware and software architecture, prevent costly redesigns and delays in later phases. In time, selection of suitable methods and techniques supports detection of errors early enough during the development lifecycle to avoid costly and time-consuming corrective actions in later phases, or even recalls.

#### CMMI or SPICE maturity models

Process improvement approaches based on maturity models like CMMI or SPICE facilitate dealing

with the implementation of requirements imposed by the safety standards. There is no need to reinvent the wheel; established processes can be reused with slight adaptations or extensions, eg:

- Requirements Management (RM) dealing with both non-safety related and safety related requirements
- Configuration Management extended for safety related work products (e.g. results of the hazard and risk analysis).

What is needed is a gap analysis prior to the start of the development phase to identify any required extensions or adaptations. Safety management activities in the early concept phase of the safety lifecycle are not supported by the SPICE or CMMI processes. A safety manager needs to be assigned to set up a safety plan and define the required processes in co-operation with the project team.

#### Reduced risk strategy

Safety and commercial risks can be reduced by applying the required processes, methods and techniques. Efficiency can be increased by setting the focus on the early safety lifecycle phases, thus avoiding costly rework in later phases. The standard process of the company needs to be extended by process steps and methods as imposed by the applicable safety standard. Adequate safety management, including defined interfaces and communication between OEM and suppliers, and involvement of subject matter experts in the hazard and risk analysis, prevent failures like this the one described below.

#### Electrical parking brake failure<sup>3</sup>

What happened? The electrical parking brake was released

although the mechanical handbrake had not been applied and the driver had left the bus. The operating manual instructs the driver to set the handbrake before leaving the bus. The author of the newspaper article doubts that this simple instruction in the operating manual is a good safety concept and proposes to implement an adequate technical solution. ■

#### For more information, contact:

**KUGLER MAAG CIE GmbH**

**Leibnizstrasse 11**

**D-70806 Kornwestheim**

**Tel: +49 7154 807 210**

**Fax: +49 7154 807 229**

**Email: [safety@kuglermaag.com](mailto:safety@kuglermaag.com)**

**Web: [www.kuglermaag.com](http://www.kuglermaag.com)**

#### Notes

- 1 "Gesetz zur Neuordnung der Sicherheit von technischen Arbeitsmitteln und Verbraucherprodukten", Artikel 1, Geräte – und Produktsicherheitsgesetz – GPSG. Bundesgesetzblatt Jahrgang 2004 Teil I Nr. 1, Bonn, January 9, 2004
- 2 ISO WD 26262 is not yet released. The IEC 61508 is the applicable generic standard, and products are assessed against it. ISO WD 26262 can help with the interpretation of the generic standard in the automotive context.
- 3 Petersen, Michael: "Bushersteller müssen eine technische Lösung finden" (Coach manufacturers must find a technical solution), in: Stuttgarter Zeitung, June 2, 2007.