

The application of IEC 61508 in the automotive industry

Ekkehard Pofahl
Ford Research & Advanced Engineering, D

Abstract

The generic standard IEC 61508 was developed to improve functional safety aspects of all electrical, electronic and programmable electronic safety-related systems (E/E/PES, abbreviated EEPES for the rest of the paper). Unfortunately the lifecycle model of IEC 61508 does not fit for cars. Many individual methods, procedures and requirements of IEC 61508, however, are targeted against generic EEPES equipment and many of them are already used in the automotive industry to guarantee functional safety for cars. These methods are considered to be included and refined in an upcoming automotive standard for functional safety. This derivative of the IEC 61508 will be prepared by the automotive companies, the automotive suppliers and technical service companies (German TUVs).

Introduction

Automobiles have been built since more than 100 years and left their mark on all modern societies. The first automobiles needed electric aggregates mainly to ignite the explosive gasoline/air mixture. Later lamps and electric windshield wipers were added to the electric system. Ever since, electric and electronic devices entered and now dominate the function of the car. The very well known EEPES systems ABS and airbag were luxury features some years ago and had to be purchased separately for a significant amount of money. Now ABS and airbag systems have been reduced in price because of mass production and are included in almost every modern car. They improve the overall road safety significantly by either preventing accidents or lowering the impact to passengers in the case of accidents.

The following paper describes the areas, which must be covered by a future standard for functional safety of EEPES systems.

Electric/Electronic/Programmable Electronic in Automobiles

The percentage of EEPES in a modern automobile is steadily increasing, both in function and in value. The increase touches all functional elements. To name the most known ones :

- Engine management,
 - Traction Control System (TCS),
- Energy management,
- Brakes,
 - Anti-Blocking System (ABS),
 - Electronic Stability Program (ESP),
- Lights,
- Suspension,
- Advanced Driver Assistance Systems (ADAS),

- Adaptive Cruise Control (ACC),
- Collision Avoidance Systems,
- Navigation System,
- Stability Elements,
- Window Lifter,
- Climate Control,
- Heating Control,
- Multimedia,
- Comfort Elements (e.g. seat adjustment, personalization),
- Security (Anti-theft “Wegfahrsperre”, alarm-devices, locking).

Former cars had electrical systems only. Modern cars make massive use of programmable electronics. Cars with more than 50 microcontrollers are not rare. Specific engineering skills are required to combine the vehicle’s sub-systems (“Distributed Systems”) to a network in a way, that functions do not interfere with each other and are available all the time.

Robustness

Robustness is defined as the ability of a technical system to keep the designed function even in the case of misuse, under harsh environmental conditions and failures of accompanying device. Because of different user profiles, under which a automobile is driven, robustness of EEPES is essential for the safety of any car.

Robustness is also a key element in today’s EEPES. Because the many different system suppliers, the individual elements must be robust against malfunctions of connected elements. For example it is not acceptable, that a brake system does not work because the data from the engine control system is missing or out of specification. Every module must maintain its designed function and work in the designed fashion.

Software

Other than the rest of the car, most software elements are hidden from the direct view of the driver. Software is experienced by the function, the software performs. Software adds many new possibilities to a modern vehicle. One of the most interesting feature is the method of permanent diagnostics for the components of the car.

Self Checks and Diagnostic

Traditional electric and electronic systems had to be checked on a regular basis to make sure, the intended function of a module is still given. By implementation of diagnostic software, these checks can be done on an automatic schedule without having to visit a workshop. In the case of malfunctions the driver gets immediate notification, so he can replace defective parts. In case of more safety related function, the diagnostic leads to a degraded or no function in the case of an detected error. A typical degraded mode would allow the driver to drive home very slowly to avoid expensive towing. Higher speeds, which could cause accidents, are impossible. This mode is called “limp home”.

Classifications

With regard to functional safety the different EEPES of a car have to be considered differently. Typically in such case all applications are divided into classes with equal requirements with regard to the differentiation criteria. These classifications have not been done in an uniform approach so far with regard to functional safety for automotive use. It is evident, that an ABS system belongs into a higher safety class than window lifter electronic.

It is expected, that also for automotive use 4 classes/levels will be created. The proposed categories most probably will be called ASIL (Automotive Safety Integrity Levels). Functions and aggregates falling into these classes then will have to follow different levels of requirements, resp. sets of requirements. It is also expected, that classification rules will be different from the generic approach of IEC 61508.

Risk graph

Many types of risk graphs are described in the literature. Also in the IEC 61508 the risk graph is described as one approach to determine a distinctive safety integrity level (SIL). The method itself is straight-forward. There are, however, some uncertainties. One of the biggest concerns with regard to common use is the use of qualitative questions to determine a risk level.

The working committees within the automotive industry are preparing an alternative risk graph, which should give a more exact category, when applied to EEPES of an automobile. This method should lead to the same ASIL category when applied by different parties.

Fail safe behavior

One of the best proven principles for maintaining safety is the fail-safe principle. This behavior leads in the case of an failure automatically to a safe situation, without operator, resp. driver, intervention.

A car is a device, where the safe state is a still standing car, which is not on a public road or on a motorway. The removal of power or stalling the engine in the case of a failure is no option for a driving car. A car is a typical fail operational system. After a failure the system functions must be maintained as long as possible, and the driver has to be alarmed about the failure. The driver then has to reach a safe state as soon as possible to be able to mitigate the problem.

One of the most safety critical systems is the brake system. The brakes are needed to remove the kinetic energy from a car. Brake systems are built with two redundant brake circuits to make sure, the car can be brought to stand, if one brake circuit fails.

Fail safe behaviors can also be engineered to other systems of the car. Either by physical redundancy, or by logical redundancy by means of diverse control and supervision devices implemented in software.

Safety

The safety systems of a car can be subdivided into systems for active and for passive safety. Many systems today are targeted for passive safety. They minder the consequences of traffic

accidents. Big improvements in this area can be observed in society. Despite of constantly rising traffic, accidents with injuries or fatalities have decreased dramatically over the last years. Even more improvements are expected from systems for active safety. One of the most prominent examples of active safety are “collision avoidance” devices.

Active safety systems are intended to help avoid collisions before they happen. They support a driver by warning of potential or imminent critical situations. There are many instances where the car of the future might be able to automatically decelerate, brake or swerve, to avoid a collision or reduce and restrict its effects. Active safety systems must be developed with the sole intention of providing the driver with meaningful support.

The validation and verification of the functional and system safety of today’s cars is reached by thorough assessment of all components and of the complete car. Also crash tests prove the safety of a car for the passengers.

The assessments and investigations are done by simulation, hardware in the loop (HIL) testing, prototypes and fleet trials. Typical methods also include Failure Mode & Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Markov Models. It may be interesting to note, that the automotive industry is one of the most prominent drivers for the international standard for a common FMEA approach.

Software Safety

With software being the architectural element, which determines the behavior of electronic hardware, aspects of software safety have to be considered in addition to the traditional safety aspects.

Currently software is assessed according to SPICE/CMMI rules, which shall guaranty the quality of software development. The individual assessment of system safety functions and diagnostic routines is mainly done during the prototype and fleet evaluation phase. Added to these methods simulation helps to validate the safe design of software control algorithms. By assessment and refinement of the software development cycle also higher levels of software safety are reached.

The installation of automatic hardware in the loop (HIL) verification environments is also used to verify the safe behavior of the used control software.

The IEC 61508 suggests the use of certified tools for software development. One of the most important tool in software generation are compilers, which translate control routines of automotive engineers into executable binary code. Because of high innovation cycles within the software industry there are no fully certified compilers or autocode generators available on the market.

To overcome this problem manual code validation and very sophisticated programming and quality rules have been introduced. The most known set of rules in this area are the MISRA guidelines for programming in “C”. These rules aid validation of safety critical software programs, in addition to validation suites for compilers. For graphically developed control algorithms with autocode generators at current all measures for hand coded “C” have to be used as minimum measures. In addition, to mitigate the specific complexity of automatic code generation, a set of additional tools is being developed at the moment.

Besides these straight forward methods university cooperation contracts are in place for new, innovative validation and verification methods for safety critical software. One project is to transform the very well proven method FMEA into the software development environment.

Automotive standards

All automobiles require an investigation, if all legal requirements for use on public roads are met. This process is called homologation. The regulations to be followed cover all types of passenger safety and environmental compliance and are guidelines of the European community and the ECE – rules.

ECE

Some years ago homologation had been necessary for each individual country within Europe, because in the countries different rules and laws were effective. Nowadays in the European community homologation for one country is valid also for the other countries of the European union. This simplifies the homologation for one of the biggest markets for automobiles.

MISRA

MISRA is the abbreviation for “Motor Industry Software Reliability Association”. The guidelines and papers which are published by the members of MISRA are no standards, which legally must be observed. They are, however, high quality guidelines, which are considered by most automotive companies.

The MISRA guidelines provide important advice to the automotive industry for the creation and application of safe, reliable software within vehicles.

The Guidelines are intended for use by all those involved in the creation, procurement and support of vehicle based software.

Users may be within vehicle design and manufacturing companies, component suppliers, development tool suppliers and diagnostic equipment suppliers.

Uses for the MISRA Guidelines include:

- guidance for creating contracts and specifications for software procurement
- an introduction to issues of automotive software reliability
- a basis for training requirements within the automotive industry
- guidance for company quality procedures
- guidance for management on resource requirements
- a basis for assessment

- a foundation for a standard.

Special guidance for automotive software is needed because there are important differences between software and other forms of automotive engineering and components. There are also differences between automotive software applications and applications in other industrial sectors.

Outlook

- The systematic safety approach as described in IEC 61508 is identified as helpful for vehicle electronics development.
- The IEC 61508 describes valid methods to guarantee functional safety, but can not be used in general for automotive applications.
- At the moment an automotive derivative standard from IEC 61508 is in preparation.
- Until an automotive derivative is finalized, the applicable parts of IEC 61508 and of the MISRA guidelines will be interpreted, adopted and used for automotive electronics.

References

IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems (<http://www.iec.ch/>)

"Development Guidelines for Vehicle Based Software", MISRA, 1994
(<http://www.misra.org.uk/>)

ECE Regulation No. 13, "Uniform Provisions concerning the Approval of Vehicles of Categories M,N and O with regard to Braking", 2003,
(<http://www.unece.org/>)