



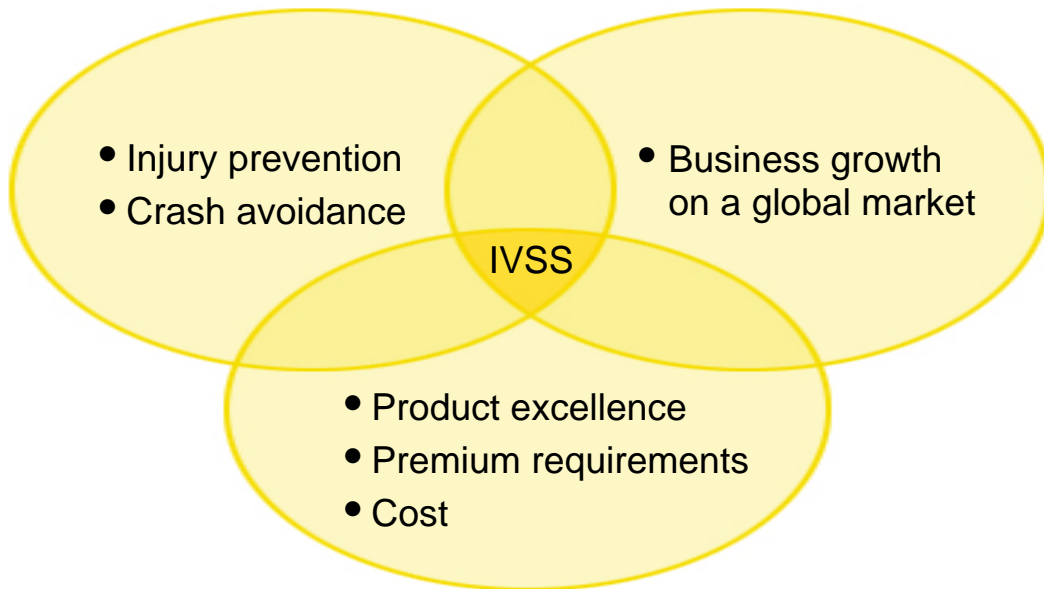
AutoVal –
Validation methods and safety requirements for
safety-related automotive systems

IVSS Project Report

The IVSS Programme

The IVSS programme was set up to stimulate research and development for the road safety of the future. The end result will probably be new, smart technologies and new IT systems that will help reduce the number of traffic-related fatalities and serious injuries.

IVSS projects shall meet the following three criteria: road safety, economic growth and commercially marketable technical systems.



Three interacting components - for better safety, growth and competitiveness:

The human being

Preventive solutions based on the vehicle's most important component.

The road

Intelligent systems designed to increase security for all road users.

The vehicle

Active safety through pro-active technology.

Title of the report: AutoVal – Validation methods and safety requirements for safety-related automotive systems

Author: Jan Jacobson, SP

Reference number: xxx

Publication date: 27 April, 2007

Contact person: Jan Jacobson, SP (email jan.jacobson@sp.se)

Table of contents

1. Background	5
2. Automotive embedded systems	6
2.1. Increased functionality and authority	6
2.2. Increased complexity	7
2.3. Dependability	8
2.4. Safety-related functions	9
3. Intelligent vehicle safety systems	11
4. Conclusions	12
5. Technical reports	13

1. Background

Increased functionality, increased complexity and dependability requirements must be combined for automotive electronics. Systematic work according to an overall safety life cycle will be essential for developing systems with adequate functional safety. The life cycle has to address the concept, the risk analysis, the system development, the hardware development and the software development.

The aim of the AutoVal project is to show how safety requirements can be specified and how safety can be demonstrated. Practical experience and techniques are prioritised.

Partners of the AutoVal project are Haldex, QRtech, Saab Automobile, SP Technical Research Institute of Sweden and Volvo AB. The following researchers and engineers have participated in the AutoVal project:

Mr Henrik Aidnell, Saab Automobile

Mrs Sabine Alexandersson, Haldex Brake Products

Mr Joacim Bergman, QRtech

Mr Per-Olof Brandt, Volvo

Mr Robert Hammarström, SP

Mr Jan Jacobson, SP (project manager)

Dr Lars-Åke Johansson, QRtech

Dr Henrik Lönn, Volvo

Mr Carl Nalin, Volvo

Mr Anders Nilsson, Haldex Brake Products

Dr Magnus Gäfvert, Haldex Brake Products

Mr Josef Nilsson, SP

Mr Lars Strandén, SP

Mr Jan-Inge Svensson, Volvo

Mr Andreas Söderberg, SP

2. Automotive embedded systems

2.1. Increased functionality and authority

More functions will be developed for road vehicles. The number of safety critical and safety related automotive embedded systems is large and will grow even larger.

Many of the functions of a modern car or truck are realised using embedded programmable electronic systems. Nearly all the recently developed functions in vehicles would be impossible without software and electronics. Electronic control units (ECUs) are embedded all over the vehicle. Drivers and passengers are expecting the electronic systems to provide at least the same reliability and availability as the mechanical parts of the vehicle. Most drivers are not even aware of which vehicle functions depend on embedded systems.

There are safety-related parts of the vehicle where a failure of control would cause a hazardous situation. An example of such a system is engine control which must not deliver unexpected engine torque. An unexpected low torque could be hazardous e.g. in an overtaking situation. An unexpected high torque might cause sudden acceleration and loss of control of the vehicle. Other examples of safety-related control are door locks, electronic stability control (ESC) and battery management in hybrid vehicles.

Active safety systems require "intelligence" implemented by programmable electronic systems. The correct employment of an airbag system depends on the correct processing of sensor signals. An airbag is expected to blow when needed at a crash, but also expected not to blow when it should not. Any failure will be safety-related.

A large number of active safety systems can be expected in future vehicles. Advanced airbag systems, electronic stability systems, lane departure warning systems, brake assistance systems and adaptive cruise control systems are already commercially available. Future active safety systems may include collision avoidance by forced steering, night vision systems and brake-by-wire systems.

There are also embedded systems that implement functions with minor safety importance. Malfunction of infotainment systems in the vehicle will be a nuisance, but is unlikely to be safety-related. Failure of automatic climate control systems will reduce the comfort for the driver, but will not be safety-related in the short time aspect.

2.2. Increased complexity

Automotive systems are becoming more complex. This complexity has to be mastered.

More computing power and larger memory capacity enhance the capability in an automotive embedded system. Performance in computing systems has become affordable also for the cost-sensitive automotive industry. The increased performance makes it possible to develop more complex systems.

The different embedded systems of a road vehicle are not isolated. The ECUs are connected together in vehicle communication networks, and data is exchanged between them.

The design principle has been to use one ECU for every function in the vehicle, and then make the ECU work together in a federated way. This will no longer be feasible as the number of functions grow continuously. New functions will have to be distributed over existing ECUs. New hardware units cannot be introduced with every new function. This will lead to increasing complexity. The partitions of an ECU are to be sufficiently isolated otherwise the functions will interfere with each other. All the ECUs performing a part of a function have to be available as "members" of the function. This also increases the complexity.

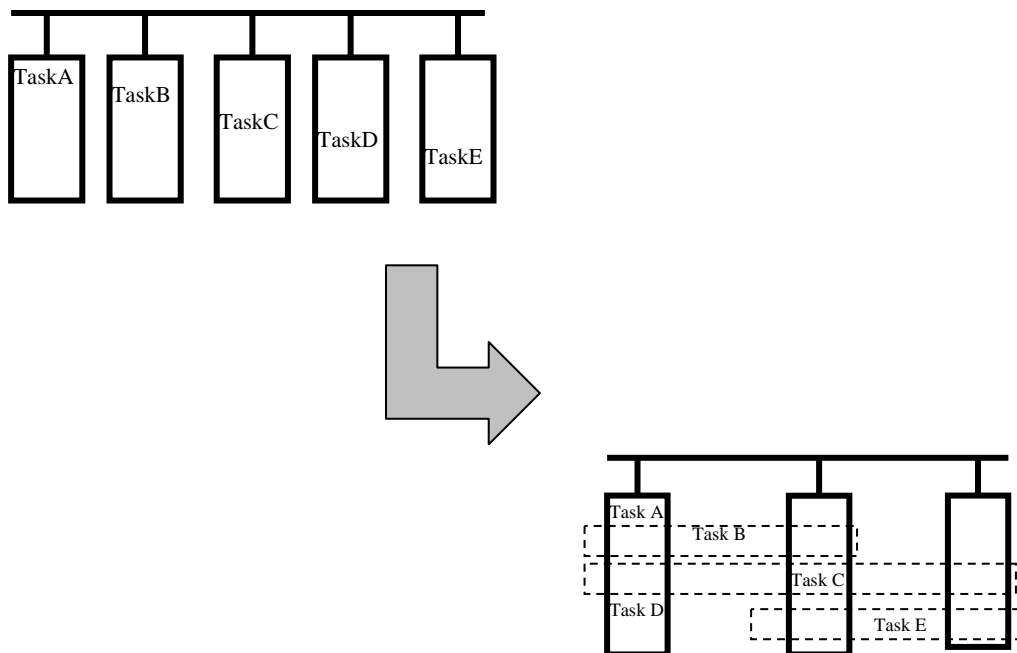


Figure 1. Complexity is increased by distribution of tasks over several nodes.

Future systems for communication vehicle-to-vehicle and vehicle-to-infrastructure will also increase the complexity. Transmission and reception of data to be used in the embedded functions of the vehicle must be handled with care. Open systems may in many situations be hard to combine with dependability.

2.3. Dependability

The safety requirements must be unambiguous, and there must be methods to validate functional safety.

There are many different risks in technical systems, mechanical risks, chemical risks, electrical risks, explosive risks etc. When we consider a system, a device or a machine as safe we mean that all these risks are sufficiently low. Safety means that there are no unacceptable risks for physical damages or injuries on health neither directly nor indirectly as a result of damages on property or environment.

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. The term "safety validation" in this report means the activities to demonstrate that the needed functional safety has been achieved. Functional safety should not be mistaken for other kinds of safety aspects such as electrical safety or safety in explosive atmospheres. Neither safety nor functional safety can be determined without considering the system as a whole and the environment with which it interacts.

Dependability is a term which summarizes several attributes:

- availability
- reliability
- safety
- confidentiality
- integrity
- maintainability

The concept of "dependable automotive systems" indicates that the system should not only be safe, but also cover the other dependability aspects.

It is not trivial to show that a complex system actually is suitable for its intended use. Careful risk analysis must be made already from the beginning of the development. Every step of the realisation must be confirmed by verification. At the end of the development, there shall be an overall safety validation to demonstrate functional safety.

This report addresses validation of dependability and functional safety. Other safety aspects such as environmental stress, electromagnetic compatibility and electrical safety are not in focus. Additional validation methods should be applied to cover also those aspects.

2.4. Safety-related functions

Development of automotive embedded systems requires handling of safety as an integrated part of the control functions.

Traditional safety functions are designed with the dedicated purpose to reduce a risk in the system. A high-pressure relief valve of a boiler in process control is a good example of a safety function. The valve has the task to open if the pressure of the boiler exceeds the limit and the risk of an explosion is eminent. Controls in the process industry often combine sensors, programmable electronic systems and actuators to build safety functions. Temperature alarms, level gauging and flow control are examples where the safety function is easily distinguished from the basic process control system. (See figure 2.) This is often not the case in automotive control.

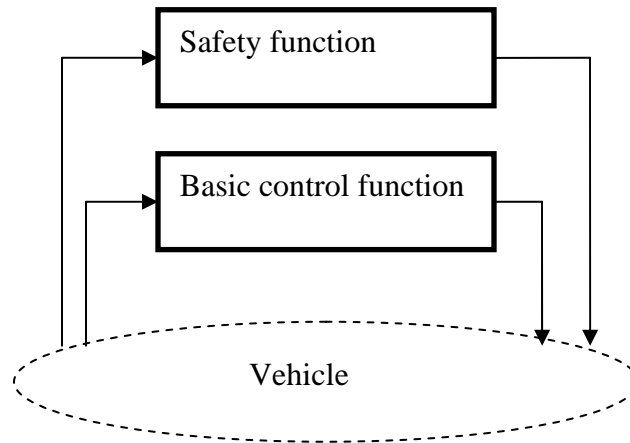


Figure 2. The safety function is well separated from the basic control functions

Many of the functions of a road vehicle are of minor importance to the safety of the driver and the passengers. Such “basic control functions” can be exemplified by the continuous charging of the battery, the engine temperature control and the illumination of the instruments on the dashboard. But it is possible to imagine situations when also these functions may affect safety.

What makes automotive electronics special is that almost every function of the car is to some extent safety-related. The switching on of the headlights is not of primary importance to safety. But what happens if both headlights are unintentionally switched off during night driving? The shifting of gear in reverse is uncritical in most driving situations, but will be safety-related when you have to back out of a dangerous area.

Few functions are safety functions in the original meaning, i.e. functions specifically designed to handle a hazardous situation. Seat belt pretensioners and airbags are examples of safety functions.

The advanced driver assistance systems have the safety-related functions as integrated parts of the system. An example is the electronic stability control (ESC) which operates the individual brakes of the wheels to improve stability. Incorrect operation of the brakes is safety-critical. (See figure 3.)

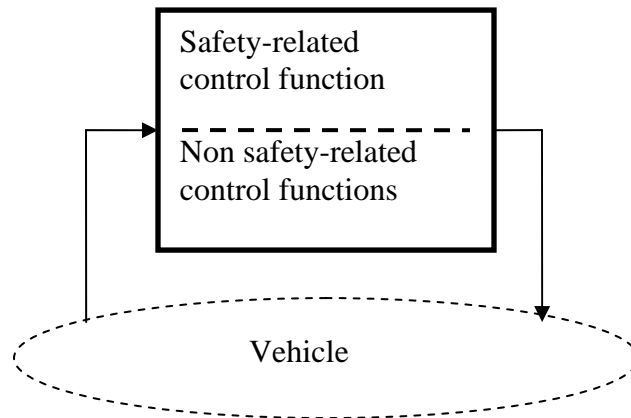


Figure 3. The safety aspects are integrated in the control function

3. Intelligent vehicle safety systems

Road safety is enabled by dependable embedded systems. Safety-related vehicle control (e.g. brake control, engine control) is realised by embedded control systems which have to be dependable. Also the Advanced Driver Assistance Systems (e.g. Lane Departure Warning, Adaptive Cruise Control) requires the electronic systems to perform in a safe and reliable way.

Guidelines and standards for functional safety are presently under development. The best known examples are the international standard IEC 61508, the international work item for draft standard ISO 26262 and the Safety analysis guidelines issued by the British organisation MISRA. There is a need for practical interpretations and dissemination of knowledge.

The AutoVal project supports road safety by implementing methods for specification of safety requirements and development of methods for verification and validation.

The **economic growth** of the automotive industry in Sweden is much depending on the strong international safety reputation of the Swedish brands. The mechanical protective structures, the seat belt and the air bag system are passive safety systems handled by Swedish OEMs and suppliers. The automotive industry has to be equally strong on active safety systems as it has been for passive safety systems.

The AutoVal project supports development of safety-related automotive electronic systems, and active safety systems.

Commercially marketable technical systems (“Intelligent Vehicle Safety Systems”) are under development at the AutoVal industrial partners. The IVSS research project has been running in parallel to the product development.

The AutoVal project supports the safety requirements specification and the safety validation of the technical systems under development at the AutoVal partners.

The AutoVal project has managed to merge information from standards and guidelines with practical experiences of development engineers. Conclusions have been drawn on techniques and measures for development of safety-related automotive systems. A summary of methods for verification and validation of safety was produced. Verification and Validation in model driven development was also developed. The intention is to give practical examples and background to the subject raised in other publications. The intention is to supplement, not to replace, other sources of knowledge.

4. Conclusions

An internationally accepted framework for functional safety in road vehicles is needed.

The use of embedded systems in automotive applications will continue to grow. There is presently no international guidelines accepted by the automotive industry. Company internal documents for risk analysis and functional safety exist. The standard IEC 61508 exists since a couple of years, but has not been accepted by the automotive industry. The development of standard ISO 26262 for functional safety of road vehicles is championed by the automotive industry, but will not be established before 2008. Safety guidelines exist from independent organisations such as MISRA.

It is difficult to work with parallel frameworks available. Future establishment of the most important functional safety standard for the automotive industry is expected to solve this. The different use of terminology causes confusion. Safety engineers, software developers, embedded systems engineers and tool vendors from different organisations have to reach a common understanding on definitions and use of words. Also this is expected to be supported establishing of a common standard.

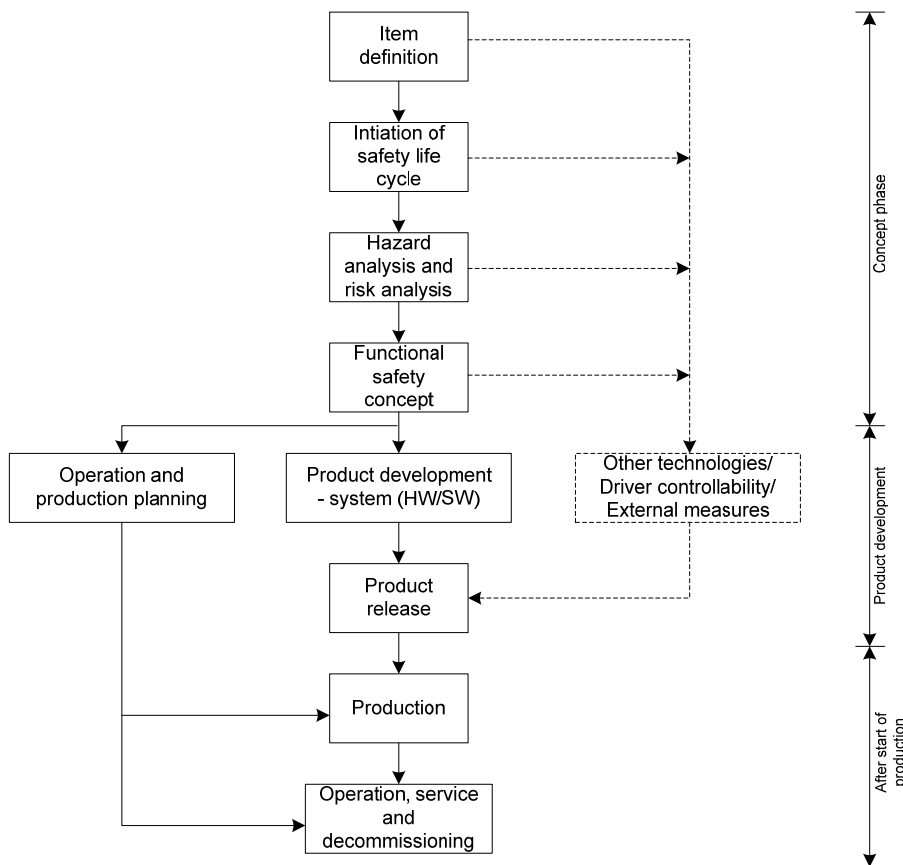


Figure 5. The overall safety lifecycle (draft standard ISO 26262)

It is possible to specify functional safety requirements.

Specification of functional safety goals requires focus on functionality. The development engineer often has knowledge of too many technical details from similar embedded systems. It is often difficult for the engineer to omit the technical implementation and focus on the safety-related functionality. Means to assist this implementation-independent analysis and design are necessary, such as model-based design.

It is possible to specify a technical safety concept.

The allocation of the identified functionality to different parts of the embedded system is part of the technical safety concept. Specification of the safety integrity level, and techniques and measures to use are also necessary. A sound architecture is important to a safe and cost-efficient system, and is thus an important part of the technical safety concept.

Safety validation is possible.

Validation requires the use of several validation methods to show functionality, hardware safety integrity and software safety integrity. The validation plan should include different methods for different aspects, and the validation activities should be planned to form an integrated part of the development work. Calculation of electronic hardware reliability is new to many automotive engineers. Tools to support reliability calculations are available. It may be hard to see how faults propagate and how they affect the overall functionality of a complex system.

This report is hoped to be read and discussed among developers of automotive embedded systems. International standards are not intended to be read as textbooks. The text and the examples of this report can be read to explain some of the concepts and issues. It should also stimulate the debate on concepts used for developing automotive systems.

5. Technical reports

The project has released the three publicly available technical reports at www.sp.se :
Jan Jacobson, Andreas Söderberg,
Lars-Åke Johansson QRtech, Henrik Lönn Volvo Technology
Safety requirements and validation methods for safety-related automotive electronics
SP Report 2007:13

Lars Strandén, Andreas Söderberg, Jan Jacobson, Josef Nilsson
Methods for Verification and Validation of Safety
SP Report 2007:14

Lars Strandén, Josef Nilsson, Henrik Lönn Volvo Technology
Model Driven Software Verification and Validation
SP Report 2007:15

IVSS partners:



Postal address: IVSS/Swedish Road Administration, SE-781 87 Borlänge, Sweden
Street address: IVSS/Swedish Road Administration, NAVET, Lindholmspiren 5, Gothenburg, Sweden
Phone: +46 (0)771 119 119
ivss@vv.se
www.ivss.se