System safety in hybrid and electric vehicles

Dr David D. Ward
MIRA Limited
Watling Street, Nuneaton, CV10 0TU, UK
david.ward@mira.co.uk

Abstract

Road vehicles have an increasing reliance on electronic systems to control their functionality and to deliver the feature and attribute demands made by manufacturers, legislators and consumers. This trend is particularly evident in the new generation of more energy-efficient vehicles that includes hybrid vehicles and full electric vehicles. The architectures of these vehicles are characterized by a greater degree of integration and interaction between the systems, as well as the introduction of new types of system with unique potential failure modes. As a result, system safety is a central part of the design and implementation process for these vehicles.

In this respect a new standard, ISO 26262 "Road vehicles — Functional safety" is in preparation. It sets out requirements for managing functional safety, hazard analysis and risk assessment, and the development and verification of systems, hardware and software. Nevertheless, in hybrid and electric vehicles functional safety is only one part of the overall process of system safety, which encompasses other domains such as electrical safety and crashworthiness.

This paper will give a brief introduction to the concepts and challenges of system safety when applied to such vehicles, including a discussion of the role of ISO 26262 and some of the key principles of that standard, including the concepts of automotive safety integrity level (ASIL), safety goals and safety concepts. The implications of the standard on emerging vehicle technology will also be examined. Finally, the need for an holistic approach to system safety in such vehicles will be presented.

Keywords: Functional safety, electrical safety, hybrid vehicles, electric vehicles, autonomous vehicles, UGV, ISO 26262.

1 Introduction

Modern road vehicles have an increasing dependence on electronic systems to control their functionality and to deliver the demands made by manufacturers, legislators and consumers for safety, environmental efficiency, comfort and brand differentiation. This trend is seen in particular focus in the new generation of more efficient vehicles, typically called "low carbon" vehicles. Examples of low carbon vehicles include hybrid vehicles and electric vehicles. Low carbon vehicles are characterized by a greater degree of integration and interaction between the electronic systems, as well as the introduction of new types of electronic system. As a result, system safety is a central part of the design and implementation process for these vehicles, and continues to grow in importance.

2 Automotive system safety and functional safety

System safety uses the concepts of systems engineering and systems management in the processes of ensuring the safety of a product. In outline the process for addressing system safety takes the form of:

- A hazard analysis and risk assessment to identify the potential hazards associated with the system and the associated risk;
- The identification and implementation of measures to control, reduce or remove the risks, such that the residual risk associated with the hazards is at a defined acceptable level;
- A safety assessment to demonstrate that the risk reduction has been correctly identified and implemented. The safety assessment is frequently conducted by a party with a degree of independence from the developers of the system.

It should be emphasized that system safety is a very wide area. In the automotive context, system safety covers many of the traditional safety disciplines as well as the new safety challenges introduced by innovative systems. Safety aspects in a vehicle have traditionally focused around crash safety. Safety measures can for example be categorized as "active safety" (measures which help prevent a vehicle from being involved in an accident or which can reduce the severity of an impact) and "passive safety" (measures which help reduce the risk of injury to the occupant if the vehicle is involved in an accident). More recently, the deployment of advanced electronic systems has lead to the introduction of terms such as "integrated safety" (EASIS 2011) to describe more wide-ranging and integrated approaches to safety.

These overall trends towards the greater use of electronic systems to achieve safety serve to emphasize the importance of the inherent safety of these systems. Frequently these systems involve a higher degree of integration of the systems, and a higher degree of interaction between them. Thus, taking a systems-led approach to the design and development of these features is essential, and this philosophy should also be reflected in the approaches to the safety of the systems.

Furthermore, in low carbon vehicles further levels of integration and interaction are introduced, as well as novel systems that have their own safety aspects.

- In low carbon vehicles, there is a trend away from imperative control of the functions to goal-based control. In a traditional vehicle, for example, the driver directly commands the engine and brakes to speed up or slow down the vehicle. In a typical hybrid vehicle, the driver requests that the vehicle speeds up, and the hybrid system controller decides whether the required torque should come from the internal combustion engine, or the electrical machine, or both.
- Hybrid and electric vehicles introduce higher voltage components, meaning that electrical safety (that is, preventing human contact with potentially fatal levels of voltage and/or current) is a new issue to be considered.
- Linked to this, the size and location of the components (particularly the traction battery) require additional considerations in the crash engineering of the vehicle.

These areas cannot be considered in isolation from each other. In the example of electrical safety, part of the necessary level of safety is achieved though design measures to prevent contact with the hazardous voltage, such as specially-constructed connectors that prevent direct contact with conductors. However, part of the safety is also achieved through electronic systems, such as a fault monitoring system that checks whether there is a leakage of hazardous voltage onto the vehicle chassis and shuts down the higher voltage system if so. Thus, to achieve the necessary level of electrical safety, correct functionality of an electronic system is also required.

The discipline of ensuring that safety is maintained through the correct functionality of electronic systems is known as "functional safety". However the foregoing discussion serves to emphasize that functional safety is a subset of system safety. Whilst the state-of-the-art practices for functional safety are based on system engineering principles, in the modern vehicle an overall approach to the safety of the vehicle treating the entire vehicle as a system is clearly necessary.

3 An automotive standard for functional safety — ISO 26262

The discipline of functional safety is generally a mature one. A particular milestone is that work started in the early 1990s on what has now become the international standard IEC 61508 (IEC 2010). First published in 1998, the standard has recently been updated to a second edition. Although originating in the industrial process control sector, IEC 61508 has become a generic standard and the baseline standard for any industry to develop its own requirements for functional safety. As early as 1994, an automotive interpretation of the requirements of this standard was published by a UK consortium (MISRA 1994) and IEC 61508 has also been applied directly to automotive systems.

Nevertheless, there are some key challenges in applying IEC 61508 to road vehicle systems. Perhaps the most significant issue is that in IEC 61508, safety functions are considered separately from the control functions. IEC 61508 has the concept of the "equipment under control" with its own control systems, and designated separate safety functions are added where necessary to achieve the required level of safety. In contrast, in traditional automotive systems the safety functionality is rarely distinguishable from the normal functionality. For example, in an electronic engine controller, the required functionality is to produce torque in response to driver demands; however if this torque is produced incorrectly this is potentially a safety issue.

Some further issues with applying IEC 61508 directly are discussed in (Ward 2008) and include:

- The principles for hazard analysis and risk assessment in IEC 61508 always require calibrating to the specific industrial application, and contrary to popular misconceptions IEC 61508 does not give a normative basis for this.
- The use of distributed development responsibilities in the automotive supply chain, including the relationship between vehicle manufacturers, major systems suppliers and the lower supply chain is not reflected in IEC 61508;
- Final safety validation for automotive systems is performed before release of a vehicle to volume production, often in conjunction with a statutory process such as "Type Approval" in Europe.
- Vehicles are not restricted to being operated in a specific location or restricted environment.
- The human is an important part of the control loop for vehicle systems, and so human reactions must be considered in designing systems. In this context it should be observed that compared to other industries, the operators of vehicle systems generally receive little or no training (either initial or ongoing) in the operation of the vehicle's safety-related systems. Therefore the reactions of an "average" human to perceived failures have to be considered.
- There is only a limited formal maintenance regime for automotive systems.
- There are few if any systems for collecting in-service data about incidents that are potentially attributable to safety-related systems.

From the foregoing discussion it is clear that an automotive-specific version of IEC 61508 should be developed. One example of such a standard is ISO 26262 (ISO 2010). ISO 26262 was developed against the background of the issues listed above and seeks specifically to address these.

Although currently in development and not due to be published as a full international standard until later in 2011, a public draft has been available since July 2009 and the standard has rapidly become established as representing "state-of-the-art" in the development of automotive electronic systems, particularly in Europe, North America and Japan.

4 Key concepts in ISO 26262

In this section, some of the key concepts of ISO 26262 are introduced; in particular:

- The safety lifecycle;
- Automotive safety integrity levels (ASILs);
- The processes for specifying safety requirements.

4.1 The safety lifecycle

In common with IEC 61508, ISO 26262 specifies a safety lifecycle to cover the essential requirements for achieving functional safety. The safety activities are divided into three main areas.

4.1.1 Management of functional safety

This subject is covered in ISO 26262 Part 2 and specifies requirements for overall safety management in an organization, including requirements for a safety culture within the organization and for competence management of personnel who will undertake functional safety activities. This Part further specifies the requirements for management of functional safety during the development of the item, including the need for appointment of a safety manager, the production of a safety plan for the functional safety activities, and the required confirmation measures. "Confirmation measures" are requirements for reviews of certain work products that have to be performed with a degree of independence from the persons responsible for generating the particular work product. These confirmation measures also include a requirement for an independent safety assessment at the highest ASILs.

4.1.2 Concept phase

This subject is covered in ISO 26262 Part 3 and specifies requirements for item definition, hazard and risk analysis, and the specification of the functional safety concept. These requirements are discussed further in the next two sections.

4.1.3 Development phase

This subject is covered in ISO 26262 Parts 4 to 9 and specifies requirements for the design, implementation and verification of the item. Part 4 in particular covers product development at the system level; whilst Parts 5 and 6 cover product development at the hardware and software level respectively. It is important to note that development of any item is led through Part 4, which includes the requirements for safety requirements specification at the top level of the design (see below) as well as the integration and safety validation. Parts 5 and 6 are concerned with the specific processes for designing and implementing hardware and software. Parts 4, 5 and 6 draw heavily upon the concept of the "V model" for developing systems.

4.2 Automotive safety integrity levels

A key requirement of ISO 26262 is the use of automotive safety integrity level (ASIL), which is defined as "one of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level". This is analogous to the concept of safety integrity level (SIL) in IEC 61508, with the following important differences:

- The 4 ASILs (A, B, C, D) of ISO 26262 do not map directly to SILs of IEC 61508. ASILs A, B and D are very approximately equivalent to SILs 1, 2 and 3 respectively; although there are some important detailed differences. There is no equivalent to SIL 4 in ISO 26262, and ASIL C represents requirements that correspond roughly to SIL 3 on the left-hand side of a "V" model and to SIL 2 on the right-hand side of a "V" model.
- ASILs do not contain any normative (i.e. "must do") requirement for probabilities. In contrast, IEC 61508 SILs have a normative probabilistic requirement, although IEC 61508 does acknowledge that in practice this can only be demonstrated in respect of the random failures of hardware. ISO 26262 does however specify optional probabilistic targets for ASIL, which are associated with the failure to achieve the safety goals (see below).

The ASILs are allocated through a process of hazard analysis and risk assessment. Such a process covers:

- Hazard identification — using a well-defined and structured process to identify the potential hazards associated with the item.
- Hazard classification — using three parameters to assess the risk associated with the potential hazards. The parameters are severity of the (eventual outcome of the) hazard, likelihood of exposure to the hazard depending on operational conditions, and the controllability of the situation by the driver. Each parameter is ranked on a subjective basis using qualitative classes. There are typically three or four classes for each parameter.
- Risk assessment — by combining the three parameters the risk associated with the hazard is determined. This is specified using ASIL, which is also the means of specifying the risk reduction requirements if all of the risk reduction is to be achieved through an electrical or electronic system. ISO 26262 does permit the risk reduction to be allocated to safety elements of "other technologies" but ASIL is not to be used for the purposes of this allocation.

4.3 Safety requirements specification

The specification of safety requirements in ISO 26262 is given at four levels:

- Safety goals, which are the top level statements of the safety requirements necessary to prevent or mitigate the hazards. Each hazard is required to have at least one safety goal. Crucially, the ASIL identified for the hazard is allocated to the safety goal, and all the safety requirements subsequently

derived from a safety goal are required to inherit this ASIL.

- Functional safety concept. This is the top level specification of functional safety requirements to fulfil the safety goal. At least one functional safety requirement is required for each safety goal. The functional safety concept can be created without knowledge of the system architecture.
- Technical safety concept. This is created during the initial design of the system, and refines the functional safety requirements into specific technical safety requirements that can be implemented, taking into account the system architecture. This step includes the allocation of technical safety requirements to hardware and software.
- Detailed hardware and software safety requirements. As the detailed hardware and software design progresses, the technical safety requirements are iteratively refined into specific requirements that can be implemented at the hardware and software level.

The safety goals and functional safety concept are specified during the "concept phase". Since the functional safety concept can be specified independently of any knowledge of the implementation of the system, this is typically viewed as being the responsibility of the developer of the item. In the typical automotive supply chain this is often the vehicle manufacturer. In contrast, the technical safety concept is developed during the "development phase" (Parts 4 onwards) and with knowledge of the system design. It is therefore often viewed as a supplier responsibility.

A key contrast with IEC 61508 can be seen here. In IEC 61508, SILs are related to assuring the reliability of safety functions. In ISO 26262, ASILs are related to assuring that the safety goals are not violated. This distinction reflects the fact that in traditional automotive systems, it is not usually possible to identify a "safety function" that is completely separate from the nominal performance of the system.

An example of the thinking behind the structure of the safety requirements in ISO 26262 can be seen in the "E-gas" concept that has been a standardized approach between some of the European vehicle manufacturers for many years (VDA 2004):

- A hazard of electronic throttle control is incorrect torque generation;
- The safety goal is to prevent incorrect torque;
- Part of the functional safety concept is to monitor the torque generated by the engine, compare it with the torque demanded by the driver through the accelerator pedal (as well as torque up/down requests from other systems e.g. cruise control, stability control), and limit torque if the delivered torque is significantly different from the demand.
- The technical safety concept specifies how this will be achieved, for example through hardware and software plausibility checks and redundant engine shutdown paths for both ignition and fuelling.

5 Implications for emerging technology

The previous sections have introduced ISO 26262 and demonstrated how it fulfils many of the requirements for a functional safety standard for the automotive industry. Nevertheless, the standard was developed against the background of the current generation of automotive electronic systems and may not be fully applicable to some emerging technologies. This is particularly the case in low carbon vehicles and autonomous vehicles.

5.1 Low carbon vehicles

A key difference between low carbon vehicles and conventional vehicles is the much greater level of integration and interaction between systems and functions. This paper has already argued that a systems-led approach to the safety of such vehicles is required, encompassing crash safety and electrical safety as well as functional safety. The overall system safety approach of identifying hazards and their associated risks, identifying the required risk reduction methods and confirming their correct implementation is equally applicable to any safety domain in the vehicle. It is therefore recommended that a unified approach be adopted, whereby the means of hazard classification in particular is not restricted to a particular technology. An example of such an approach can be found in the MISRA Safety Analysis guidelines (MISRA 2007), where an intermediate parameter of "presumed hazard risk" is used. Allocation between different means of risk reduction can be performed based on this parameter. For example, considering the hazard of "electric shock during maintenance" the MISRA risk parameter could be used to determine the allocation of risk reduction between electronic systems (e.g. a high voltage interlock loop) and the regulatory requirements for protected connectors. The principles of this allocation are discussed further in (Ward *et al* 2009) and will be the subject of a future MISRA publication.

Furthermore, for achieving the required functional safety of functions such as high voltage interlock, fault detection and even certain aspects of battery management, it may be that the IEC 61508 model of risk reduction through a separate "safety function" is more appropriate. Again the MISRA Safety Analysis approach (MISRA 2007) includes an alternative means of performing hazard classification that is more appropriate for such functions.

Finally, some of the technologies used in low carbon vehicles (notably electrical machine control, battery management and high voltage fault detection) are not unique to the automotive industry. Other safety-relevant industries where these technologies may be used may have their own interpretations of IEC 61508 (e.g. IEC 61800-5-2 for variable speed electrical drives (IEC 2007)). One of the guiding principles of applying IEC 61508 and producing industry-specific versions of that standard is that a specific safety integrity level (SIL) should mean the same level of risk reduction regardless of the industry sector, even though the definition of risk and the level of acceptable risk may be different. Thus, an electrical machine controller developed to SIL 3 requirements in the automotive sector should in theory be capable of being used in the machinery sector where the

risk reduction requirements allocated to this device are SIL 3 or less. However, since the ASILs of ISO 26262 do not translate directly to and from SILs, this may prove a major challenge in such a cross-sector application.

5.2 Autonomous vehicles

There is considerable interest in both civilian and defence applications of the use of autonomous ground vehicles (including uninhabited ground vehicles or UGVs). There are several concepts under wide investigation ranging from augmenting of driver tasks through remote operation to fully-fledged autonomous operation.

ISO 26262 is primarily intended to apply to series production vehicles and as such does not address modification of standard production vehicles. Furthermore topics such as the exchange of data between a vehicle and other vehicles and/or the transport infrastructure, or any kind of autonomous operation, are not considered to be in scope. In this latter respect frequent reference was made during the development of the standard to the 1968 Vienna Convention on Road Traffic (UN 1968) which states that "every moving vehicle or combination of vehicles must have a driver" and that "every driver shall at all times be able to control his vehicle or to guide his animals", and thereby that any kind of autonomous operation could not be considered "in scope".

However it is clear that the capability of technology has already reached the point where remote or autonomous operation of ground vehicles is feasible and several public demonstrations of such concepts have been made. Where future applications rely on donor platforms from production vehicles that have been developed according to ISO 26262 or other processes with a similar mindset, it could well be a challenge to derive and apply appropriate safety processes.

6 Conclusions

This paper has described the discipline of functional safety, and how it is part of the wider discipline of system safety. The importance of system safety and functional safety in vehicles, particularly the emerging "low carbon" vehicles and also autonomous vehicles, has been discussed. A key recommendation made is that safety of vehicles should consider the vehicle as a system, and ensure a co-ordinated and systems-led approach to managing safety.

In the specific domain of functional safety, the new international standard ISO 26262, which is rapidly becoming established as the state-of-the-art, was presented and an overview given of some key features of the standard. The paper also discussed some of the challenges in applying this standard, particularly for emerging technologies such as "low carbon" and autonomous vehicles, and the cross-sector application of components such as electrical machine control and battery management.

7 References

EASIS (2011): EASIS European Project. http://www.esafetysupport.org/en/esafety_activities/related_projects/research_and_development/easis.htm. Accessed 8 April 2011.

IEC 61508 (2010), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*, in 7 Parts, Second Edition, International Electrotechnical Commission.

MISRA (1994): *Development guidelines for vehicle based software*, (The "MISRA Guidelines"), ISBN 0-9524156-0-7, MIRA, also available as ISO/TR 15497:2000.

Ward, D.D. (2008): The need for safety-related software development standards, in *SAE Convergence 2008*, Detroit, USA, SAE Paper Number 2008-21-0018.

ISO/DIS 26262 (2009): *Road Vehicles – Functional Safety*, in 10 Parts, International Organization for Standardization.

VDA (2004): *Standardized e-Gas monitoring concept for engine management systems of gasoline and diesel engines*, V 2.0.

MISRA (2007): *Guidelines for safety analysis of vehicle based programmable systems*, ("MISRA SA"), ISBN 0-9524156-5-8, MIRA.

Ward, D.D., Jesty, P.H. and Rivett, R.S. (2009): Decomposition scheme in automotive hazard analysis, in *SAE World Congress 2009*, Detroit, USA SAE Paper Number 2009-01-0745.

IEC 61800-5-2 (2007), *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional*, International Electrotechnical Commission.

United Nations (1968): *Convention on road traffic*, Vienna.