Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

SAE International

Review and Assessment of the ISO 26262 Draft Road Vehicle - Functional Safety

2012-01-0025
Published
04/16/2012

Qi Van Eikema Hommes
Volpe Transportation Systems Center

doi:10.4271/2012-01-0025

ABSTRACT

ISO 26262 is the first comprehensive automotive safety standard that addresses the safety of the growing number of electric/electronic and software intensive features in today's road vehicles. This paper assesses the standard's ability to provide safety assurance. The strengths of the standard are: (1) emphasizing safety management and safety culture; (2) prescribing a system engineering development process; (3) setting up a framework for hazard elimination early in the design process; (4) disassociating system safety risk assessment from component probabilistic failure rate. The third and fourth strengths are noteworthy departure from the philosophy of IEC61508. This standard has taken much-needed and very positive steps towards ensuring the functional safety of the modern road vehicles. SAE publications from industry show a lot of enthusiasm towards this standard.

This paper suggested a number of items to be considered further strengthen the standard's ability to provide safety assurance. First, the Automotive Safety Integrity Level (ASIL) assessment may want to consider only the severity level, so that the subjectivity involved in likelihood assessment is eliminated. The ASIL assessment also needs to be standardized across manufacturers in order to address the tension between safety and business competitiveness. Government, industry consortium, and research institutions may want to work together on ASIL standardization efforts. Second, this standard provides little guidance on how to eliminate hazards in the design, but rather provides details on how to design and evaluate the effectiveness of component failure detection and control mechanisms. This paper identifies research that could be conducted on how to adapt the System Theoretic Accident Modeling and Process model during the design phase. Third, this standard gives detailed guidance on reliability engineering methods for component failures, but little on system safety design methods. Reliability and safety are different attributes of the system. This standard can be improved by further research on adapting system safety engineering methods to this standard. Fourth, the standard also substitutes good software systems engineering practices for software safety, although this is on par with other industry standards. Further research is needed to address software safety assurance. Fifth, the need for more detail in the safety assurance process and plan for product and operation phases of the product are discussed. Last, the needs for better design methods and safety assurance plan concerning driver/vehicle interaction design are also presented.

INTRODUCTION

Today's automobiles comprise increasing number of advanced electronics features that enhance vehicle dynamics, and driver comfort and convenience. Examples of such features include: Adaptive Cruise Control, Electronic Throttle Control, Automatic Start/Stop, Antilock Braking, etc. [1]. They have turned the automobiles into software-intensive complex cyber physical systems, with more lines of code than that on the Boeing 787 Dreamliner or the Joint Strike Fighter [2]. Many of these new electronics features improve the safety of the driver, passengers, and pedestrians during normal vehicle operation by providing the capability to avoid accidents.

However, the majority of existing passenger vehicle safety regulations and standards in the United States focus on individual vehicle's ability to protect the occupants and pedestrians in the event of a collision (e.g. FMVSS). ISO 26262 is the first comprehensive standard that addresses safety related automotive systems comprised of electrical, electronic (E/E), and software elements that provide safety-related functions. This paper reviews and assesses the effectiveness of the approaches suggested in ISO 26262 for

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

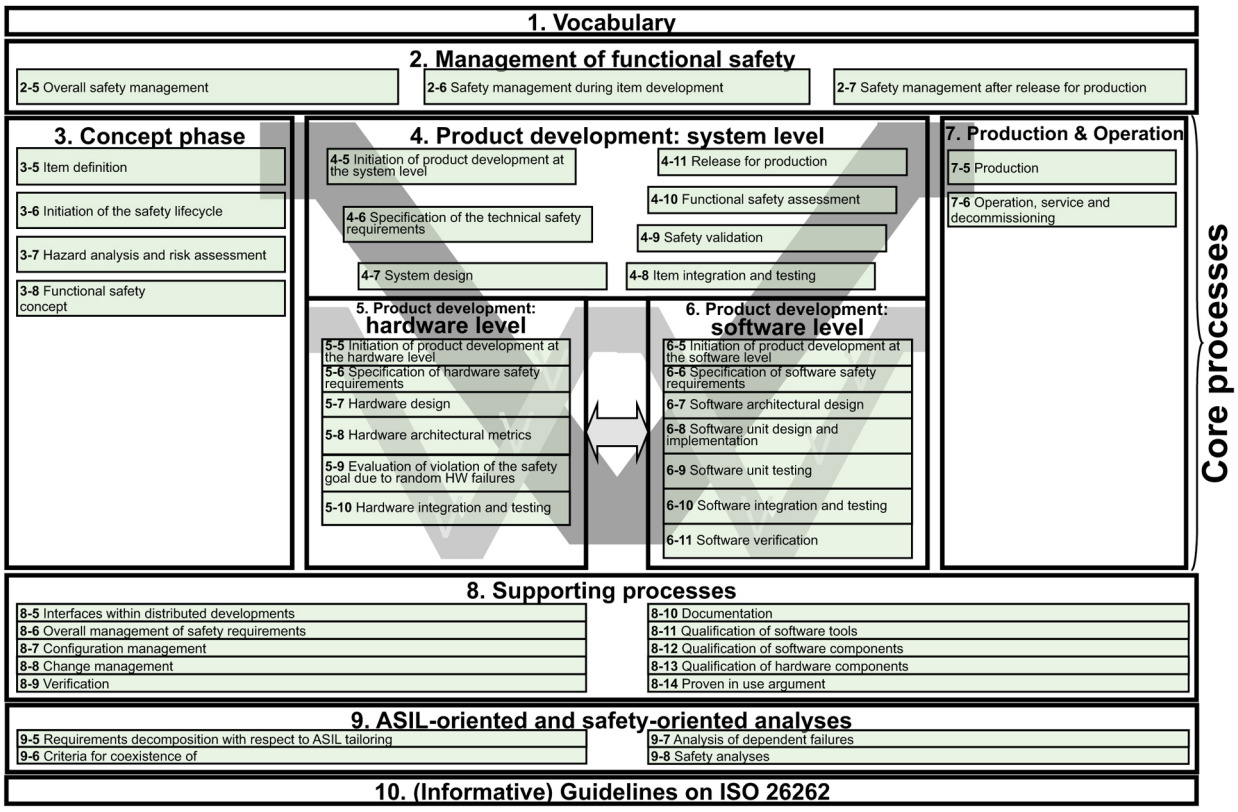

Figure 1. Overview of ISO 26262 [3]

safety assurance. At the time of this study (June and July 2011), the final version of the standard was not yet published. Therefore, all of the assessments made in this paper are based on the 2009 draft standard [3]. The final version of the standard was published in November 2011 after the submission of this paper. Future discussions regarding the standard should be based on the final standard.

This paper starts with a brief overview of the standard, followed by assessments of the methods and approaches suggested in the standard. Next, published industry pilot applications and their feedbacks are summarized. Last, based on the above assessments, areas for improvements and future research directions are suggested.

OVERVIEW OF THE STANDARD

ISO 26262 is an adaptation of the IEC 61508 [4] to road vehicles, and is also strongly influenced by ISO TS 16949 Quality Management System. ISO 26262 recognizes and intends to address the important challenges of today's road vehicle technologies. These challenges include (1) the safety of new E/E and software functionality in vehicles, (2) the trend of increasing complexity, software content, and mechatronics implementation, and (3) the risk from both systematic failure and random hardware failure.

The scope of the standard is limited to safety-related systems that include one or more E/E systems and that are installed in series production passenger cars with a max gross weight up to 3.5 ton. It addresses possible hazards caused by malfunctioning behavior of E/E safety related systems including interaction of these systems. It does not address hazards such as electric shock, fire, smoke, heat, radiation, toxicity, reactivity, corrosion, release of energy, and similar hazards unless directly caused by malfunctioning behavior of E/E safety related systems (see Part 1 [3]).

Figure 1 offers an overview of the standard. The standard has ten parts in total. Part 2 through 7 are the core of the standard. Parts 1, 8, 9, and 10 provide supporting information to various parts of the core content.

ASSESSMENTS

The assessment in this paper is focused on the standard's ability to address the challenges in ensuring the safety of complex software intensive E/E systems. There are other aspects of the standard that may be also important, but are not discussed here. In order to put this safety standard into the perspective of other existing safety standards, the following classification is used [6]:

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

1. Prescriptive:

a. Product: specify required safety design features. Examples include building code.

b. Process: specify the process to be used in producing the product or system or in operation. MIL-STD_882D is an example.

2. Performance-based or goal-setting approaches: focus on desired measurable outcomes, rather than required product features or prescriptive processes.

Based on the above classification, ISO 26262 is a mix of prescriptive process standard and performance-based/goal-setting standard. This underlying nature of the standard leads to many of its strengths as well as limitations that will be discussed next.

STRENGTHS

Safety Management and Safety Culture

Part 2 of the standard defines the organizations that are responsible for the safety management throughout the product lifecycle from concept inception, product design, to production and operation. It is very plausible to address the management of functional safety at the very beginning of the standard. Numerous literature have identified that most catastrophic accidents in large complex systems were not simply caused by technical failures, but rather managerial decisions on the safety of system design, manufacturing, and operation [5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. This standard not only calls for safety management, but also clearly states that safety management must be implemented throughout the design, production, and operation of the system, starting with the early concept generation phase. This emphasis of formal safety lifecycle management is absolutely necessary for the success of complex systems.

Furthermore, this standard states, "*the organization shall create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety* (Clause 5.4.2.1)." Dekker [8, 9] has stressed the importance of creating a safety culture within the company so that safety is not compromised during decision process and operations. It is very positive that this standard put such a high emphasis on safety culture.

Prescriptive Systems Engineering Process

Implicitly, the standard prescribes a product development process, initially discussed in Part 2 (Figure 1), and further illustrated by Part 3 through 7. Therefore, this standard belongs to the category of "prescriptive process" standard [6]. The prescribed product development process is the systems engineering V process [15]. Safety requirements, hazard analysis, and design efforts flow down the system decomposition hierarchy, and integration testing, and safety assessments go up the decomposition hierarchy. This process is generally suitable for the development of large complex systems, and is appropriate for the automotive E/E systems. In fact, to the author's best knowledge, most companies in the automotive industry already follow such a product development process. Therefore, the industry should not have trouble adapting to this prescribed product development process.

In addition, the latest research on system safety argues that the safety of complex cyber physical systems is not the same as reliability engineering [5]. Reliability engineering might have been sufficient for the simpler mechanical dominated systems in the past, but the increasing complexity level in today's cyber physical systems require us to go beyond reliability for safety assurance. Safety is an emergent behavior in the complex sociotechnical systems [5,8,10], and requires the use of a systems engineering approach. Prescribing the systems engineering V process for product development hence lays a solid ground for addressing system safety.

Departure from Safety as an Afterthought

Although based on IEC 61508, ISO 26262 takes a noteworthy departure in the safety design philosophy. The safety design philosophy emphasized in IEC 61508 is that one designs for the main functions of a system first, and then designs in safety afterwards by adding *Safety Functions*. However, the least costly and most effective approach to safety is to eliminate hazards in the first place during the design, before resorting to hazard reduction and control techniques (Figure 2). IEC 61508 Part 1 Clause 7.4.2.2 also agrees that the elimination of hazards in design is important, but it says this is out of the scope of the standard. Instead, immediately after the hazard analysis step, IEC 61508 suggests develop *Safety Functions* (Part 1 Table 1 [4]). *Safety Function* is defined as the "*function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the E(quipment) U(nder) C(ontrol), in respect of a specific hazardous event*" (Part 4 Clause 3.5.1 [4]). The *Safety Function* concept therefore is about hazard reduction and control (Figure 2). Hazard reduction and control method is not wrong, but it teaches a design philosophy that safety is added on after the main functions are designed for, since one cannot possibly be designing fault detection and control until a substantial amount of details about the design is decided. The negative consequence is that safety is seen as an afterthought and extra cost on the original design, leading to tradeoff between safety and other design considerations. We run the risk that safety may be compromised in design decisions in order to ensure profitability or other corporate goals [5 (Chapter 10), 6, 10 (Chapter 9)]. The second problem with this philosophy is that once the safety function is added to a design, there isn't an explicit requirement on the safety monitoring of the safety

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

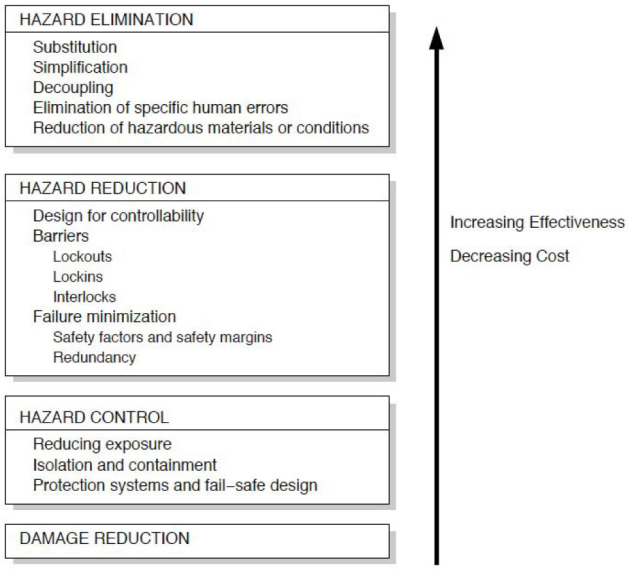

Figure 2. System Safety Design Procedure [5]

device. In the event that a safety device malfunctions, the system safety can still be compromised. A more effective and less costly approach is to consider eliminating hazards in the design in the first place.

Different from IEC 61508's focus on *Safety Function*, the step after hazard analysis in ISO 26262 is the development of high-level *Safety Goals*. The *Safety Goals* are top-level safety requirements on the system (Part 1 Clause 1.105 [3]), which is much broader than functions that detect and control faults. Additionally, ISO 26262 also introduces two new terms- *Safety Measures* and *Safety Mechanisms*. *Safety Mechanism* is defined as the "*measure implemented by a E/E function or element, or in other technologies, to detect or control failures in order to achieve a safety state of the item, or maintain a safety state of the item, or both*" (Part 1 Clause 1.107 [3]). This is similar to *Safety Function* in IEC 61508, and is focused on technical devices to reduce and control faults. *Safety Measure*, on the other hand, is a more general term. It is defined as "*activity or technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures, or mitigate their harmful effects*" (Part 1 Clause 1.107 [3]). Design methods and processes are safety measures, in addition to safety mechanisms. Furthermore, the standard also does not say that efforts to eliminate the hazards in design are out of scope. In fact, ISO 26262 requires the flow down of top-level safety goals to the lower levels of the system hierarchy as safety requirements. Therefore, ISO 26262 has set up the framework for designing safety into the system-hazard elimination in the first place (Figure 2).

Nonetheless, this important departure in the safety design philosophy seems subtle for a reader unfamiliar with the standard's development history and effort, and hence may be misunderstood in the actual practice. Suggestions on how to further strengthen this very important aspect of the standard will be provided in the next section.

Disassociate Safety Risk Level from Probabilistic Failure Rate

One of the very first steps of both IEC 61508 and ISO 26262 is to identify the hazards and classify the associated risks levels. The risk level then dictates the system development efforts for safety assurance. IEC 61508 uses the *System Integrity Level* (SIL) to indicate the acceptable risk levels of the safety functions. *Safety Integrity* is the "probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time" (Part 4 [4]). Therefore, SIL uses the failure probability to classify the risk levels (Part 1 Table 2 and 3, [4]). However, for many of the system functions using new technology, such probability values do not exist. Additionally, for human operators and software components, the concept of failure rate also does not apply [5]. Therefore, SIL is not an appropriate risk indicator for the modern software intensive E/E systems that contain human interactions.

ISO 26262 does not using the probabilistic failure rate concept. In ISO 26262, once the top-level safety goal is established, the Automotive Safety Integrity Level (ASIL) is assessed for each of the safety goal. ASIL is determined based on three categories: severity of the accident if the safety goal is not met (Figure 3), probability of exposure regarding operational situations (Figure 4), and the controllability of the hazardous situation (Figure 5). The final ASIL for the safety goals are assessed based on the table in Figure 6. In Part 3 Annex B, the standard specifically states

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

Class	S0	S1	S2	S3
Description	No Injuries	Light and Moderate Injuries	Severe and Life-threatening Injuries(survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Figure 3. Classes of Severity (Table 1 of Part 3) [3]

Class	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium Probability	High Probability

Figure 4. Probability of Exposure Regarding Operational Situations (Table 2 of Part 3) [3]

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Figure 5. Classes of Controllability (Table 3 of Part 3) [3]

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

D—highest safety integrity level, A—Lowest safety integrity level, QM—Quality Management

Figure 6. ASIL Determination (Table 4 of Part 3) [3]

that the component failure rate is not considered in the risk assessment, therefore avoiding the problem of using probability assessment mentioned in the last paragraph.

CONSIDERATIONS FOR IMPROVEMENTS

ASIL Assessment

Two aspects of the ASIL assessment may be further studied and improved:

1. Consider worst-case instead of most-likely case.
2. Standardize ASIL assessment among OEMs and suppliers.

The ASIL determination involves the assessment of the *Probability of Exposure* (E) (Figure 4, Table B2 in Part 3 Annex B [3]), which often is called *Likelihood* in risk assessment terms. While the severity of a hazard is usually easy to estimate using the worst-case accident, the likelihood assessment of the worst-case scenario can be subjective, especially for new technical systems that may not have a finished design, and do not have years of history to drawn upon [5 (Chapter 10), 6, 10 (Chapter 9)]. Consider the Fukushima nuclear power plant accident that happened in April 2011. The severity of the failure of the back-up cooling system would undoubtedly be S3 (Figure 3), but the likelihood probably had been classified in the range of E0 to E2 (Figure 4), since power plant engineers probably thought they had had sufficient protection for tsunami. Ignoring the C value for this non-automotive case, S3 and E0-E2 would have given very low risk level for the failure of the back up cooling system (Figure 6), and hence making the power plant unprepared in April 2011. It has been suggested that the likelihood assessment be eliminated from the risk evaluation since it brings in subjectivity [5 (Chapter 10), 6, 10 (Chapter 9)]. The ISO 26262 standard may want to consider doing the same so that more emphasis will be placed on the worst-case scenarios.

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

The ASIL assessment may also vary among different OEMs due to the differences in their assumptions and analyses about the system. In addition, the determination of ASIL faces the challenge of the inherent tension between a firm's ethical and legal obligation and the cost of product development and manufacturing activities. A lower ASIL of certain safety goals can save development cost and help the firm stay competitive. Yes, since ASIL assessments carry legal implication, an OEM would want to choose a conservative assessment, which could in turn put itself in a less competitive position. For suppliers, inconsistency in the ASIL assessment among OEMs can create challenge for the certification of their components, since now the same component will need to fulfill different ASIL's.

Recognizing this issue, Hamann et al. proposes a "Harmonized ASIL Classification" [16]. They suggested standard ASIL's for a number of components. The examples used in their paper, such as airbag and electric window lift seem reasonable. However, such a focus on component-level hazard classification is a bottom-up approach to a system level emergent property-safety. Many components' ASIL may only be determined in the context of the system that they function in. Therefore, harmonizing the components' ASIL may not be as straightforward as the paper suggests.

It is to the author's best knowledge that as of December 2011, the Socienty of Automotive Engineering (SAE) has formed a committee to address ASIL assessment. The committee may want to consider the following questions:

1. Shall ASIL be only based on severity of the accident so that effort is put on preventing the worst-case accident scenario, rather than the most-likely accident scenario?

2. For suppliers interested in developing standard ASIL for their components, what kind of context assumption they should provide along with the component ASIL assessment? What must OEMs do as they review the component ASIL suggested by the suppliers in the context of their specific system implementation?

3. Can ASIL harmonization be achieved by industry consortium alone? Shall government participate to assist the discussions?

Further Emphasizing Hazard Elimination in Design

The "Strengths" section of this paper states that one of the major departures of ISO 26262 from IEC 61508 is providing a framework for designing safety into the system in the first place. However, the way that the standard explains this significant advancement lacks clarity for readers without the background knowledge of the history of the standard development.

First, *Safety Measure* is mentioned in the "Introduction" section of every Part of the standard. However, except for the two-line definition provided in Part 1 Clause 1.106, the standard did not explain what safety measures really are. The standard calls for the use of safety measures throughout the design process, but does not connect this term to the system engineering process prescribed, the philosophy of design safety into the system in the first place, or the possibility of using methods and processes in addition to safety mechanisms.

Contrary to the ambiguity of the Safety Measure concept, one can easily find in the standard how to design and evaluate the effectiveness of Safety Mechanisms. For example, Part 4 Clause 6.4.7 and 6.4.8 describes how to develop requirements for safety mechanisms. Throughout the hardware design phase (Part 5), Safety Mechanisms are discussed at length as a means to ensure hardware safety (Clause 6.4, 7.4.3.3, 7.4.3.4, etc.). Furthermore, Annex C-G of Part 5 provides details to a great extent on how to assess the safety mechanisms' ability to detect and control faults, using probability calculations. To a reader unfamiliar with the design philosophy change that ISO 26262 intends to make, the content concerning safety mechanism is detailed and rich with explanations and examples. It is natural for a reader to think that safety mechanism is the dominant safety measure, especially when the standard's predecessor-IEC 61508-also promotes such a design philosophy.

To improve the standard so that hazard elimination is emphasized, the following suggestions may be considered:

1. The standard may want to add a section in Part 1 to clarify the shift in its safety philosophy from IEC 61508. A diagram like the one in Figure 2 can be a simple yet effective way to convey the idea.

2. The connection between "Safety Measure" and the systems engineering approaches that this standard has prescribed may be clarified so that readers will not confuse safety measure with safety mechanisms.

3. A research question to be considered is what design for safety methodology is available beyond the probability-based hardware failure analysis methods used for the effectiveness of safety mechanisms (Appendix C-G in Part 5). Without providing recommendations on what to do beyond the probability risk analysis, the concept of safety measure can still be ambiguous. Since the standard recognizes the safety of automotive E/E system should follow a systems development process, the System Theoretic Process Analysis (STPA) based on the System Theoretic Accident Modeling Process (STAMP) model [5] is a method that can provide a process to identify system level hazards and eliminate them in the first place. Research work may be conducted to understand the effectiveness of the STPA approaches in the automotive E/E systems.

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

Separating System Safety from Reliability Engineering

The latest research on system safety suggests safety and reliability are two *different* concepts. Although reliability positively contributes to safety, it is not sufficient to ensure safety. A number of such examples are illustrated in Chapter 1 of Leveson's latest book [5], including the Mars Polar Lander and a batch chemical plant in England. On the other hand, safety does not necessarily require highly reliable components either [5].

Reliability engineering is focused on failure prevention [17, 18]. Failure is defined as "the event when a required function is terminated (exceeding the acceptable limits)" [18]. Therefore, if a component satisfies its required function, then the component has not failed, even if the required function may be unsafe in certain larger context of the system. Safety, on the other hand, is defined as the absence of accidents. Safety engineering therefore should focus on identifying and preventing hazards. The outcome of safety engineering should be design requirements to ensure the prevention and control over hazardous system states, which has a very different focus from reliability engineering [5].

As previously stated in this paper, ISO 26262 provides a system safety-engineering framework by introducing the concept of "safety goals" and "safety measures." However, the standard discusses reliability engineering methods at length, and provides very limited guidance on how to effectively identify hazards and eliminate them in the first place. For instance, in Part 5 Clause 8, Hardware Architecture Metric (HAM) is computed to evaluate the hardware architecture against the requirement of fault handling. Annex F of Part 5 offers an example illustrating how such metrics are computed. The computation of the metrics is based on hardware component failure rate and the safety mechanism's diagnostic capability for each hardware part failure. The total system HAM is an addition of all the component fault metrics. There are several limitations to this approach. First, this method of computing HAM is only limited to random hardware part failure (Part 5 Clause 8.2), and cannot address common causes and systemic causes of failures, which are often the reasons for accidents [5, 10]. Second, this bottom up approach ignores interactions among the components, which are prevalent in highly complex automotive E/E systems. Third, the diagnostic coverage estimations of a safety mechanism are three discrete levels (Table D.1 of Part 5). They are estimated at the component level, but computed as if they are continuous values to produce the system level HAM metrics, which then provide rationale for safety assessment. Since the diagnostic coverage values are up for interpretation, this approach lacks rigor and the quantitative and continuous value of HAM may be misleading.

Another example of using reliability engineering concept can be found in the design analysis methods frequently recommended (not mandated) by the standard throughout the hardware design process part-Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA). FMEA is an inductive method (bottom up) that focuses on low-level component failures and their effect on the system level performance. FMEA is inadequate in addressing the safety of a complex system. First of all, based on the discussion above, component reliability is not sufficient to ensure safety. Second, for a complex system, it is not only the failure of a single component, but often two or multiple components and their interactions that may lead to the system failure. It is a laborious and impossible task for an analyst to identify and analyze all possible component failures and combination failures that will cause system level failure [12]. It is even more impossible to foresee all the combinations of non-failure states of components that will lead to hazardous conditions. Third, when focusing on component failures, the concept only applies to hardware in the technical systems. Software components and human do not fail.

FTA on the other hand, is a top down approach focused on identifying faults and their causes. It somewhat alleviates the analysts' daunting task of finding all combinations of potential component failures that may lead to sever system level failures [12]. However, FTA does not provide enough guidance on how to come up with the lower level events that lead to the higher-level system faults. Fault Trees are more like a record of the results of brainstorming or expert opinion, providing little guidance on the hazard causal analysis thought process [7]. Furthermore, once a Fault Tree is built, the emphasis of FTA is on the Quantitative Reliability Analysis (QRA). The probability of bottom events, often component failures, is aggregated up the tree to produce top-level event's probability. If the top-level event has a probability of occurrence below the acceptance level, then the system is considered safe. However, not all of the bottom events' probability data exist, especially for the new automotive E/E technology, software, or human operators. This leaves a lot of room for subjectivity and potential manipulation of numerical values. This approach is also inadequate to handle the situations when none of the component fails, but the interaction among components lead to hazardous conditions.

Using Safety Case approach for safety assurance (e.g. Part 2 Clause 6.4.5 and Part 10 Clause 9) may further exacerbates the negative effects of applying the reliability concepts for safety. In this standard, a Safety Case "communicates a clear, comprehensive and defensible argument (supported by evidence) that a system is acceptably safe to operate in a particular context (Part 10 Clause 9.1)." Typically, the design engineering team prepares the safety case and an independent party will review the safety case (Part 2 Table 1). When preparing for the safety case, the design team may spend

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

efforts looking for proof that their favorite chosen design is safe. This is called *confirmation bias* in psychology [6], and isn't anything unique or special about automotive engineers. QRA fits well in safety case construction since it can provide quantitative assessment on how safe a system is, and since the analysis method is well explained in this standard. Furthermore, since engineering teams typically chose a design based on a number of other constraints such as performances, weight, fuel economy, cost, etc., the QRA-based safety case may lead to trading off safety with other technical and business goals (Chapter 10 in [10]). It is important to note that the standard does an excellent job requiring independent safety assessment on the safety cases. Nonetheless, an independent party that is less familiar with the design than the engineering team may not be able to find errors in the safety case argument.

To summarize, this standard does not clearly distinguish the reliability engineering methods and the safety engineering framework. The amount of details on reliability engineering techniques in contrast with the lack of guidance on hazard identification and elimination hinders the standards ability to sufficiently provide safety assurance. Unfortunately, this is the case for many industry safety standards rooted in IEC 61508. As stated earlier, ISO 26262 already took a step forward in the right direction. To further improve this standard, the following points may be considered:

• The role of the team that conducts independent assessment of the safety case should be to independently identify hazards and their causes in the new system, and then prove that they have all been eliminated or mitigated by the improved design using the safety case as evidence. The team should not just review the submitted safety case document.

• One of the powerful methods developed recently for complex embedded control systems is the STPA based on STAMP model. Future research may want to examine this and other approaches in order to improve the standard's ability to guide engineers to apply safety-engineering framework [5].

Software Safety Assurance by the Elimination of Design Errors

In ISO26262, software safety assurance is provided by following good systems engineering process (Part 6 Figure 2) and applying good software engineering methods and practices. For instance, the standard suggests good software design practices in both the architecture design and unit design phases, such as considering the verifiability, testability, modularity, minimum complexity, etc. (Clause 7.4.2 and Clause 8.4.3). Yet, little guidance is provided on how to arrive at these properties and how to measure whether these attributes have been achieved to a satisfactory level. Furthermore, there has not been rigorous proof that good software systems engineering sufficiently lead to software safety. So although good software systems engineering will improve the quality of the software, it does not guarantee the safety of the software system.

The software safety assurance approach that ISO 26262 takes is similar to those in other industries, such as DO-178. The lack of a rigorous software safety assurance plan in this standard reflects an intellectual gap in our understanding of what safety means for complex software systems. Similar to the language used in DO 178, this standard implies that the software function fails (Part 6 Clause 6.4.1), but the hardware component failure concept is meaningless for software. Software is an abstraction, and it does not fail randomly like hardware parts. Software faults are due to design errors, often caused by missing or incomplete requirements [5]. In order to assure the safety of software, a new framework that emphasizes hazard elimination is needed. Similar to previous sections, methods that enable the early identification of hazards and causes will be critical to ensure the elimination of software design errors in the first place. Future research may want to assess methods such as STPA [5].

Further Developing Safety Assurance in the Production and Operations Phases

Production is the stage when design concepts are materialized. The manufacturing of features essential to safety need to be carefully planned, managed, and monitored. However, this standard is very light on this topic (Part 7). On one hand, it provides a lot of room for different manufacturers to tailor the assurance plan. On the other hand, it is a stark contrast when compared to Part 5 and Part 6 how little detail is provided in this part. More research is needed to identify how to leverage the current system safety approaches and design for manufacturing approaches in the safety assurance plan.

Operation is another important phase of the vehicle's lifecycle when the product is actually in the users' hand. Similar to the Production section, the safety assurance plan for the Operation phase of the lifecycle is very brief, providing little guidance on what it takes to ensure the product is safe during operations. Below are a few research questions as thought starters:

1. If the software can be upgraded after the vehicle is sold, how will the safety after modification be assured? In the standard, Part 8 Clause 8 describes a general change management process. Part 3 Clause 6.4.2 requires impact analysis for modification changes. However, neither place provides further guidance about how to conduct these analyses. On one hand, this leaves lots of room and flexibility to adopt the best analysis techniques. On the other hand, the lack of guidance and recommended practices can leave this step vulnerable. More importantly, this standard does not discuss how aftermarket modifications will be addressed or regulated to ensure safety. Government involvement may be helpful to regulate the aftermarket activities.

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

2. What is the process of checking to ensure sensors and actuators are functioning as intended throughout the lifetime of the vehicle? What will be the plan to maintain the electronics?

3. Is there a need for government to mandate a yearly vehicle safety inspection, similar to the yearly emissions inspection required in some states, especially considering the potential aftermarket modifications?

4. What will be the education and training plan for the service shop technicians regarding the safety of E/E hardware and software?

Incorporate Design for Safe User Interaction

Although today's increasing numbers of electronics features in automobiles are intended to provide safety, comfort, and convenience to the drivers and passengers, the ISO 26262 standard focuses only on the technical system-the vehicle, without mentioning the interactions between the vehicle and the users. The drivers of the vehicles play a major role in ensuring the safety. All of the major automotive OEM's have engineering teams studying the vehicle-user interactions. By not addressing user interactions issues, the standard takes a narrow view on the safety of modern automotive E/E system.

The Aviation industry is years ahead in introducing automation into the cockpit to assist the pilots and reduce their workload. However, automation in the cockpit has also been linked to a number of aviation accidents. Literature concerning the design of cockpit automation points out that there are both benefits and costs to automating the functions that had been performed by human. Billings [20] and Starter and Woods [21] argue that when the technical system becomes "mode-rich," it increases the cognitive demands on the operators. The operators can easily make "mode-error." The automation can become "clumsy", i.e. the new cognitive demands can easily congregate at high-tempo and high criticality periods. What the automation is doing can become "opaque," and the automation can fall into the trap of "literalism." Much of the research in the aviation area has pointed out that automation can lead to safety problems and contribute to accidents, if the technical design exhibits the above-mentioned characteristics. In order to ensure safety, the system design must take into consideration the operators' cognitive capability and human learning patterns [22].

Similar concerns also exist among the emerging automotive active safety features that will automate some portion of the drivers' tasks. For instance, adding the adaptive cruise control feature on top of the traditional cruise control leads to an additional operating mode in the system. Some car manufacturers also have a forward distance warning feature in vehicles. Drivers can set the system to different modes of the system-cruise control only, cruise control with or without distance warning, adaptive cruise control with distance warning, etc. In addition, other active safety features such as lane keeping may also be engaged. These features produce a driving environment that is more cognitively taxing and unfamiliar to most drivers. Furthermore, different OEM's may also implement these features differently in their vehicle, further confusing the untrained drivers. Without careful design considerations for safety regarding the vehicle/driver interaction, the well-intended new automotive E/E features could instead be hazardous.

This paper does not intend to exhaustively list all of the potential hazards of various E/E functions. Neither is it the intent of the paper to provide a thorough literature review to the field of user centered automation design. However, through the above brief discussion, the author hopes to shed light on the seriousness of the fact that ISO 26262 missed a very important aspect of the safety of automotive E/E systems-the interaction between the technical system and the drivers and passengers. Future improvements of the standard may want to consider including this topic.

INDUSTRY APPLICATION REVIEWS

With the adoption of ISO 26262 in Europe and the upcoming completion of its first draft, most of the US automotive OEMs and suppliers have reviewed and even run pilot trials of the standard [16, 23, 24, 25, 26, 27]. The overall sentiment from the industry is enthusiastic, as everyone recognizes that this is an important and necessary standard, as the automotive products become more software/controls intensive, and the complexity of these E/E systems are becoming increasingly challenging. It was acknowledged that the prescribed product development process in this standard is not different from the mature product development process employed by many companies. It is also argued that the standard aligns well with model-based product development approaches [24].

On the other hand, industry also expressed concerns about the implementation of ISO 26262. They are summarized below:

1. The standard will require a large amount of documentation, which will significantly add to the cost and speed of development.

2. Since the standard is about the entire product life cycle, the effect of the standard will take some time to show.

3. The concept phase is easy to implement, but there is difficulty to integrate a pilot project into the rest of the system that was not developed based on the standard.

4. ASIL classification harmonization needs more discussion.

5. It takes too long to collect sufficient data to illustrate the effectiveness of the standard.

6. The definition of "proven in use" in the standard makes it a step that will never be visited.

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

7. Qualification of software tools safety may be very challenging considering how many software tools are used in the typical product development process today.

SUMMARY AND RECOMMENDATIONS

ISO 26262 has taken a very important and positive first step towards ensuring the safety of the complex and growing number of E/E systems and software in modern road vehicles. This standard can be further improved with additional research and investigation. It calls for collaboration among government agencies, industries, and research institutions. Based on the assessment detailed in this paper, next steps have been recommended at the end of each section. They are summarized below:

1. In the short-term, government, industry, and research institutions may wan t to consider working together to improve the standardization of ASIL, in order to level the playground for manufacturers. Future research may want to understand how the system implementation context may affect the determination of component ASIL and whether standardization of ASIL for all components is possible.

2. ASIL may want to remove the likelihood assessment term.

3. The standard may want to further stress the important philosophical shift from IEC 61508-the concept of safety goals and safety measures as oppose to safety functions used in IEC 61508.

4. Long-term research activities may be considered to identify and adapt better methods for hazard identification and elimination, so that more guidance may be given on safety engineering, instead of reliability engineering methods. STPA based on the STAMP causality model is a promising approach worthy of investigation [5].

5. In the near term, government may want to play a role in certifying software tools used for the development in order to assure consistency across manufacturers.

6. Research could be conducted to investigate how to identify key manufacturing parameters to ensure safety and how to assess that manufacturing meets the safety assurance standards.

7. Research could also be conducted to investigate how to assure safety during the operational life of the vehicle. The government may want to develop a program similar to emissions testing in a number of states. The government may also want to develop driver training programs that will familiarize the users with the latest E/E features so that drivers can safely operate them.

8. Long-term research may be conducted to investigate how to improve safety for the vehicle and driver interactions. This research effort should go beyond the traditional screen design and ergonomics design. It should take into consideration the negative effects automation may have on operator's cognitive load and consequent actions and behavior. It should lead us to designing safer technical systems that goes beyond component reliability.

REFERENCES

1. Hubing, T., "Analyzing Unintended Acceleration and Electronic Controls." Presentation on July 1, 2010 to the Transportation Research Board, http://onlinepubs.trb.org/onlinepubs/ua/100701hubing.pdf, referenced on December 22, 2011.

2. Charette, R. N., "This Car Runs on Code." *IEEE Spectrum*, February, 2009.

3. *ISO 26262, Road Vehicles Functional Safety*. Draft, 2009. International Organizations for Standards.

4. *IEC 61508, Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems*. International Electrotechnical Commission. Edition 2.0, 2010-04.

5. Leveson, N., *Engineering a Safer World*, MIT Press, Jan. 2012.

6. Leveson, N., "The Use of Safety Cases in Certification and Regulation." *Journal of System Safety*, Nov/Dec 2011. MIT Engineering Systems Division Working Paper (ESD-WP-2011-13), http://esd.mit.edu/WPS/2011/esd-wp-2011-13.pdf.

7. Leveson, N., *Safeware*, Addison-Wesley Professional, 1995.

8. Dekker, S., *The Field Guide to Understanding Human Error*, Ashgate, 2006.

9. Dekker, S., *Just Culture: Balancing Safety and Accountability*. Ashgate, 2007.

10. Perrow, N., *Normal Accidents: Living with High Risk Technologies*, Princeton University Press, 1999.

11. Roberts, K., "Some Characteristics Of One Type Of High Reliability Organization." *Organization Science*, Vol 1, No. 2, 1990.

12. Weick, K. E. and Roberts, K., "Collective Mind in Organizations: Heedful Interrelatingo n Flight Decks." *Administrative Science Quarterly*, 38 (1993): 357-381.

13. LaPorte, T. R., and Consilini, P. M., "Working in Practice But Not in Theory: Theoretical Challenges of 'High-reliability Organizations." *Journal of Public Administration Research and Theory*, 1 (1991):1:19-47.

14. Leveson, N., Dulac, N., Marais, K., and Carroll, J. "Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex

Gratis copy for Qi Van Eikema Hommes
Copyright 2012 SAE International
E-mailing, copying and internet posting are prohibited
Downloaded Thursday, March 15, 2012 12:49:55 PM

Systems." *Organization Studies*, February/March 2009 vol. 30 no. 2-3 227-249. doi: 10.1177/0170840608101478.

15. *Handbook of Systems Engineering*, V3.2.1, International Coucil of Systems Engineering, 2011.

16. Hamann, R., Kriso, S., Williams, K., Klarmann, J., and Sauler J., Bosch GmbH. "ISO 26262 Release Just Ahead: Remaining Problems and Proposals for Solutions," SAE Technical Paper 2011-01-1000, 2011, doi: 10.4271/2011-01-1000.

17. Birolini, A., *Reliability Engineering: Theory and Practice*, Springer, 2010.

18. Rausand, M., Hoyland, A. *System Reliability Theory: Models, Statistical Methods, and Applications*. 2nd Edition, Wiley 2004.

19. US Nuclear Regulatory Commission, *Fault Tree Handbook*, NUREG-0492, 1981.

20. Billings, C. E., *Aviation Automation: The Search for a Human-centered Approach*. Lawrence Erlbaum Associates, Publishers, 1997.

21. Starter, N. B., and Woods, D. D. "How in the World Did We Ever Get into That Mode? Mode Error and Awareness in Supervisory Control." *Human Factors*, 1995, 37(1), 5-19.

22. Rasmussen, Jens. *New Technology and Human Error*. John Wiley and Sons, 1987.

23. Ressler, G., "Application of System Safety Engineering Processes to Advanced Battery Safety," SAE Technical Paper 2011-01-1369, 2011, doi:10.4271/2011-01-1369.

24. Buttle, D., Blanche, G., Lefarth, U., and Wolff, H., "Having Your Cake and Eating It: A Model-Based Approach for Satisfying USO 26262 Software Development Requirements," SAE Technical Paper 2011-01-1001, 2011, doi:10.4271/2011-01-1001.

25. Schwarz, J., and Buechl, J., "*Preparing the Future for Functional Safety of Automotive E/E-Systems*."

26. Dold, A., Daimler,, "*Implementation of Requirements From ISO 26262 in The Development of EE Components and Systems*." Presentation, 2008.

27. Murray, B., UTRC, "Software Safety Assurance Process and Challenges in the Automotive and Aviation Industries." Presentation, March 2011.

DISCLAIMER

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

The U.S. Government assumes no liability or responsibility for the contents of this paper or the use of this paper. The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the paper has been included only because it is essential to the contents of the paper.

CONTACT INFORMATION

Dr. Qi D. Van Eikema Hommes
qhommes@mit.edu

(617) 253-8973

The Engineering Meetings Board has approved this paper for publication. It has successfully completed SAE's peer review process under the supervision of the session organizer. This process requires a minimum of three (3) reviews by industry experts.

ISSN 0148-7191

Positions and opinions advanced in this paper are those of the author(s) and not necessarily those of SAE. The author is solely responsible for the content of the paper.

SAE Customer Service:
Tel: 877-606-7323 (inside USA and Canada)
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE Web Address: http://www.sae.org
Printed in USA