Overview of the 2nd Edition of ISO 26262: Functional Safety – Road Vehicles

Rami Debouk, General Motors Company, Warren, MI, USA

ABSTRACT

Functional safety is of utmost importance in the development of safety-critical automotive systems, especially with the introduction of driver assist and automated driving systems. ISO 26262, Functional Safety – Road Vehicles, has been the de facto standard for functional safety in the automotive electronics domain since the release of its first edition in 2011. It is currently available as a second edition final draft international standard and is expected to be published as an ISO international standard later in the year.

In this report, we present an overview of the standard that applies to all activities during the safety lifecycle of system development. At the concept phase of ISO 26262, the hazard and risk assessment process focuses on identifying possible hazards caused by malfunctioning behavior of Electrical/Electronic safety-related systems and mitigating them through the identification of safety goals. The design phase includes system, hardware, and software development with requirements developed from the safety goals. ISO 26262 also prescribes the functional safety management activities to be performed during the safety lifecycle and provides requirements on the supporting processes.

In addition to presenting an overview of the standard, this report points to some major changes introduced in the second edition such as the extension of the standard's scope to include all road vehicles, the objective-oriented confirmation reviews approach, and references to Cybersecurity at the Concept and System Level development to name a few.

1 - INTRODUCTION

Safety-critical systems are systems that have the ability to create potentially hazardous issues in case they do not operate properly or as designed [1,2]. These systems are in general analyzed using rigorous and systematic safety processes [3] that define all safety activities during the lifecycle development of the system. In the automotive domain, ISO 26262 [4], Functional Safety – Road Vehicles, emerged in 2011 as the go to standard for functional safety: It was launched as the adaptation of IEC 61508 [5] to comply with needs specific to the application sector of Electrical/Electronic (E/E) systems within road vehicles.

ISO 26262 applies to all activities during the safety lifecycle of system development. At the concept phase, the hazard and risk assessment process focuses on identifying possible hazards caused by malfunctioning behavior of E/E safety-related systems and mitigating them through the identification of safety goals. The design phase includes system, hardware, and software development with requirements derived from the safety goals. ISO 26262 also prescribes the functional safety management activities to be performed during the safety lifecycle and provides requirements on the supporting processes.

As is the case with the introduction of any new process, lessons have been learned from the application of the first edition of ISO 26262 and such learnings necessitated the early release of the second edition which is currently at the final draft international standard stage [6] and expected to be published later this year. The scope of applicability has been extended to include additional-road vehicles as part of the improvement to the standard. In addition, channels of communication between functional safety and cybersecurity have been identified at both the functional safety management level and product development at the system level. Requirements on trucks, buses, trailers and semi-trailers as well as their supporting processes have been introduced in the second edition. A new part defining motorcycles specific requirements in the safety lifecycle has been added. Guidance on semiconductor development has been described in a new informative part of the standard. Finally, improvement on many of the existing definitions and requirements and some restructuring to enhance readability have been introduced.

This report is organized as follows. Section 2 describes the basic definitions used in the standard as well as its scope of applicability. Section 3 introduces the functional safety management while Section 4 discusses the approach for hazard analysis and risk assessment. Section 5 introduces requirements of product development at the system, hardware and software levels, in addition to a brief summary discussing requirements for production, operation, service and decommissioning. Section 6 summarizes required supporting processes and provides a discussion on some safety analyses. Sections 7 and 8 introduce motorcycles specific and trucks and buses specific requirements, respectively. Section 9 provides guidance on semiconductor development. Finally, Section 10 provides a general summary.

2 – SCOPE OF APPLICABILITY AND DEFINITIONS

ISO 26262 is the adaptation of IEC 61508 [5] to comply with needs specific to the application sector of E/E systems within road vehicles. It applies to all activities during the safety lifecycle of system development and its scope includes all series production road vehicles. The latter is a modification of the scope of the first edition which limited the applicability to vehicles with 4 wheels (carrying passengers or goods) with a maximum vehicle gross mass of up to 3500 Kg.

ISO 26262 defines functional safety as the absence of unreasonable risk due to any potential source of harm caused by malfunctioning behavior of electrical and or electronic systems. A malfunctioning behavior is not limited to failures but also includes unintended behavior (with respect to design intent).

Figure 1 below describes how safety is defined in ISO 26262 as the absence of risk judged to be acceptable given valid societal and moral concepts. *Risk* itself is computed using three factors: severity, exposure (as measured by a probability) and controllability. It is worth emphasizing here that the concept of *harm* is defined in the context of injury or damage to humans.

Figure 2 below provides a classification of ISO 26262 specific terminologies starting with the item which is a system or combination of systems to which the standard applies. The item itself implements a given function at the vehicle level. The *system* is a set of components that relates at least a sensor, a controller and an actuator. *Components* are comprised of hardware parts and software units. The concept of an *element* is introduced to refer to a system, component, a hardware part and a software unit.

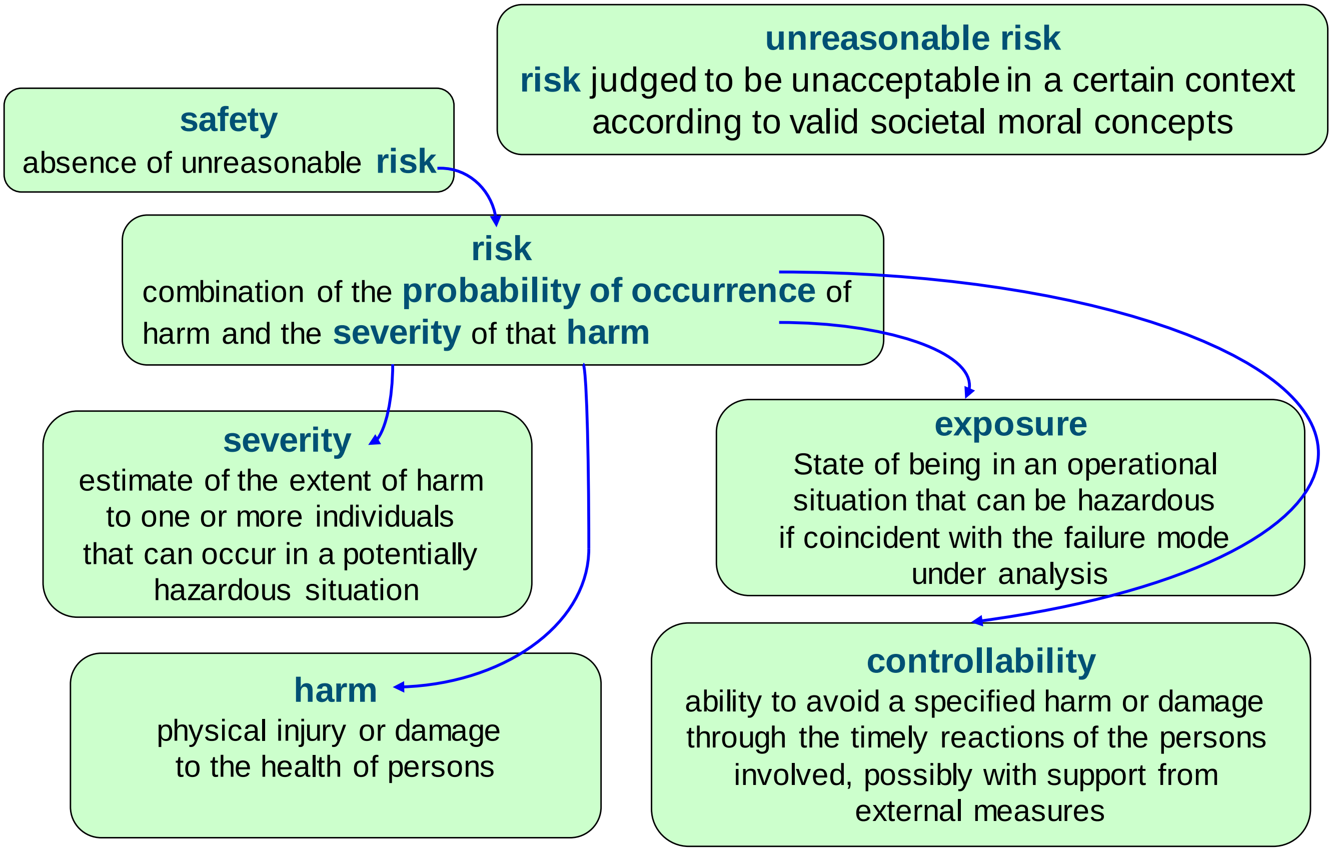

unreasonable risk
risk judged to be unacceptable in a certain context according to valid societal moral concepts
safety
absence of unreasonable risk
risk
combination of the probability of occurrence of harm and the severity of that harm
severity
estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation
exposure
State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis
harm
physical injury or damage to the health of persons
controllability
ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures

Figure 1: ISO 26262 definitions of safety and risk

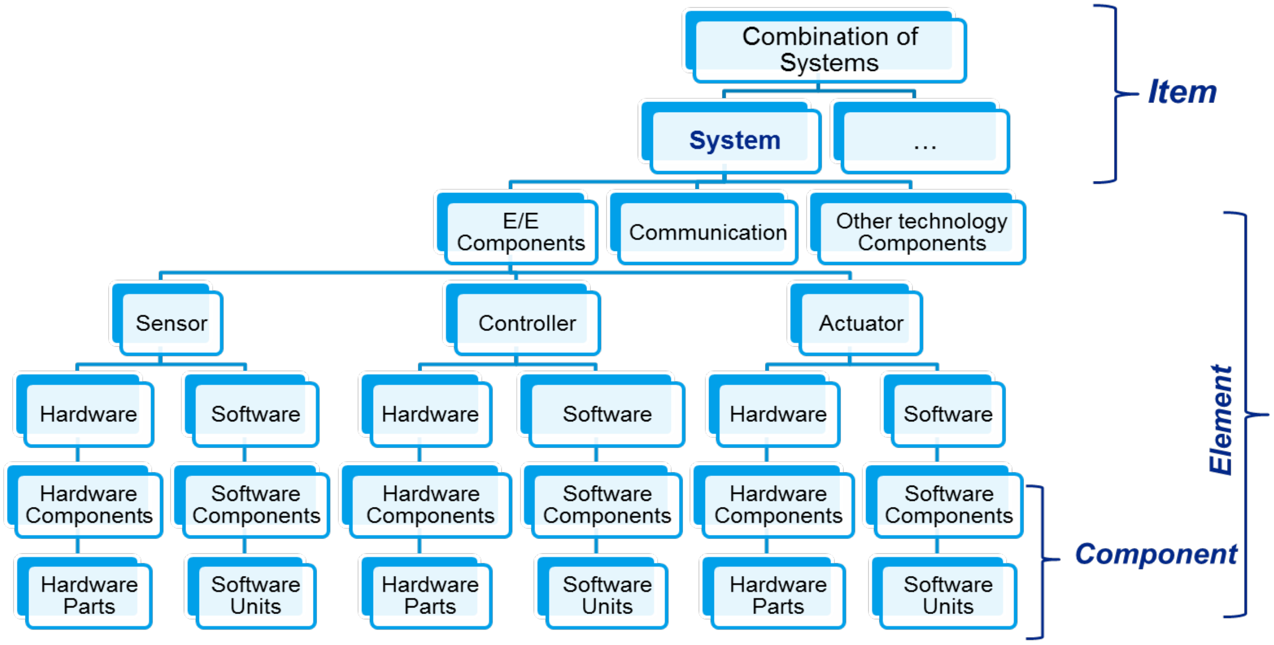


Figure 2: ISO 26262 Terminologies

Finally, the following are definitions of a few concepts introduced or emphasized by ISO 26262.

- Safety goal: top level safety requirement resulting from the hazard analysis and risk assessment as described in Section 4 below.
- Safe state: the mode of operation, without an unreasonable level of risk, of the item, following the occurrence of a failure
- Safety mechanism: technical solution to detect and mitigate (through avoidance or control) faults/failures in order to maintain intended functionality or achieve or maintain a safe state
- Work product: documentation that results from an ISO 26262 requirement(s)
- Confirmation review: confirmation that a work product provides sufficient and convincing evidence to the achievement of functional safety
- Safety case: documentation to communicate a clear, comprehensive and defensible argument (supported by evidence compiled in work products) that a system is acceptably safe to operate in a particular context

3 – FUNCTIONAL SAFETY MANAGEMENT

The functional safety management involves planning, coordinating and documenting all activities related to functional safety. In general, it involves the following as pictured in Figure 3:

- establishing an internal functional safety process for the company,
- establishing a safety organization that oversees the institutionalization of a safety culture within the company and the definition of roles and responsibilities within that organization
- training and qualifying employees to perform safety activities
- institutionalizing the functional safety confirmation measures including reviews, audits and assessments
- managing all the corresponding documentation aspects

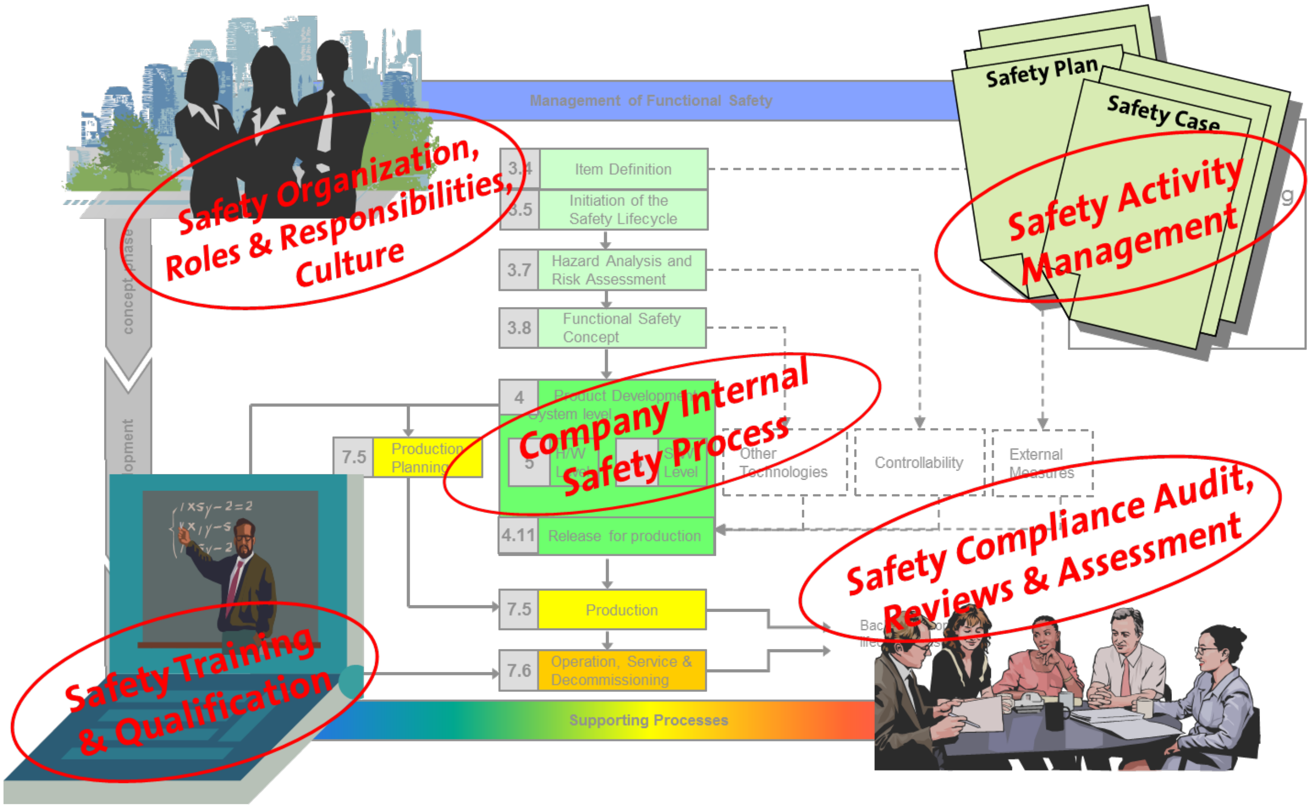

Management of Functional Safety
Safety Plan
Safety Case
Safety Organization, Roles & Responsibilities, Culture
Safety Activity Management
concept phase
3.4 Item Definition
3.5 Initiation of the Safety Lifecycle
3.7 Hazard Analysis and Risk Assessment
3.8 Functional Safety Concept
4 Product Development System level
5 H/W Level
6 S/W Level
Company Internal Safety Process
Other Technologies
Controllability
External Measures
7.5 Production Planning
4.11 Release for production
7.5 Production
7.6 Operation, Service & Decommissioning
Safety Compliance Audit, Reviews & Assessment
Safety Training & Qualification
Supporting Processes

Figure 3: Management of functional safety

Part 2 of ISO 26262 discusses implementing a management plan for all phases of the safety lifecycle, including:

- the overall safety management
- the project dependent safety management
- the safety management for production, operation, service and decommissioning

Overall safety management: involves defining requirements for organizations that are responsible for or perform safety activities in the safety lifecycle. A management plan is put forward to incorporate:

- institutionalization of the safety culture
- effective communication channels between functional safety and cybersecurity (new topic introduced in the 2nd Edition of ISO 26262)
- organization-specific rules and processes
- processes to resolve safety anomalies
- competence management
- quality management
- project-independent tailoring of the safety lifecycle

Project-dependent safety management: involves defining requirements for the safety management during the concept and development phases of a project including roles and responsibilities, as well as performing an impact analysis at the item level in case of a modified/re-used item. A management plan is put forward to incorporate:

- roles and responsibilities in safety management
- impact analyses and tailoring of the safety activities
- planning and coordinating of the safety activities
- progression of the safety lifecycle
- safety case development
- confirmation measures

It is worth mentioning here that the impact analyses and tailoring of the safety activities have been added to the functional safety management of a given project compared to them being performed at different phases of development as required by the 1st Edition of ISO 26262. Moreover, the confirmation reviews (part of the confirmation measures) have been re-defined to provide sufficient and convincing evidence to the achievement of functional safety, an objective oriented approach compared to the prescriptive definition in the 1st Edition of ISO 26262 to meet requirements.

Safety Management for production, operation, service and decommissioning: involves defining responsibilities of persons and organizations in charge for achieving and maintaining functional safety regarding production, operation, service and decommissioning. For instance, requirements are established to appoint persons to execute processes to achieve and maintain the functional safety of the item regarding field monitoring and collection of data.

4 – HAZARD ANALYSIS AND RISK ASSESSMENT

In Part 3 of ISO 26262, potential hazards are identified following an analysis of the operational situations of the item. The item may be a vehicle, a vehicle system, or a vehicle function. The identified potential hazards are then categorized based on the following factors: severity, probability of exposure and controllability. Following the categorization results, an *Automotive Safety Integrity Level or ASIL* is determined for the potential hazard. The ASIL is also assigned to the safety goal(s) formulated to prevent or mitigate the potential hazard, in order to avoid unreasonable risk. Risk reduction (safety) requirements or safety requirements are then derived from these safety goals and inherit the corresponding ASIL. The following provides a brief overview of these activities and the reader is referred to [7] for a detailed account.

Situation analysis and hazard identification: The potential hazards are determined given the operating modes of the item in which a malfunctioning behavior may trigger them. The hazards are described and evaluated and their consequences are identified and documented.

Hazard Classification: The identified potential hazards are classified based on the estimation of severity, probability of exposure, and controllability as defined in Section 2 above. Severity or S has 4 classes ranging from S0 or no injuries to S3 or fatal injuries. Exposure or E ranges from an E0 or extremely unusual situation to E4 or a highly likely situation. Finally, controllability C ranges from C0 or simply controllable to uncontrollable or C3.

ASIL Determination: An ASIL is to be determined for each hazardous event using the parameters S, E and C as shown in Table 1 below. Four ASILs are defined, where ASIL A is the lowest safety integrity level and ASIL D the highest one. In addition to these four ASILs, the class QM (Quality Management) denotes no requirement in accordance with ISO 26262, however any other requirements such as Quality, Reliability, and Durability need to be accounted for.

Table 1: ASIL Determination (Source ISO 26262 2nd Ed. FDIS – Draft)

		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

Safety goal formulation: A safety goal is to be determined for each hazardous event evaluated in the hazard analysis. Functional safety requirements needed to avoid an unreasonable risk for each potential hazard are derived from these safety goals which are not expressed in terms of technological solutions, rather in terms of functional objectives. Functional safety requirements inherit the ASIL of the safety goal from which they are derived.

The ASIL determined for the hazardous event is assigned to the corresponding safety goal. A potential hazard may have more than one safety goal, and if similar safety goals are determined, they can be combined into one safety goal that will be assigned the highest ASIL of the similar goals.

5 – PRODUCT REQUIREMENTS AT SYSTEM, HARDWARE AND SOFTWARE LEVELS

The product development at the system level starts with developing the technical safety concept. The technical safety concept specifies the technical safety requirements and their allocation to system elements (hardware and software). The technical safety concept defines the system architectural design as well. The development of the technical safety concept is then detailed at both the hardware and software levels. Once the hardware and software development is complete, all elements are integrated and tested. Finally, safety validation is completed at the vehicle level, that is evidence is provided that safety goals have been met. This is graphically represented in Figure 4 and detailed in the following.

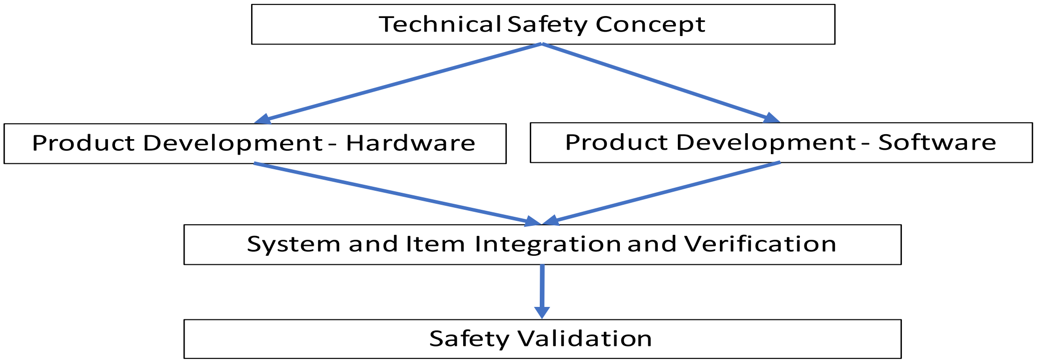

Technical Safety Concept
Product Development - Hardware
Product Development - Software
System and Item Integration and Verification
Safety Validation

Figure 4: Product development at the system level

Technical safety concept: the technical safety concept comprises all technical safety requirements. These requirements are the technical refinement of their corresponding functional safety requirements: they specify safety mechanisms to detect faults and mitigate or control failures that may lead to the violation of these functional safety requirements and hence the safety goals. These technical safety requirements inherit the ASIL of the functional safety requirements they refine. In addition, a system architectural design that implements the technical safety requirements is defined as part of the technical safety concept and is supposed to be suitable to satisfy the safety requirements according to their respective ASIL.

In defining technical safety requirements, some of these requirements may come from a cybersecurity concept as a result of the established channels of communication between functional safety and cybersecurity discussed in the functional safety management summary above. Moreover, some technical safety requirements are derived to address safety issues during production, operation, service and decommissioning.

Product development at the hardware level: at this level a hardware implementation of the technical safety concept is specified and safety analyses are performed to identify potential faults and their effects on the violation of safety requirements. In addition, any required coordination with development at the software level is identified.

The hardware implementation of the technical safety concept involves identification of hardware requirements or in other words assignment from technical safety requirements to hardware elements given the system architectural design. The hardware design itself is supposed to be consistent with the system architectural design specification and fulfils the hardware safety requirements while protecting for safety concerns considering the performed safety analyses. The suitability of the hardware architectural design (to detect and control random hardware failures) is assessed using two metrics, single fault metric and latent fault metric. Both metrics have target values depending on the ASIL of the requirements being implemented. An alternative approach to assess the suitability of the hardware architectural design (to detect and control random hardware failures) is to evaluate the probability of safety goals violation. The latter can be completed using a global probabilistic approach or by analyzing individual cut sets. In both cases the assessment is also dependent on the ASIL of the safety goal.

Finally, once all hardware elements are integrated, a verification of the compliance of the hardware design with the hardware safety requirements (given their respective ASILs) is expected.

Product development at the software level: at this level of development software safety requirements are derived from technical safety requirements and a software architecture that satisfies all software requirements is developed. In addition, any required coordination with development at the software level is identified and/or refined.

Similar to hardware requirements, software safety requirements are derived from the technical safety concept and the system architectural design specification. These requirements inherit the ASIL of their respective technical safety requirements, in general. The software architectural design is required to be suitable to satisfy the software safety requirements with their respective ASILs and support the implementation and verification of the software being developed. The latter includes the software unit design, implementation and verification; the software integration and verification; and the testing of the resulting embedded software.

System and item integration and verification: the integration steps are defined for all levels of integration including integration of hardware and software of an element, integration of elements resulting in an item, and integration of the item with other systems at the vehicle level. Evidence that the integrated system elements fulfil their safety requirements is also provided. Finally, the proper implementation of safety mechanisms is verified.

Safety validation: this final step as part of the system product development provides evidence that the safety goals are achieved at the vehicle level and that the developed safety concepts are appropriate for the functional safety of the item. Validation of safety goals is applied to the item integrated at the vehicle level and the validation plan includes test procedures for each safety goal with a pass/fail criterion.

As discussed earlier, some technical safety requirements address safety concerns related to production, operation, service and decommissioning. The objective of these requirements is to ensure that functional safety is achieved throughout the whole lifecycle of the vehicle.

As part of planning for production, operation, service and decommissioning, it is required to develop:

- a production process for safety-related system(s) to be installed in road vehicles
- all necessary information and documentation regarding operation, maintenance and repair, and decommissioning to be used by whomever is interfacing with the safety-related system(s)

In addition to the planning, the production process needs to be analyzed to uncover any process failures and their effects on achieving functional safety and implement and verify the effectiveness of measures to mitigate or control these process failures. Related to the information and documentation for operation, maintenance and repair, and decommissioning, a field monitoring process needs to be established to address potential safety-related incidents related to the system(s) with the objective of collecting field data that can be analyzed to detect the presence of functional safety issues and initiate corrective actions for these issues.

6 – SUPPORTING PROCESSES AND SAFETY ANALYSES

Supporting processes are usually labelled as "secondary processes" that come along with the core processes and contribute indirectly in delivering a product. For functional safety, ISO 26262 identified a dozen of these processes each containing a set of consolidated common requirements. The following briefly discusses a few of those supporting processes and the reader is referred to Part 8 of ISO 26262 for a detailed discussion of all the supporting processes.

Interfaces within distributed developments: define the interactions and dependencies between integrators and suppliers for development activities and describe corresponding allocation responsibilities. In addition, it provides a means to evaluate the supplier's capability to develop and produce items of comparable complexity and ASIL according to ISO 26262. The Distributed Interface Agreement (DIA) includes requirements on:

- Safety managers at the integrator's and supplier's
- Joint tailoring of the safety lifecycle, with identification of activities and processes to be performed by the customer and by the supplier;
- The information required; work products to be exchanged; persons responsible
- …

Specification and management of safety requirements: ensures correct specification of safety requirements with respect to attributes and characteristics and support consistent management of safety requirements throughout the safety lifecycle. These are achieved by defining requirements on the notations used for the specification of safety requirements; attributes, characteristics and properties of safety requirements; and how the safety requirements are managed.

Confidence in the use of software tools: provides criteria to determine the required level of confidence in a software tool and means for the qualification of that software tool. A tool confidence level (TCL) is determined based on analysis, the tool impact and the tool error detection. Given the TCL, ISO 26262 describes methods to be applied to qualify the software tool given the ASIL of the safety goal(s).

Qualification of software components: provides evidence for the suitability of the software components for re-use in items developed per the ISO 26262 standard. ISO 26262 requires information to treat a software component as qualified (specification of the software component, evidence that the software component complies with its requirements and is suitable for its intended use, and evidence of an appropriate software development process) and prescribes requirements on the verification of the qualification of the software component.

Evaluation of hardware elements: ensures that the element functional behavior is adequate to meet its allocated safety requirement(s). This type of evaluation is used for COTS parts not developed per ISO 26262 or considered safety-related once integrated into an item. In addition, it can be used as an alternative means of compliance with the product development requirements at the hardware level. Different classes are considered depending on the difficulty of the verification of the safety-related functionality and the role of the hardware element within the safety concept. The evaluation is carried through either testing, testing and analysis, or testing, analysis and argumentation.

Part 9 of ISO 26262 provides an overview of some types of safety analyses. The following briefly describes an ISO 26262 specific method for decomposing requirements.

Requirements decomposition with respect to ASIL tailoring: shortly known as ASIL Decomposition, is a method to decompose safety requirements into redundant safety requirements (not necessarily identical) to allow ASIL tailoring at the next level of detail. The redundant requirements are allocated to sufficiently independent design elements. It is worth noting here that even though the development of the design elements to which the redundant requirements are allocated is performed at the decomposed ASIL level, the evaluation of the hardware metrics and the safety goal violations targets due to random hardware failures remains unchanged by ASIL decomposition. Table 2 below provides the rules for ASIL decomposition. These rules can be applied iteratively as long as traceability is maintained.

Table 2: ASIL Decomposition rules

ASIL A	ASIL B	ASIL C	ASIL D
ASIL A(A) + QM(A)	ASIL B(B)+ QM(B)	ASIL C(C)+ QM(C)	ASIL D(D)+ QM(D)
	ASIL A(B)+ ASIL A(B)	ASIL B(C)+ ASIL A(C)	ASIL C(D)+ ASIL A(D)
			ASIL B(D)+ ASIL B(D)

7 – MOTORCYCLES

Part 12 is a new addition to ISO 26262 2nd Edition to give an overview of the adaptation of the standard to motorcycles that were out of scope in the 1st Edition. All requirements of Parts 2 through 9 in ISO 26262 apply to motorcycles, however some tailoring is required. Therefore, requirements in Part 12 supersede the corresponding requirements in all other parts.

The major adaptation of requirements in the case of motorcycles applies to the development of the hazard analysis and risk assessment and the determination of the S, E, and C parameters. A motorcycle specific hazard analysis is performed and accounts for

- The dynamic behavior of motorcycles which differs greatly from other vehicles
- Motorcycle rider dependence to achieve controllability
- Motorcycle specific operational situations and hazard identification

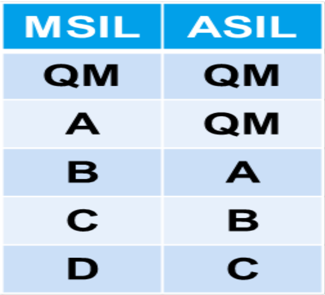
As part of the hazard analysis and risk assessment, a Motorcycle Safety Integrity Level (MSIL) is determined for each hazard from the combination of a motorcycle specific S, E and C of the hazardous event. The MSIL is later mapped to the ASIL as depicted in below and safety goals are assigned to the mapped ASIL and from there onwards confirmation reviews, vehicle integration and testing, and safety validation are performed given the ASIL.

8 – TRUCKS, BUSES, TRAILERS, AND SEMI-TRAILERS

Truck, Buses, Trailers and Semi-trailers (T&B for short) have been added to the scope of the standard in its 2nd Edition version. Similar to motorcycles, requirements of Parts 2 through 9 apply to T&B and any specific modification or new requirements for T&B are listed within the parts of the standard wherever they apply. Additional requirements are listed under:

- Functional safety management – supporting processes
- Hazard analysis and risk assessment
- System level validation environment
- Production, operation, service and decommissioning

Table 3: MSIL to ASIL mapping



MSIL	ASIL
QM	QM
A	QM
B	A
C	B
D	C

Before discussing T&B specific requirements, it is worth noting here that in the context of T&B a body builder is an organization that adds its own equipment to a base vehicle such as a machine, body, or cargo carrier. Consequently, the body builder becomes the integrator in the case of a T&B while the role of the original equipment manufacturer of the base vehicle is relegated to that of a supplier.

As part of the functional safety management in the case of T&B, a tailoring of safety activities is required when a:

- T&B related application that is out of Scope of ISO 26262 is being interfaced with a base vehicle that has been developed in accordance with ISO 26262, or a
- T&B related system not developed according to ISO 26262 is to satisfy the required

level of functional safety needed for the integration into an item developed in accordance with ISO 26262.

In these specific situations, some manufacturer-supplier or DIA requirements do not apply.

Interfacing an application that is out of scope of ISO 26262: an application out of scope of ISO 26262 is supposed not to violate the safety goals of the base vehicle that has been developed in accordance with ISO 26262. In that specific situation, It is required that the integrator is made aware of the modified systems and the permitted safety limits / requirements of the modifications by the manufacturer/supplier. The manufacturer/supplier is in fact responsible to communicate safety measures required to be applied by the integrator so that functional safety is maintained.

Integration of safety-related systems not developed according to ISO 26262: a development not according to ISO 26262 satisfies the required level of functional safety needed to be integrated into an item developed according to ISO 26262. In that specific situation, the integrator is required to define the criteria to argue that the safety-related system that has been developed to another safety standard meets the required level of functional safety. Consequently, the integrator and the supplier are required to agree on the relevant set of measures to verify that the criteria are met.

Hazard analysis and risk assessment: in the context of T&B, variances of T&B vehicle operation are defined as the use of a T&B vehicle with different dynamic characteristics influenced by cargo or towing during the service life of the vehicle. As a consequence, while performing the hazard analysis and risk assessment, the following variances are to be considered:

- type of base vehicle;
- the T&B vehicle configuration; and
- the T&B vehicle operation.

This will impact the operational situations, hazardous events and the S, E, and C classification.

System level validation environment: since the safety goals are validated for the item in a representative context at the vehicle level, then different base vehicle types in the case of T&B could be the subject of a safety validation.

Operation, service and decommissioning: the operation, service and decommissioning of the item is required to be conducted and documented in accordance with the service plan, instructions for service, and instructions for decommissioning. Such a requirement is important for T&B since elements of T&B can be remanufactured and corresponding plans and instructions can be modified. Therefore, it is required that all the right plans and instructions are maintained and documented.

9 – GUIDANCE ON SEMICONDUCTOR DEVELOPMENT

With the introduction of the 1st Edition of ISO 26262, semiconductor manufacturers were not well versed in the area of automotive functional safety. That resulted in some confusion in early application of the standard to semiconductor components. A project was launched within the working group developing ISO 26262 to assess and understand the impact of applying the standard to semiconductors. Two publicly available specifications were developed to address these issues [8,9] and these became the origins of Part 11 in ISO 26262 2nd Edition.

Part 11 of ISO 26262 2nd Edition is an informative part and a necessary extension of the 1st Edition of ISO 26262 to provide guidelines for semiconductors used in automotive application. It provides guidelines on semiconductor components and semiconductor technologies. A semiconductor component can be developed as:

- part of the item – in that case the safety analysis performed per the product development at the hardware level applies, or
- as a Safety Element out of Context (SEooC) – in that case the development is assumed to meet a given ASIL independent of an item and its safety goals and is based on assumptions to be verified at integration. If these assumptions are indeed verified then the SEooC can be integrated into an item without further safety analyses.

10 – SUMMARY

ISO 26262 in its second edition is expected to be released later this year. In this report, we summarized the content of the standard including its scope of applicability, definitions, and requirements per its core and supporting processes as well as some guidelines provided for semiconductor development. While presenting the summary, a few major modifications and additions were discussed. This summary is intended to be informative and is not intended to be a substitute to read the standard in order to apply it.

REFERENCES

1. C. A. Ericson II, Hazard Analysis Techniques for System Safety, John Wiley & Sons, New Jersey, 2005.

2. N.G. Leveson, Safeware: System Safety and Computers, Addison Wesley, 2001.

3. N.J. Bahr, System Safety Engineering and Risk Assessment: A Practical Approach, Taylor and Francis, 1997.

4. ISO 26262 1st Ed., TC 22/SC3/WG16, Road Vehicles – Functional Safety Parts 1-9", Nov 2011.

5. IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems Parts 1-7, International Electrotechnical Commission, Switzerland, 1998.

6. ISO/FDIS 26262 2nd Ed., TC 22/SC32/WG08, Road Vehicles – Functional Safety Parts 1-12", Mar 2018.

7. R. Debouk and J. Joyce, ISO 26262 Hazard and Risk Assessment Methodology, Proceedings of the 28th International System Safety Conference, August 2010.

8. ISO/PAS 19451-1: Application of ISO 26262:2011-2012 to semiconductors — Part 1: Application of concepts, 2016

9. ISO/PAS 19451-2: Application of ISO 26262:2011-2012 to semiconductors — Part 2: Application of hardware qualification, 2016