Quint Safety

ISO26262: The impact of ASIL C safety goals on product design

Stephen Norton, Quint Safety GmbH

Abstract

This whitepaper addresses the impact of ASIL C and ASIL D safety goals on the design of electronic products. It compares the requirements where the safety goals are ASIL B or lower with the requirements where at least one safety goal is ASIL C or higher.

Contents

1. Introduction

Since 2011, the ISO 26262 [1] "Functional Safety for Road Vehicles" is applicable for all automotive (electrical, programmable) electronic products. A "Hazard Analysis and Risk Assessment" (HARA) has to be performed by the vehicle manufacturer (OEM) for every "Item". If an item, or an element of that item is assigned one or more safety goals rated ASIL A or higher, then Functional Safety Management processes must be applied to the product development. The effort required to achieve functional safety increases dramatically from ASIL B to ASIL C.

2. Product Liability

At time of writing, the ISO 26262 [2] has not been introduced into national or international legislation. Compliance with ISO 26262 is not directly a legal requirement: non-compliance in itself cannot be prosecuted. Therefore, no requirement in ISO 26262 can be considered as "mandatory". However, if a product causes injury to a person, then the manufacturer of the product may be liable for damages. Hazards rated by the HARA as "QM" may still be safety relevant and thus potential sources of product liability.

If a liability claim is made, the manufacturer of the product must demonstrate that the product was designed according to the "state-of-the-art in *science* and technology" at the time of *entry-to-market*. International standards define only the minimum of processes, activities and documentation to be performed.

It is already the state-of-the-art to perform many of the activities and to implement many of the recommendations that are defined in ISO 26262 as optional or "informative" text. For example, although the whole of ISO 26262 – Part 10 is defined as "informative", the information contained, including FTTI/EOTTI, safety case, fault classification and SEooC, is very much state-of-the-art. When authorising the release for (series) production, the supplier of a product should therefore ensure not only the compliance with ISO 26262, but also that the product safety is achieved according to the current state-of-the-art in science and technology.

It is best practice to include a justification in the product safety case for every requirement (and informative text) that is not implemented. As a rough guideline for the minimum of justification, the author recommends:

- "0" / informative text — *1 line*
- "+" / recommended — *1 paragraph*
- "++" / highly recommended — *1 page*

3. Safety Management

[ISO 26262-2:2018 §6.4.11.1] It is *recommended* to perform a Functional Safety Audit of the engineering and safety processes for projects with at least one safety goal of ASIL B or higher. It is *highly recommended* to perform the Functional Safety Audit when at least one safety goal is ASIL C or higher.

[ISO 26262-2:2018 §6.4.12.1] It is *recommended* to perform a Functional Safety Assessment of the achieved safety for products with at least one safety goal of ASIL B or higher. It is *highly recommended* to perform a Functional Safety Assessment of the achieved safety for products when at least one safety goal is ASIL C or higher.

[ISO 26262-2:2018 §6.9.4.1] For both the Functional Safety Audit and Assessment there are requirements for the independence of the auditor/assessor. For ASIL B the four-eyes rule applies, but there is no requirement for organisational independence. For ASIL C the auditor/assessor must be from an independent team, having a different disciplinary line manager from the author(s) of the work products. For ASIL D the auditor/assessor must be from an independent department, having different management, resources and release authority from the author(s) of the work products. The same levels of independence apply for all other confirmation measures (except Impact Analysis and HARA).

In the experience of the author, most manufacturers perform at least a limited Functional Safety Assessment for safety goals with ASIL A to detect and avoid potential product liability issues. It is very rare for a manufacturer not to perform the Functional Safety Assessment when one or more safety goals are ASIL B or higher.

The effort to perform the Functional Safety Audit and Assessment is determined primarily by the complexity of the product design, the number of safety goals, technical safety requirements and safety mechanisms to be implemented. It is not necessarily the case that a product with an ASIL C safety goal is more complex than a product with safety goals of ASIL B or lower.

4. Notation

[ISO 26262-8:2018 §6.4.1] For ASIL A and ASIL B it is sufficient to use informal notation to specify system requirements and architecture. For ASIL C and ASIL D it is *highly recommended* to use semi-formal notation to specify system requirements and architecture.

It is state-of-the-art to use UML® or SysML® for semi-formal notation. It will soon be state-of-the-art to use a subset of SysML® developed for the automotive industry called "Safety Concept Description Language" (SCDL) [3].

Semi-formal methods are more rigorous and thus incur more process effort for the project team. There is therefore an increase in the process cost to implement safety goals of ASIL C or higher in a product.

It is the experience of the author that most automotive suppliers struggle with the organisational and process changes when implementing semi-formal methods for the first time. Therefore, the impact of introducing an ASIL C safety goal into a product will be significantly higher the first time the team or the company is designing a product with ASIL C safety goals.

5. Technical Safety Concept

It is *highly recommended* to define technical safety requirements and implement safety measures to prevent the violation of all safety goals rated ASIL A or higher.

[ISO 26262-4:2018 §6.4.2.1] "The technical safety requirements shall specify the safety mechanisms that detect faults and prevent or mitigate failures present at the output of the system that violate the functional safety requirements."

[ISO 26262-4:2018 §6.4.2.3] For ASIL A and ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* to specify safety mechanisms to prevent faults from being latent.

[ISO 26262-4:2018 §6.4.2.4] For ASIL A and ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* to avoid multiple-point failures by specifying a test strategy for each safety mechanism implemented to detect multiple point faults.

[ISO 26262-4:2018 §6.4.2.5] For ASIL A and ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* that (additional) safety mechanisms implemented to prevent dual-point faults being latent shall be (developed to) at least

- ASIL B for a safety (goal) with ASIL D;
- ASIL A for a safety (goal) with ASIL B / ASIL C;
- QM for a safety (goal) with ASIL A.

"EXAMPLE: A memory has a parity as its safety mechanism, with requirements rated ASIL B. The requirement for the self-test that tests the capability of the parity to detect and signal memory faults can be rated ASIL A."

Interpretation: The requirement to implement detection measures for detecting latent dual-point failures implies that only applying detection measures to a single-point fault would be insufficient for safety goals/requirements with ASIL C and ASIL D. If so, the architecture must be such that single-point failures cannot lead directly to a violation of ASIL C and ASIL D safety goals.

[ISO 26262-4:2018 §6.4.4.1] It is *highly recommended* to perform inductive (bottom-up) analysis, such as an FMEA for all safety goals rated ASIL A or higher. For ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* to perform deductive (top-down) analysis, such as an FTA.

[ISO 26262-4:2018 §6.4.4.2, §6.4.4.3] The causes of internal and external failure shall be eliminated, or their effects mitigated to comply with the safety goals or requirements.

Interpretation: If a failure cannot be eliminated by design, then the design has to be modified so that the failure is detected and its effect mitigated. A safety mechanism tries to prevent the failure leading directly to a safety goal violation.

[ISO 26262-4:2018 §6.4.5.2, §6.4.5.3] For ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* to select a method and define target values for the hardware metrics, safety-goal violating failure rates and diagnostic coverage.

[ISO 26262-4:2018 §6.4.9.2] For ASIL A, it is sufficient to perform verification of the system requirements and architecture by a walkthrough. For ASIL B, ASIL C and ASIL D it is *highly recommended* to perform verification of the system requirements and architecture by inspection. For ASIL A and ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* to perform simulation, system prototyping and vehicles tests.

6. Hardware Safety Mechanisms

ISO 26262 defines categories of failures that can lead to safety goal violations and permitted rates of failure for each category:

No Safety Mechanism	After Safety Mechanism added
Single Point Fault	Residual Fault
Multiple Point Fault	Latent Fault

As noted in §5, it is required to implement safety measures to prevent the violation of all safety goals rated ASIL A or higher. However, no detection or mitigation measure can prevent 100% of the safety goal violations. The gap in diagnostic coverage and failures in the detection and mitigation measures still lead to the safety goal violation.

After applying detection and mitigation to a single point fault, the remaining failure rate leading to safety goal violation is called the residual fault. Since it has the same effect (but less often) than the signal point fault, the rates are added together when calculating the Single Point Fault Metric (SPFM).

Independent multiple point faults do not immediately lead to safety goal violations. However, without detection, these faults could persist indefinitely, and thus their failure rates are assigned 100% to the latent fault metric. After applying detection and mitigation to a multiple point fault, only the remaining (undetected or unmitigated) failure rate is assigned to the latent fault metric.

[ISO 26262-5:2018 §6.4.8] "The hardware safety requirements shall comply with the *multiple-point fault detection* interval as specified in ISO 26262-4:2018, §6.4.2. NOTE 1 In the case of ASIL C and D safety goals, and if the corresponding safety concept does not prescribe specific values, the *multiple-point fault detection* intervals can be specified to be equal to or lower than the item's "power-up to power-down" cycle."

Interpretation: The requirement to comply with the multiple-point fault detection interval implies that the architecture for ASIL C and ASIL D safety goals should not have single-point or residual failures.

[ISO 26262-5:2018 §7.4.3.3] For ASIL A and ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* to provide "evidence of the effectiveness of implemented safety mechanisms to prevent faults from leading to single-point failures or to reduce residual faults."

[ISO 26262-5:2018 §7.4.3.4] For ASIL A and ASIL B it is *recommended*; for ASIL C and ASIL D *highly recommended* to provide "evidence of the effectiveness of implemented safety mechanisms to prevent a fault from being latent."

Interpretation: The challenge in the first requirement is how to understand "reduce residual faults". The implication of the second requirement is that the safety mechanism for ASIL C and ASIL D safety goals has a (latent) multiple-point fault. Therefore, a safety mechanism that only detects a single-point fault, converting it to a residual fault would be insufficient.

[ISO 26262-5:2018 §9.4.1.2] For ASIL C and ASIL D it is *highly recommended* that a "hardware part's single-point fault shall only be considered acceptable if an argument for its sufficiently low probability of occurrence is provided by one of the following options:

a) dedicated measures are taken;

b) for a safety goal ASIL D, the following criteria are satisfied: a conservative data source is used, only a small portion of the failure rate (e.g. one particular failure mode) can violate the safety goal, and the resulting single-point fault failure rate is smaller than one-tenth of the value corresponding to failure rate class 1; [$< 10^{-11}$ /h]

c) for a safety goal ASIL C, the following criteria are satisfied: a conservative data source is used, only a small portion of the failure rate (e.g. one particular failure mode) can violate the safety goal, and the resulting single-point fault failure rate is smaller than one-tenth of the value corresponding to failure rate class 2." [$< 10^{-10}$ /h]

Note: Only option a) was included in the 1st Edition.

The primary impact between ASIL B and ASIL C safety goals is therefore the complexity and the cost of the detection and mitigation measures: for higher ASIL ratings, ISO 26262 requires higher levels of diagnostic coverage and lower failure rates leading to safety goal violations.

It is a possible interpretation that ISO 26262 *implies* the need for a redundant safety path to prevent single or residual faults violating ASIL C and ASIL D safety goals. However, there is no requirement in ISO 26262 to convert single-point faults into multiple-point faults by modifying the architecture. The ISO 26262 explicitly requires *justification* in the safety case for the existence of single point failures that could violate safety goals with ASIL C or ASIL D.

The design team must choose how to mitigate single-point faults that violate safety goals by either modifying the architecture to convert them to multiple-point faults, or by providing a justification for the probability of occurrence. Acceptable justifications generally are based on dedicated measures or particularly low probability of occurrence. It is not sufficient justification just to achieve the SPFM, LFM or PMHF metrics.

7. Conclusions

(1) The increase in effort between a safety goal with ASIL B and a safety goal with ASIL C occurs in two categories: process-effort and product-cost (NRC of design, RC of parts).

(2) In the experience of the author (see §3), it is common practice to perform, and thus already incur the costs of, Functional Safety Audits and Assessments for products with safety goals from ASIL B.

(3) The effort and thus the costs of performing audits and assessments are proportional to the complexity of the processes and the product, which may or may not be proportional to the ASIL rating of the safety goals.

(4) The process-cost increases from ASIL B to ASIL C safety goals/requirements due to the change from informal to semi-formal methods for notation and verification.

(5) There may be a significant, additional increase in process-cost (see §4) if the team or the company is designing a product with ASIL C safety goals for the first time.

(6) The ISO 26262 requires (see §5) to define technical safety requirements and implement safety measures to prevent the violation of all safety goals rated ASIL A or higher.

(7) The ISO 26262 explicitly requires justification in the safety case for the existence of single point failures that could violate safety goals with ASIL C or ASIL D. Acceptable justifications (see §5) may be based on dedicated measures or particularly low probability of occurrence. It is not sufficient justification just to achieve the SPFM, LFM or PMHF metrics.

(8) In the opinion of the author, it would be highly advisable to have the arguments and evidence of such justifications in the safety case confirmed in a Functional Safety Assessment performed by a competent, neutral, independent 3rd party organisation. This would reduce both the risk of potential issues remaining unnoticed by the team and also the liability risk due to potentially controversial justifications.

(9) Since many products implement architectures with a second safety path to mitigate faults that could violate ASIL C and ASIL D safety goals, this could be considered as defining the state-of-the-art. A design that does not prevent single or residual faults from violating ASIL C and ASIL D safety goals might therefore be compliant with ISO 26262, but not be "state-of-the-art". If an injury were caused by such a product, the manufacturer of the product might then be liable for damages.

8. Glossary

Abr.	Term	Definition
EOTTI	Emergency Operation Tolerance Time Interval	Transient state to extend the time available to safely reach the safe state.
FTTI	Fault Tolerant Time Interval	The time interval following occurrence of a fault, after which a a hazardous event can occur.
HARA	Hazard Analysis & Risk Assessment	Evaluation of Hazards at vehicle-level, caused by malfunctioning behaviour of an item in certain situations, based on severity, exposure and controllability.
/	Item	ISO 26262 term: A system or array of systems at vehicle-level.
OEM	Original () Manufacturer	Common term in automotive industry for the vehicle manufacturer.
/	Safety Case	An argument how the evidence (included) demonstrates that the product is sufficiently safe, including evidence of compliance for all safety-relevant activities (design, verification, process audits, supplier audits, assessments) and the competence of the persons involved in those activities.

9. References

[1] ISO 26262, 1st Edition: Parts 1-9 2011, Part 10 2012.
[2] ISO 26262, 2nd Edition, 2018-12.
[3] Safety Concept Description Language (SCDL), Version 1.5, 09.01.2020, scn-sg.com