Safety and Reliability

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tsar20

Mapping to IEC 61508 the hardware safety integrity of elements developed to ISO 26262

Peter Okoh & Thor Myklebust

To cite this article: Peter Okoh & Thor Myklebust (2024) Mapping to IEC 61508 the hardware safety integrity of elements developed to ISO 26262, Safety and Reliability, 43:2, 114-130, DOI: 10.1080/09617353.2024.2343959

To link to this article: https://doi.org/10.1080/09617353.2024.2343959

Published online: 09 May 2024.

SAFETY AND RELIABILITY
2024, VOL. 43, NO. 2, 114–130
https://doi.org/10.1080/09617353.2024.2343959

Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS

Check for updates

Mapping to IEC 61508 the hardware safety integrity of elements developed to ISO 26262

Peter Okoh[a] and Thor Myklebust[b]

[a]Autronica Fire and Security, Trondheim, Norway; [b]SINTEF Digital, Trondheim, Norway

ABSTRACT

Over the years, several functional safety standards for industries that handle safety electrical, electronic and electromechanical systems have been developed from IEC 61508 (generic). These include ISO 26262 (automotive), IEC 61511 (process), EN 50129 (railway), IEC 620621 (machinery), IEC 61513 (nuclear), etc. The emergence of these standards gives to the associated industries domain-specific identities. However, in certain cases, the rate of updating the standards is greatly overtaken by the rapid evolution of new technologies with a high potential to obsolete existing designs. Besides, IEC 61508-based critical components may experience shortage in the event of a global disaster as seen during the Covid-19 pandemic, hence the need for a robust substitution means. To address these problems, the concept of cross-domain reuse of resources is being promoted between industries that have unequal pace of alignment to the state-of-the-art. However, the framework for domain-to-domain (D2D) exchange must be clearly defined to avoid confusion. The objective of this paper is to investigate whether and how safety levels defined in ISO 26262 (automotive) can be mapped to safety levels in IEC 61508. The paper builds on review of literature and standards and is delimited to hardware elements.

ARTICLE HISTORY 18 July 2023; 28 March 2024; 5 April 2024

KEYWORDS Automotive; industrial; railway; functional safety; ASIL; SIL; ISO 26262; IEC61508

1. Introduction

Prior to 2011, automotive functional safety developments applied IEC 61508, but in 2011 this changed with the publication of revision 1 of ISO 26262 followed by revision 2 at the end of 2018. Subsequently, the automotive industry experienced a speedy evolution in the development of advanced hardware and software (based on ISO 26262) to satisfy the rising quest for continuous technological improvement, while developments based on IEC 61508 experienced a lag. This led to a paradigm shift whereby the general industrial sector (based on IEC 61508) saw an opportunity to

CONTACT Peter Okoh okohpee@yahoo.com Autronica Fire and Security, Trondheim, Norway.

reuse hardware and software from the automotive industry in order to align with the fast pace of technological change, shorten time to market and improve the financial bottom line. However, there still exists a flow of safety elements from other domains to the automotive, which is supported by the Safety Element out of Context (SEooC) provision in ISO 26262. In support of this, is the reuse of external safety manuals in ISO 26262. Safety manuals are only defined and described in IEC 61508 and the content list is presented in the normative Annexe in parts 2 and part 3.

Currently, no criteria have yet been set by consensus on how to requalify elements originally developed according to ISO 26262 but intended to be reused in relation to IEC 61508. Hence, in practice, a direct correlation between Safety Integrity Level (SIL) and Automotive Safety Integrity Level (ASIL) is not readily assertable. However, efforts have been made to provide approximate mappings between them. The objective of this paper is to review existing literature in relation to the mapping of the safety levels in ISO 26262 (ASIL) to the safety levels in IEC 61508 (SIL) in order to see whether any and what mapping scheme can serve as a reasonable alternative for approximating a given ASIL to a given SIL after the ASIL has already been certified by a certification body.

The objective of having a cross-domain definition of integrity levels is to demonstrate, based on established safety science, a relationship between such safety assurance measures and thus provide a safety justification for the cross-acceptance of components across industries (Okoh et al., 2022). This can, for example, promote critical component substitution, which was very crucial in the days of the Covid-19 pandemic wherein the shortage of critical components slowed or stalled development in certain industries. A lesson from the Corona era is that a global emergency can happen unexpectedly whether naturally or artificially, and from this perspective, it is useful to have an initiative in place that can also contribute to mitigate risk at such a time. In addition, cross-domain definition of safety levels and associated relationship supports the further work recommended by the report of Khastgir (2022) for an integrated (land, air, marine, etc.) automated transport system, one of which is to 'create a scalable safety assurance framework as a function of operating conditions and behaviour capabilities' (Khastgir, 2022).

The evolution of safety science influenced the development of IEC 61508, the parent standard on functional safety, wherein a focus on risk reducing measures is obvious. Notable risk management methods, techniques and measures are mentioned in the standard. This influence of safety science propagates further into specific standards where different perspectives of risk exist, a reason for the development of the specific (or child) standards to align with the perspective of regulators within specific domains. This is supported by the fact that the definition of a major accident, for example, varies across high-risk industries (Okoh & Haugen, 2013). Besides, an interesting analogy can be drawn from the interpretation of the risk term 'probability', which depends on whether an individual or a group is aligned to the classical (objective), frequentist (objective) or

Bayesian (subjective) school of thought (Rausand, 2011). Yet, another interesting aspect is whether the functional safety risk assessment in a domain is probabilistic, consequentialist or both (Verhulst et al., 2013). On a related note, a safety case (i.e. safety justification/argument asserting that a system is safe for use) can be used as a legal instrument in the railway industry unlike in other industries.

The use of different terms, parameters and reference values by creators of specific standards has the potential to create confusion in a project cutting across domains, e.g. an integrated (land, air, marine, etc.) automated transport system or a rail tanker for transporting fuel from a refinery to an airport/seaport. Hence, the need for interpreting cross-domain standards and establishing their relationships is technically driven although it also offers commercial opportunity. It is known that the membership of the IEC 61508 standard committee in Norway consists of industrial experts, research scientists and professors, one of which has recently published a paper on the application of inherent safety to functional safety as a contribution to the improvement of the standard (Okoh, 2023).

The current paper is expected to give an insight into our research-based market access project that is intended to be part of an application for an artificial intelligence (AI) centre. The expected output of this project is SafeSoft/Zeabuz, an AI innovation described in Figure 1.

This paper is delimited to hardware elements, focusing on random hardware integrity. However, in a subsequent paper, we will compare software methods in ISO 26262 with the Techniques and Measures (T&M) in IEC 61508. This will precede the issuance of the Technical Report (TR) IEC TR 61508-6-1 'Treatment of hardware or software developed to ISO 26262' in 2025, the culmination of the mandate of the JTG20 Work Group. The rest of the paper is structured as follows. Firstly, the concept of continuous demand/high demand mode is described according to IEC 61508:2010 and in relation to ISO 26262:2018 and EN 50129:2018. Further description of this mode according to ISO 26262 is then presented. Subsequently, a review of the literature is presented, showing existing mapping schemes of ASIL to SIL. Next, discussion and recommendations are presented, followed by a conclusion.

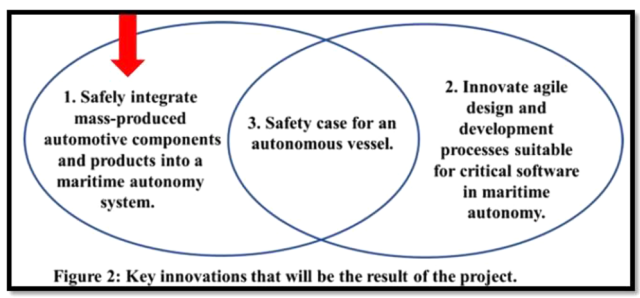

Figure 1. SafeSoft innovations. Zeabuz.

2. Continuous demand/high demand mode perspective of IEC 61508

As far as demand mode is concerned, this perspective of IEC 61508 aligns with the Electrical/Electronic/Programmable Electronic (E/E/PE) safety systems in the automotive industry which are frequently or continuously performing safety functions and whereby a dangerous failure in such systems may directly lead to a hazardous event. In IEC 61508, the average frequency of dangerous failures per hour (PFH) is a dominant reliability metric applied to continuous demand/high demand systems. However, it is challenging to establish equivalence between safety levels in IEC 61508 and ISO 26262 quantitatively.

The aforementioned perspective also aligns with the E/E/PE safety systems (e.g. signalling system) in the railway industry which is another example where continuous demand applies. With respect to the frequency of hazardous failures, PFH values in relation to SIL in IEC 61508 are identical to THR (Tolerable Hazard Rate) values in relation to SIL in EN 50129:2018 of the railway industry as shown in Table 1. In other words, PFH and THR have a quantitative basis for SIL equivalence, even though they are different domain-specific nomenclatures (Braband et al., 2009; Okoh et al., 2022).

According to ARC. (2022), when THR is broken down into Tolerable Functional Failure Rate (TFFR) (i.e. by determining the failure rate of each function that protects against the hazard, if such a function exists), each TFFR is modified with the Probability of Failure on Demand (PFD) of the corresponding safety function and then assigned an appropriate SIL, as demonstrated in Appendix A4.5 of EN 50129 (EN 5019). This is supported by the argument that a cause-and-effect relationship does not exist between the SIL of a given railway safety function and the THR that is derived from a national safety target (e.g. as stated by The Danish national safety authority), if accident causes are not classified. Consequently, the relationship between the effective TFFR and SIL is defined as shown in Table 2 (ARC, 2022; Weits et al.,2019). Hence, Table 1 may be redrawn as Table 3. Based on these and other reports related to the railway industry, it is seen that TFFR is considered as an initiating event frequency (i.e. the rate of failure on demand of the safety function) which when multiplied by the PFD would result in an effective TFFR which is a contributing THR to the overall THR (ARC, 2022, 2022a; Braband et al., 2009; Okoh et al., 2022).

Table 1. SIL equivalence table for IEC 61508-related continuous/high demand safety system in relation to EN 50129 (Okoh et al., 2022).

THR (Railway industry – EN 50129)	SIL	PFH (Generic – IEC 61508)
10^{-9} to $<10^{-8}$	4	10^{-9} to $<10^{-8}$
10^{-8} to $<10^{-7}$	3	10^{-8} to $<10^{-7}$
10^{-7} to $<10^{-6}$	2	10^{-7} to $<10^{-6}$
10^{-6} to $<10^{-5}$	1	10^{-6} to $<10^{-5}$

Table 2. Effective TFFR relationship with SIL in the railway industry [adapted from ARC (2022)].

Effective Tolerable Functional Failure Rate **(TFFR) (per hour)**	SIL
10^{-9} to 10^{-8}	4
10^{-8} to 10^{-7}	3
10^{-7} to 10^{-6}	2
10^{-6} to 10^{-5}	1
$\geq 10^{-5}$	0 / Basic Integrity

Table 3. SIL equivalence based on PFH (IEC 61508) and Effective TFFR (EN 50129) for continuous/high demand safety system [adapted from Okoh et al. (2022)].

Effective TFFR (Railway industry – EN 50129)	SIL	PFH (Generic – IEC 61508)
10^{-9} to 10^{-8}	4	10^{-9} to 10^{-8}
10^{-8} to 10^{-7}	3	10^{-8} to 10^{-7}
10^{-7} to 10^{-6}	2	10^{-7} to 10^{-6}
10^{-6} to 10^{-5}	1	10^{-6} to 10^{-5}

Table 4. Probability of Exposure Classification (ISO 26262, 2018).

Class	Description
E1	Incredible
E2	Very low probability
E3	Low probability
E4	Medium probability
E5	High probability

3. Continuous demand mode perspective of ISO 26262

In the automotive industry and according to ISO 26262, risk is defined as:

$$\text{Risk} = \text{Exposure}(\text{E}) * \text{Controllability}(\text{C}) * \text{Severity}(\text{S})$$

The probability of exposure according to ISO 26262 (2018) is classified as shown in Table 4. The underlying risk reduction strategy in relation to exposure is the separation of the human target from a given hazard in time or in space (Okoh & Haugen, 2014).

In addition, controllability according to ISO 26262 (2018) is classified as shown in Table 5. It is important to note that the definition of controllability in ISO 26262 (2018) conflicts with that in SAE J3016 (2012). The former defines varying likelihood of the driver's control of the vehicle in different hazardous situations, whereas the latter defines a range from when the driver is required to control the vehicle himself while driving (i.e. little or no automation - SAE Level 0, SAE Level 1 and SAE Level 2) to when little or no control effort is required of the driver himself (i.e. advanced and increasing level of automation – SAE Level 3, SAE Level 4 and SAE Level 5). Even though SAE J3016 is dedicated to on-road vehicles,

Table 5. Controllability classification (ISO 26262, 2018).

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

Table 6. Severity classification (ISO 26262, 2018).

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

advanced SAE Levels are more challenging to implement on human-driven vehicles compared to ASIL D which is fault-tolerant. This is supported by Mariajoseph et al. (2020) who acknowledged that SAE Level 3 demands the full attention of the driver to fulfil certain safety task, but the driver may become over-dependent on automation leading to human error of omission and probably an accident. Considering this knowledge, it is reasonable to suggest the application of SAE Level 4 and SAE Level 5 strictly to autonomous on-road vehicles in non-public traffic.

Furthermore, severity according to ISO 26262 (2018) is classified as shown in Table 6. The severity, in like manner exposure, clearly indicate that the overarching loss prevention objective is the protection of the vehicle occupants, the fact notwithstanding any damage to the vehicle during the risk mitigation process.

The safety levels of the automotive industry, Automotive Safety Integrity Level (ASIL) are determined qualitatively from the combination of Table 4, Table 5 and Table 6 as shown in Table 7. With respect to random hardware integrity, the qualitative nature of ASIL assignment makes it difficult to establish equivalence with SIL assignment which is of a quantitative nature. Hence, the need to find a way to obviate this drawback.

4. Review of literature mapping ASIL to SIL

Considering the discussions and the reviews in existing literature, it is obvious that a direct correlation between SIL and ASIL is not easily realisable. However, efforts have been made to provide approximate mappings between them.

According to Meany (2019), SIL and ASIL may be compared based on diagnostic coverage and dangerous failure rate metrics as shown in Tables 8 and 9 respectively. He mentioned that for ASIL C, 99% diagnostic coverage is very hard to achieve in a single channel system, whereas 97% is

Table 7. ASIL Determination (ISO 26262, 2018).

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

Table 8. Comparison of ASIL and SIL using diagnostic coverage (Meany, 2019).

SIL (IEC 61508)	Min. Diagnostic Coverage	Vs.	ASIL (ISO 26262)	Min. Diagnostic Coverage
SIL 1	60%		ASIL A	No minimum
SIL 2	90%		ASIL B	90%
–	–		ASIL C	97%
SIL 3	99%		ASIL D	99%
SIL 4	99%		–	–

Table 9. Comparison of ASIL and SIL using dangerous failure rate metric (Meany, 2019).

SIL (IEC 61508)	Max. PFH (FIT)	Vs.	ASIL (ISO 26262)	Max. PMHF (FIT)
SIL 1	10000		ASIL A	No maximum
SIL 2	1000		–	–
SIL 3	100		ASIL B	100
–	–		ASIL C	100
SIL 4	10		ASIL D	10

realisable with effort, which is apparently borne from his experience. Moreover, diagnostic coverage is relevant to consider since it tends to improve safety integrity through the management of detected dangerous failures. This is complemented by the dangerous failure rate metrics where the idea is that a given level of a system's safety is partially assured if dangerous failure occurrence is limited. Fundamentally, dangerous failures will not be detected if they are not created whether randomly or artificially. Even though a proportion of the dangerous failures still go undetected, the aim in diagnostic coverage is to, as much as possible, reduce this quantity.

The probabilistic metric for random hardware failures (PMHF) applied in the automotive industry and mentioned in Table 9 is identical to the average frequency of dangerous failures (PFH) applied in the generic industry, but unlike the latter, is not used directly to determine safety levels. Safety levels according to ISO 26262 are rather determined directly from the qualitative combination of exposure, controllability and severity

as mentioned earlier. Therefore, Table 9 is an attempt by Meany (2019) to demonstrate a correlation between dangerous failure frequency and safety levels for ISO 26262 in like manner IEC 61508. Failure In Time (FIT), which is used in Table 9 as the unit for PFH and PMHF, is a measure of failure rate representing the number of failures in 10^9 hours.

Furthermore, In Tables 8 and 9, there is a fair pattern in matching diagnostic coverage stipulation in IEC 61508 with diagnostic coverage stipulation in ISO 26262 and dangerous failure frequency stipulation in IEC 61508 with dangerous failure frequency stipulation in ISO 26262. However, inconsistency is noticed when the results from both tables are compared. The implication is that further analysis is necessary to reduce uncertainty.

In Table 9, PFH and PMHF are expressed in the same unit (FIT), such that PFH of 100 FIT, for example, is assumed to be equal to PMHF of 100 FIT. However, the composition of the FITs are different as explained in the following. According to Efody (2023): Safe Fault (SF) is a fault that cannot affect safety critical logic either because it does not have physical connection or is masked by some logic along the path; Single Point Fault (SPF) is a fault that can affect a safety critical logic such that there is no safety mechanism (e.g. Cyclic Redundancy Check) to detect or correct it; Residual Fault (RF) is a fault that occur in an area that is buffered from safety-critical functionality by a safety mechanism, but which cannot be detected by the safety mechanism; Multiple Point Fault is a fault that is detected or corrected by a safety mechanism, but which can become dangerous in combination with another fault in the safety mechanism; Detected Multiple Point Fault (MPFD) is a fault that is detected and corrected by a safety mechanism; Latent Multiple Point Fault (MPFL) is a fault that is corrected, although there is no indication that it ever existed; and Perceived Multiple Point Fault (MPFP) is a fault that is not detected, but has an obvious impact on driving experience. Besides, Divakarla (2017) defines multiple-point fault as an individual fault that, in addition to other individual and independent faults, leads to a multiple-point failure. Based on these failure definitions, a comparison of failure classes for calculating FIT for PFH (IEC 61508, 2010) and PMHF (ISO 26262, 2018) is presented in Table 10.

Considering Table 10 and the equations in ISO 26262 (2018) for calculating PMHF metric, it is seen that for a given architecture, the values of the PMHF metric (in FIT) are higher than that of PFH (in FIT) due to contribution of failure rates of dual point faults. Hence, if e.g., 100 FIT according to IEC 61508 is assumed to be equal to 100 FIT according to ISO 26262, it implies that 100 FIT of DU-failure according to IEC 61508 is assumed to be equal to 100 FIT according to ISO 26262 which consists of X FIT of DU-like failure (i.e. SPF, RF and MPFP) + Y FIT of SU-like failure (i.e. MPFL) + Z FIT of SD-like failure (i.e. MPFD). The implication of this is that, if we are mapping from ASIL to SIL assuming that e.g. 100 PMHF's

Table 10. Comparison of failure classes for calculating FIT for PFH and PMHF.

	Failure Classes (IEC 61508)	Failure Classes (ISO 26262)
	Safe Detected (SD)	Safe Fault (SF) Detected Multiple Point Fault (MPFD)
	Safe Undetected (SU)	Latent Multiple Point Fault (MPFL)
	Dangerous Detected (DD)	–
	Dangerous Undetected (DU)	Single Point Fault (SPF) Residual Fault (RF) Perceived Multiple Point Fault (MPFP)
	PFH	**PMHF**
Failure Classes for Calculating FIT	DU	SPF, RF, MPFP, MPFL and MPFD

Table 11. Comparison of SIL levels of functional-safety standards (Frigerio, 2022).

FuSa Standard	Safety Levels (lowest to highest)				
IEC 61508	–	SIL 1	SIL 2	SIL 3	SIL 4
ISO26262	ASIL A	ASIL B	ASIL C	ASIL D	
DO-178C	Level E	Level D	Level C	Level B	Level A
IEC 62304	Class A	Class B		Class C	
EN 50128	SSIL 0	SSIL 1	SSIL 2	SSIL 3	SSIL 4

FIT = 100 PFH's FIT, we are being conservative by limiting the SIL that a given ASIL can map to, since there is a lesser quantity of DU-rated FIT in the PMHF. Hence, it implies that uncertainty/risk is mitigated during such a mapping.

Furthermore, Frigerio (2022) stated that although all the SIL and equivalent parameters are not interchangeable, they may be compared to clarify the relationship between them as shown in Table 11, although he did not describe how his mapping scheme evolved.

Besides, Verhulst et al. (2013) stated that no 1-to-1 mapping of the domain specific safety levels to IEC 61508 SIL levels exists. However, they suggested an approximate mapping shown in Table 12. According to them, the Risk Reduction Factors in the various domains are justified by system usage pattern (infrequent vs. continuous) and 'fail safe' mode, and are significantly different, e.g. a train can be stopped in the event of detecting a failure, whereas a plane must at all cost be kept airborne in such a state that allows for safe landing.

The relationship between SIL and ASIL are further explained by Verhulst et al. (2013) as follows:

- ISO2626 was intended for automotive systems with a single central engine. Hence, such a vehicle is by design not fault-tolerant and therefore cannot comply with SIL4, which requires a fault-tolerant design. SIL 4 imposes redundancy. Hence, ASIL D would correspond to SIL 3 in terms of casualties.

Table 12. Mapping of the safety levels of different domains (Verhulst et al., 2013).

Domain	Domain-specific Safety Levels				
General (e.g. IEC 61508)	(SIL 0)	SIL 1	SIL 2	SIL 3	SIL 4
Automotive (e.g. ISO 26262)	ASIL A	ASIL B	ASIL C	ASIL D	
Aviation (e.g. DO178C)	DAL E	DAL D	DAL C	DAL B	DAL A
Railway (e.g. EN 50128)	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4

Table 13. SIL and ASIL comparison (Marcus & Mieslinger, 2012).

SIL (IEC 61508)	ASIL (ISO 26262)	Description
	QM	–
SIL 1	ASIL A	–
SIL 2	ASIL B	SIL 2 is not fully equivalent ASIL B
	ASIL C	SIL 2 Development requirements SIL 3 Verification requirements
SIL 3	ASIL D	SIL 3 is not fully equivalent ASIL D
SIL 4	–	–

- ASIL C more or less would map onto SIL 3 (given that in the event of a failure the system should transition to a fail-safe state). ISO 26262 introduces ASIL C requiring a supervising architecture, such that together with a degraded mode of operation (e.g. limp mode), it can be considered as fault-tolerant, if no common mode failure terminates the operation of both processing units.

Yet, another suggestion from Marcus and Mieslinger (2012) is presented in Table 13. Although they did not describe how their mapping scheme evolved, they expressed uncertainty in it with some caveats in the column 'Description'.

5. Discussion and recommendations

5.1. Discussion

5.1.1. ASIL D

ASIL D is not designed to be fault-tolerant and so cannot be mapped to SIL 4 (which imposes redundancy), however it can be mapped to SIL 3 in terms of casualty (Verhulst et al., 2013) and diagnostic coverage (99%) as shown in Table 8 (Meany, 2019). Besides, Agirre et al. (2018) suggested that, as a rule of thumb, ASIL D should be mapped to SIL 3 in the pursuit of certification. Hence, the mapping of ASIL D to SIL 4 in terms of maximum allowable FIT, as shown in Table 9 (Meany, 2019), iis not encouraged in order to minimise uncertainty.

5.1.2. ASIL C

In terms of diagnostic coverage (Table 8), ASIL C has a higher diagnostic coverage than ASIL B (97% vs. 90%) where ASIL B is mapped onto SIL 2 (Meany, 2019). However, in terms of maximum allowable FIT (Table 9), ASIL C maps onto SIL 3 on the same basis as ASIL B (Meany, 2019). Hence, considering that the argument for mapping ASIL D to SIL 3, as discussed above, is stronger, it is logical to map ASIL C to SIL 2 and ASIL B to SIL 1. This is consistent with the mapping schemes of Frigerio (2022) and Verhulst et al. (2013) in Tables 11 and 12 respectively.

5.1.3. ASIL B

In Tables 8 and 9, it is indicated that ASIL B maps to SIL 2 in terms of diagnostic coverage (90%) and to SIL 3 in terms of maximum allowable FIT respectively (Meany, 2019). Considering the aforementioned analysis, it is reasonable to downgrade ASIL B as mapping to a lower SIL (i.e. SIL 1). This is consistent with the mapping schemes of Frigerio (2022), Verhulst et al. (2013) and Marcus and Mieslinger (2012) in Tables 11–13 respectively.

5.1.4. ASIL A

According to Table 8 and Table 9, ISO 26262 does not set acceptable minimum of diagnostic coverage and maximum of failure rate for ASIL A (Meany, 2019). Hence, it is reasonable to rate ASIL A below SIL 1, since it tends to imply that even a very low effort can achieve ASIL A. This will help address the uncertainties associated with the absence of the aforementioned thresholds for ASIL A. This mapping is consistent with Frigerio (2022) and Verhulst et al. (2013) in Table 11 and Table 12 respectively.

Furthermore, the least significant levels of integrity in functional safety standards can be compared as shown in Table 14, where SIL 0 indicates that there is no safety requirement (EN 50128, 2020), Design Assurance Level-DAL E qualifies hardware whose failure would not affect the aircraft's operational capability or pilot workload (Military Aerospace Electronics, 2016), basic integrity is not safety integrity (EN 50126, 2017; EN 50129, 2018) and QM (Quality Management) does not dictate any safety requirement (Exida, 2023). These levels are identical. Yet, they are rated below ASIL A if the failure rate and diagnostic coverage associated with ASIL A do not become trivial. Whether the characteristics of ASIL A are trivial or not can be determined from Table 16.

5.2 Recommendations

5.2.1. Mapping ASIL to SIL

Based on the aforementioned, a proposed mapping scheme from ASIL to SIL is presented as shown in Table 15. For ASIL A that is considered lower

Table 14. Comparing the least significant levels of integrity.

Domain	Domain-specific Safety Levels
General (e.g. IEC 61508)	(SIL 0)
Automotive (e.g. ISO 26262)	QM / ASIL A (conditional)
Aviation (e.g. DO178C)	DAL E
Railway (e.g. EN 50128)	SIL 0
Railway EN 5129:2018	Basic integrity
Railway EN 50126-2:2017	Basic integrity

Table 15. Proposed mapping scheme for ASIL to SIL.

Standard	Safety Levels				
ISO26262	ASIL A	ASIL B	ASIL C	ASIL D	–
IEC 61508	–	SIL 1	SIL 2	SIL 3	SIL 4

Table 16. Proposed architectural constraints for ISO 26262 in relation to IEC 61508.

Diagnostic Coverage (ISO 26262)	Hardware architectural metric (PMHF Range in FIT)		
	$1000 < PMHF \leq 10000$	$100 < PMHF \leq 1000$	$1 \leq PMHF \leq 100$
<90%	SIL 1	SIL 1	SIL 2
90 – 97%	SIL 1	SIL 2	SIL 2
97 – 99%	SIL 2	SIL 2	SIL 3
≥99%	SIL 3	SIL 3	SIL 3

in status than SIL 1, it is recommended to perform further detailed analysis on it in order to bring it up to SIL 1 status.

Furthermore, to reduce the uncertainty associated with the mapping of ASIL to SIL, it is recommended, irrespective of the ASIL, to take further measures to satisfy requirements for architectural constraints and systematic integrity for the assigned SIL. This would enhance the confidence in the assurance/certification of the ASIL-certified element as conforming to IEC 61508. The architectural constraints will help to limit the SIL claimed after mapping from ASIL (Rausand, 2014), whereas the systematic integrity will provide safety assurance against systematic failures (IEC 61508, 2010).

5.2.2. Architectural constraints

Based on Table 8 and Table 9 and considering how difficult it is to realise diagnostic coverages of 97% to 99% (Meany, 2019) and the fact that hardware architectural metrics (e.g. PMHF) can be used to determine whether an automotive system meets a given ASIL requirement (Munir, 2017), an architectural constraint scheme for ISO 26262 in relation to SIL is proposed as shown in Table 16.

Alternatively, the safe failure fraction (SFF) and hardware fault tolerance (HFT) can be determined for the hardware acquired from the ISO 26262 domain to demonstrate architectural constraints. Hence, the safety architecture and the Failure Modes, Effects and Diagnostics Analysis (FMEDA)

from the ISO 26262 domain will be considered to provide input for the architectural constraints table of IEC 61508 for complex systems.

5.2.3. Systematic integrity

For systematic integrity, the approaches in ISO 26262 and IEC 61508 are identical, applying qualitative recommended measures for the prevention, avoidance and control of systematic failures (Agirre et al., 2018). Hence, a fresh analysis with Tables A-B series of IEC 61508-2:2010 is not necessary.

5.2.4. Treatment of ASIL A

As seen earlier in this paper (See Tables 8 and 9), the absence of thresholds for tolerable frequency of dangerous failure (PMHF) and diagnostic coverage for ASIL A in ISO 26262, led to the challenge of not being able to map it satisfactorily to any SIL in relation to IEC 61508 (Meany, 2019). However, this problem can be solved by using Table 16 to re-evaluate ASIL A, considering its PMHF value and the achieved diagnostic coverage. This implies that ASIL A may be rated as SIL 0 or SIL 1, depending on the quality of the diagnostic coverage (i.e. whether below or above 90% and to what extent) and its PMHF (i.e. to what extent above 100 FIT). This is similar to Table 3 of IEC 61508-2:2010 (i.e. maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem), wherein an item with even zero HFT (i.e. a simplex) has the possibility of being SIL 1, SIL 2 or SIL 3, depending on how high the SFF is (IEC 61508, 2010).

5.2.5. Proposal for autonomous vehicle: ASIL E and 'ASIL (letter)-capable' designation for sensor

From the discussion in Section 3, it is clear that the ASILs (ASIL A, ASIL B, ASIL C and ASIL D) defined by the current edition of ISO 26262 (2018) are not aligned to the philosophy of autonomous (or self-driving) vehicles which depends on redundancy to satisfy safety goals. Besides, SAE J3016 (2012) is not a functional safety standard for autonomous vehicles but defines levels of automation which are aligned to current applications of ISO 26262 and autonomous vehicles. Hence, there is the need to revise the current edition of ISO 26262 to provide for autonomous vehicles if a separate functional safety standard will not be developed for autonomous vehicles. To this end, a new ASIL, ASIL E, is highly recommended in ISO 26262 to cater for the functional safety of autonomous vehicles. It is expected that ASIL E, when eventually defined, should be equivalent to SIL 4, from the perspective of extreme fault tolerance.

Furthermore, as seen from the autonomous vehicle domain, one and the same sensor can provide safety assurance ranging from QM to ASIL D, depending on the safety measures associated with the sensor's failure as illustrated in Table 17. Hence, it is appropriate for such a sensor in the manufacturer's possession to be certified as capable of a certain maximum ASIL. However,

Table 17. Safety goals (Copied from 55GAA, 2019).

Hazardous event and associated risk	Safety Goal (SG)	Possible ASIL ratings for selected hazardous events
Controlled Vehicle (CV) causes an accident by receiving wrong or late information from Control Centre (CC) and thus causes a severe accident	SG1: Avoid wrong control information being received by the Controlled Vehicle SG2: Avoid late control information being received by the Controlled Vehicle	If vehicle's autonomous sensors are still functioning the incorrect information could be checked and therefore accidents due to wrong information can be avoided -> Quality Management (QM) If vehicle's autonomous sensors are no longer functioning or they are degraded (e.g. because Control Centre commands put vehicle outside Operational Design Domain - ODD) -> ASIL D

during the vehicle's development further certification should acknowledge the effective ASIL depending on how the sensor is configured for use.

5.2.6. Other observations about ISO 26262 that need to be addressed by the standard's committee

It is recommended that the following deficiencies in the automotive standard are addressed in future editions:

1. No idea of proof testing in the automotive industry. Proof testing has been mostly of interest to process control in the industrial domain.
2. No low-demand system in the automotive industry, with everything effectively high or continuous demand (despite the fact that an airbag and a fire safety system would be low-demand according to IEC 61508)
3. IEC 61508 has lots of support standards including IEC 61784-3 for networking, but ISO 26262 has to handle everything alone.

6. Conclusion

This paper has realised a framework for mapping safety levels (ASIL) of ISO-26262-based hardware to safety levels (SIL) based on IEC 61508. The objective is to guide the reuse of safety-related resources of the automotive industry by the generic industry without compromising safety. The paper built on a review of literature and standards. It is intended to give to engineers, standard organisations and certification bodies more insight into inter-domain cooperation between the automotive (based on ISO 26262) and the generic industry (based on IEC 61508) in order to collectively match the changing pace of technological development whereby one industry may already be ahead of the other in terms of alignment with the state-of-the-art.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work has been supported by The Norwegian Research Council, Project name 'Integrated Service & Safety Platform', project number: 309406.

Notes on contributors

Peter Okoh holds a PhD in Reliability, Availability, Maintainability and Safety (RAMS). He studied at the Department of Mechanical and Industrial Engineering, at Norwegian University of Science and Technology, Trondheim, Norway.

Thor Myklebust is a senior researcher at SINTEF Digital and a member of the IEC 61508 maintenance committee.

ORCID

Peter Okoh http://orcid.org/0000-0001-5086-7989

References

5GAA. (2019). Safety Treatment in Connected and Autonomous Driving Functions Report. 5GAA Automotive Association Technical Report.

Agirre, I., Cazorla, F. J., Abella, J., Hernandez, C., Mezzetti, E., Azkarate-Askatsua, M., & Vardanega, T. (2018). Fitting software execution-time exceedance into a residual random fault in ISO-26262. *IEEE Transactions on Reliability*, *67*(3), 1314–1327. https://doi.org/10.1109/TR.2018.2828222

ARC. (2022). International Engineering Safety Management (IESM) Good Practice Handbook, Volume 2, Issue 1.4: Methods, Tools and Techniques for Projects. Abbot Risk Consulting Ltd. Retrieved from https://static1.squarespace.com/static/60e5bc3a5cbea5566b74ada9/t/627093c0ef8e2040b9a3def8/1651545038338/iESM_Volume_2_Issue_1.4.pdf

ARC. (2022a). International Engineering Safety Management (IESM) Good Practice Handbook, Application Note 9, Issue 1.2: Safety Integrity Within Engineering Safety Management. Abbot Risk Consulting Ltd. Retrieved from https://static1.squarespace.com/static/60e5bc3a5cbea5566b74ada9/t/62709965fa5f667208d2a3c2/1651546475902/iESM_AN9_Issue_1.2.pdf

Braband, J., Vom Hovel, R., & Schabe, H. (2009). Probability of failure on demand – The why and the how. In B. Buth, G. Rabe, & T. Seyfarth (Eds.), *26th International Conference, SAFECOMP, 2009* (pp. 46–54). Springer.

Divaklar, K. P. (2017). ISO26262 and IEC61508 Functional Safety Overview. AMF-AUT-T2713. Retrieved from https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/tech-days/160/1/AMF-AUT-T2713.pdf

Efody, A. (2023). Getting ISO 26262 Faults Straight. Siemens. Retrieved from https://verificationacademy.com/topics/functional-safety/articles/Getting-ISO-26262-faults-straight

EN 50126. (2017). Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). European Committee for Electrotechnical Standardization (CENELEC).
EN 50128. (2020). Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems. European Committee for Electrotechnical Standardization (CENELEC).
EN 50129. (2018). Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling. European Committee for Electrotechnical Standardization (CENELEC).
Exida. (2023). Automotive Safety Integrity Level (ASIL). Retrieved from https://www.exida.com/Resources/Term/Automotive-Safety-Integrity-Level-ASIL
Frigerio, A. (2022). Functional-safety analysis of ASIL decomposition for redundant automotive systems [PhD thesis 1 (Research TU/e/Graduation TU/e), Electrical Engineering]. Eindhoven University of Technology.
IEC 61508. (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.
ISO 26262. (2018). Road vehicles – Functional safety.
Khastgir, S. (2022). Cross domain safety assurance framework for automated transport systems. Retrieved from https://warwick.ac.uk/fac/sci/wmg/research/research-areas/verification-and validation/ukriflf/cross_domain_safety_assurance_framework_for_automated_systems.pdf
Marcus, F., & Mieslinger, J. (2012). Embedded processing marketing MCU industrial & automotive. In *Functional Safety Seminar & 1-Day HerculesTM Workshop*. Arrow Roadshow Silkeborg.
Mariajoseph, M., Gallina, B., Carli, M., & Bibbo, D. (2020). A physiology-based driver readiness estimation model for tuning ISO 26262 controllability. 1–5. https://doi.org/10.1109/VTC2020-Spring48590.2020.9129132
Meany, T. (2019). Automotive vs industrial functional safety. ADI engineer Zone. Retrieved from https://ez.analog.com/ez-blogs/b/engineerzone-spotlight/posts/automotive-vs-industrial-functional-safety
Military Aerospace Electronics. (2016). Retrieved from https://www.militaryaerospace.com/computers/article/16714656/what-is-safetycertifiable-avionics-hardware-that-meets-design-assurance-levels-dal
Munir, A. (2017). Safety assessment and design of dependable cybercars: For today and the future. *IEEE Consumer Electronics Magazine*, *6*(2), 69–77. https://doi.org/10.1109/MCE.2016.2640738
Okoh, P. (2023). The application of inherent safety to functional safety. *Safety and Reliability*, *42*(1), 5–15. https://doi.org/10.1080/09617353.2023.2263727
Okoh, P., Dong, H. S., & Liu, Y. (2022). Cross-acceptance of fire safety systems based on SIL equivalence in relation to IEC 61508 and EN 50129. *Safety and Reliability*, *41*(2), 103–120. https://doi.org/10.1080/09617353.2022.2107255
Okoh, P., & Haugen, S. (2013). Maintenance-related major accidents: Classification of causes and case study. *Journal of Loss Prevention in the Process Industries*, *26*(6), 1060–1070. https://doi.org/10.1016/j.jlp.2013.04.002
Okoh, P., & Haugen, S. (2014). Application of inherent safety to maintenance-related major accident prevention on offshore installations. *Chemical Engineering Transactions*, *36*, 175–180.
Rausand, M. (2011). *Risk assessment: Theory, methods, and applications* (1st ed.). John Wiley & Sons.

Rausand, M. (2014). *Reliability of safety-critical systems: Theory and applications*. John Wiley & Sons.

SAE J3016. (2012). *Recommended practice: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*. Society of Automotive Engineers.

Verhulst, E., Vara, J., Sputh, B., & Florio, V. (2013). ARRL: A criterion for composable safety and systems engineering.

Weits, E., Munck, S., & Eigenraam, A. (2019). Deriving THR and SIL from National Safety Targets, accounting for scale and exposure. In *Proceedings of the 2nd International Railway Symposium Aachen 2019*. Retrieved from https://publications.rwth-aachen.de/record/775096/files/775096.pdf