SaRS Safety and Reliability Society

Safety and Reliability

The Journal of the Safety and Reliability Society

ISSN 0961-7353 Vol 41 No 2

Safety and Reliability

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

Cross-acceptance of fire safety systems based on SIL equivalence in relation to IEC 61508 and EN 50129

Peter Okoh, Hyun Soo Dong & Yiliu Liu

To cite this article: Peter Okoh, Hyun Soo Dong & Yiliu Liu (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, DOI: 10.1080/09617353.2022.2107255

To link to this article: https://doi.org/10.1080/09617353.2022.2107255

SAFETY AND RELIABILITY
2022, VOL. 41, NO. 2, 103–120
https://doi.org/10.1080/09617353.2022.2107255

Taylor & Francis
Taylor & Francis Group

ARTICLE

OPEN ACCESS Check for updates

Cross-acceptance of fire safety systems based on SIL equivalence in relation to IEC 61508 and EN 50129

Peter Okoh[a], Hyun Soo Dong[b] and Yiliu Liu[b]

[a]Autronica Fire and Security, Trondheim, Norway; [b]Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT
Several sectors, e.g. process, railway, etc., have set their functional safety standards based on the generic IEC 61508. Yet, a product that is originally developed based on IEC 61508 is not automatically accepted for use in specific industries. Therefore, companies that are keen on selling safety products across sectors are faced with the challenge of satisfying the requirements sector by sector, thus incurring more cost and time to market. Cross-acceptance across industries is expected to solve this problem. However, an approach with a quantitative focus (e.g. in relation to SIL) has yet to be identified and validated. Demonstrating consistency and compatibility between cross-domain standards in relation to system safety is necessary for harmonising safety integrity claims. This paper applies the relationship between PFD_{avg} and THR to cross-acceptance, establishing SIL equivalence as a basis for cross-acceptance, supporting this with data prioritisation and recommending it together with architectural constraints, systematic capability, the original safety case, a supplementary safety case (accounting for differences between the original and target standards provisions), and the original safety manuals (for COTS components and the whole system) as a framework for achieving both IEC 61508 (generic) and EN 50129 (railway) certification for a fire detection system.

ARTICLE HISTORY Received 8 November 2021; Revised 16 May 2022; Accepted 10 July 2022

KEYWORDS Cross-acceptance; fire safety system; SIL equivalence; safety integrity; certification; safety case

1. Introduction

Several functional safety standards (e.g. IEC 62021, IEC 61511, ISO 26262, IEC 61513, and EN 50129, etc.) for specific industrial sectors (e.g. machinery manufacturing, process, automotive, power plant, railway, etc.) have

CONTACT Yiliu Liu yuliu.liu@ntnu.no Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, 7491, Norway

evolved over the years from the generic IEC 61508. This is accompanied by the challenge of getting certification across industries for a safety system originally developed based on IEC 61508. The fact that a product is developed based on IEC 61508 does not automatically afford it cross-acceptance in a specific sector. Yet, going through the certification process from the scratch for every new market in pursuit of cross-acceptance can be tedious, costly, and time-consuming.

From the 'pre-CENELEC era' to the first decade of the twenty-first century, cross-acceptance was realised *via* Memorandum of Understanding (MoU) between European countries based on mutual recognition of the reputation of national railway authorities and equipment manufacturers (EBA, 2021; Reder, 2006). Within this period, several authors and authorities have made proposals for its regulation. In 1992, The Institution of Railway Signal Engineers (IRSE) proposed a cross-acceptance methodology encompassing (1) commonly accepted vital regulations, (2) Methods for establishing safety requirements and proving safety, and (3) process for establishing proof of safety, and in 2003, it proposed a process for cross-acceptance (Coenraad, 2005; IRSE, 1992, 2003).

In spite of the emergence of EN 50129 standard within the European railway industry with the expectation of providing a common basis for safety approvals, national regulations can still stipulate additional criteria (Baufreton et al., 2010). However, further emphasis on cross-acceptance in BS PD CLC/TR 50506-1:2007 (TR 50506, 2007), is expected to keep the concept alive and ease cross-country approvals eventually. Besides, the scope of cross-acceptance needs to transcend the railway-to-railway scenario to include also other industry-to-railway scenarios to improve globalisation (Baufreton et al., 2010; Kessell, 2020; Machrouh et al., 2012; Ruiz et al., 2017). The BS PD CLC/TR 50506-1 recommends the following sequential process for cross-acceptance: (1) Establish a credible case for the native (baseline) application, (2) Specify the target environment and application, (3) Identify the key differences between the target and native cases, (4) Specify the technical, operational and procedural adaptations required to cater for the differences, (5) Assess the risk arising from the differences, (6) Produce a credible case for the adaptations adequately controlling the risks arising from the differences, and (7) Develop a generic cross-acceptance case (TR 50506, 2007).

Even though cross-acceptance is still not harmonised and constrained by bureaucracy (IRSE, 2020; Kessell, 2020), proposals are still being put forward by experts to improve it. For cross-acceptance to the railway industry of a product of generic or other origins, Filip (2020) proposed the approach of showing safety justification with a safety manual and risk management with CSM-RA (if a significant change to the railway domain is expected) of a 'pre-existing' item (EN 50129, 2018; Filip, 2020; IEC 61508, 2010). Another approach from Ruiz et al. (2017) is that of mapping the basis for safety in the original standard used to develop/certify a product with the one in the standard for which additional certification is desired, then mapping the safety deliverable from the original product development project to the latter project, and subsequently checking whether and what gaps should be filled (Machrouh et al., 2012; Ruiz et al., 2017).

Cross-acceptance across industrial sectors still has gaps to be filled (Ruiz et al., 2017). This is supported by the fact that an approach with a quantitative focus (e.g. in relation to SIL) has yet to be identified and validated. Besides, according to IRSE (2003), cross-acceptance should be applicable and encouraged even if non-European standards are used. Hence, since EN 50129 evolved from IEC 61508, establishing a common ground between them should be encouraged. The same goes also for situations not involving IEC 61508.

This paper applies the relationship between PFD_{avg} and THR to cross-acceptance, establishing SIL equivalence as a basis for cross-acceptance, supporting this with data prioritisation and recommending it together with architectural constraints, systematic capability, the original safety case, a supplementary safety case (accounting for differences between the original and target standards provisions), and the original safety manuals (for COTS components and the whole system) as a framework for achieving both IEC 61508 (generic) and EN 50129 (railway) certification for a fire detection system. The rest of the paper is structured as follows: The concept of cross-acceptance is defined, followed by a description of SIL and the relationship between THR and PFD_{avg} in relation to IEC 61508 and EN 50129. Next is the application of the relationship between PFD_{avg} and THR to cross-acceptance based on SIL equivalence. Furthermore, the influence of SIL-related input data sources on cross-acceptance is analysed. Subsequently, discussion and recommendations are presented and finally, a conclusion is drawn.

2. The concept of cross-acceptance

There is no universal definition of cross-acceptance. Various definitions exist across a few domains and authorities as presented in Table 1, which probably implies that the term has yet to gain widespread multi-domain application.

As seen in Table 1, the various definitions imply alignment in the reuse of artefacts across boundaries such that the artefacts do not lose value in the transition. In the first three definitions ([1], [2], and [3]), the scope of cross-acceptance is narrow, focussing on intra-domain boundaries, whereas the fourth definition ([4]) advocates for cross-domain co-operation. Meanwhile, Ruiz et al. (2017) used a different term ‘cross-domain reuse’ to

Table 1. Cross-acceptance definitions.

Authority	Definition	Comment
[1] New Jersey State Planning Commission (NJSPC)	'Cross-acceptance is the process of comparing municipal and county plans and regulations with the Preliminary State Development and Redevelopment Plan in an effort to achieve consistency and compatibility across the various levels of government in New Jersey'. (NJSPC, 2021)	Specific to New Jersey's geographical area and the built environment. However, some key generic ideas are 'consistency' and 'compatibility' of alternative items.
[2] EN 50129	'The status achieved by a product that has been accepted by one authority to the relevant European Standards and is acceptable to other authorities without the necessity for further assessment' (EN 50129, 2018).	Restrictive to European standards.
[3] Railtrack PLC	'A process for accepting and approving equipment for use on a railway administration's infrastructure, based upon an acceptance already given for the same product by another railway administration or acceptance body together with an analysis of the safety issues arising from the application of the equipment in the "targeted" railway administration's environment' (IRSE, 2003).	Specific to the railway industry.
[4] Institution of Railway Signal Engineers (IRSE)	'At a high level, the concept of cross-acceptance puts forward a scenario "that if a technology/system operated safely and reliably in one country, then it should be able to do so in another country without the need for back-to-basics approval tests" … cross-acceptance is also applicable if other than European standards were used … ' (IRSE, 2003)	A more universal perspective.

refer to the same concept. Though an uncommon term, it is still within the context, since cross-reuse will not happen without acceptance in the new jurisdiction. In this paper, the focus is on cross-domain cross-acceptance for cross-domain certification.

3. SIL and the relationship between THR and PFD_{avg} in relation to IEC 61508 and EN 50129

Safety Integrity Level (SIL) is one of four possible discrete levels of reliability performance with respect to safety, measured in terms of the probability of an Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related system satisfactorily performing the specified safety function under all the stated conditions within a stated period of time (IEC 61508, 2010; Rausand, 2014; Rausand & Høyland, 2004). An Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related system, according to Rausand and

Table 2. Safety integrity levels according to IEC 61508 (2010).

SIL	Low demand mode operation (average probability of failure on demand—PFD$_{avg}$)	Continuous/high demand mode (average frequency of dangerous failures—PFH)
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

Table 3. Safety integrity levels according to EN 50129 (2018).

SIL	Tolerable hazard rate—THR
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Høyland (2004), is 'a designated system that implements the required safety functions necessary to achieve or maintain a safe state for some equipment'. Safety integrity levels according to IEC 61508 (2010) and EN 50129 (2018) are presented in Tables 2 and 3, respectively.

According to EN 50129 (2018) and as seen in Table 3, the low-demand mode is not applied in the railway industry. However, comparing Tables 2 and 3 shows that the Tolerable Hazard Rate (THR) as presented in EN 50129 is the identical concept to the average frequency of dangerous failure (PFH) of the continuous/high-demand mode as presented in IEC 61508 (Braband et al., 2009; Li, 2018). Besides, Braband et al. (2009) defined a relationship between PFD_{avg} (a measure used in IEC 61508 for a generic system in the low-demand mode of operation) and THR (a measure used in EN 50129 for the continuous/high-demand railway operation) as seen in the following.

The objective of safety systems is to reduce the major accident risk (Okoh et al., 2019; Okoh & Haugen, 2013, 2014). In this study, the risk will be measured as the Individual Risk Index (IR_i), which is defined as follows.

For a single accident scenario (Rausand, 2011):

$$IR_i = f_A \times P(F|A) \tag{1}$$

Where:

- IR_i denotes the Individual Risk Index
- f_A denotes the frequency of accident
- $P(F|A)$ denotes the probability of fatality given accident

Equation (1) can be rewritten as:

$$IR_i = f_H \times P_A \times P(F|A) \tag{2}$$

Where:

- f_H denotes the frequency of hazardous event
- P_A denotes the probability of accident

With respect to THR, Equation (2) can be rewritten as (Braband et al., 2009):

$$IR_i = THR \times P_A \times P(F|A) \tag{3}$$

Where THR, tolerable hazard rate, is actually an overall frequency of hazardous events per hour per safety function that can be used as-is.

With respect to PFD_{avg}, Equation (2) can be rewritten as (Braband et al., 2009):

$$IR_i = d \times PFD_{avg} \times P_A \times P(F|A) \tag{4}$$

This is so for this case, because the PFD_{avg} (i.e. average probability of failure of a safety system on demand), being a probability and not a frequency of the hazardous event, must be multiplied by d, the demand rate of the safety system (i.e. a frequency of hazardous event per hour per safety function), to get the overall frequency of hazardous event per hour for the given safety function.

Comparing Equations (3) and (4) leads to the following relationship (Braband et al., 2009):

$$THR = d \times PFD_{avg} \tag{5}$$

4. Applying the relationship between PFD_{avg} and THR to cross-acceptance based on SIL equivalence

4.1. Case 1: IEC 61508-related low-demand safety system

With respect to Equation (5), if the SIL of a safety system developed according to EN 50129 is defined by a specified range of THR, a similar product developed according to IEC 61508 as low-demand must have a demand rate, d equal to 10^{-4} per hour to be considered as having an equivalent SIL as shown in Table 4. This is explained as follows.

In the process industry, the initiating event frequency for small fires according to CCPS (2001) is 10^{-1} per year. This is the same as the demand rate, d (per year) at which a fire safety system (an Independent Protection Layer—IPL) is required to respond in a fire scenario involving one IPL (CCPS, 2001). Converting the demand rate of 10^{-1} per year to per hour gives $\sim 10^{-5}$ per hour—a more desirable value than the corresponding one used in Table 4. If it is assumed that the aforementioned initiating event frequency is too conservative and it is therefore increased by e.g. 100-folds to 1 per year, this converts to $\sim 10^{-4}$ per hour—the condition that guarantees SIL equivalence as shown in Table 4.

Table 4. SIL equivalence table for IEC 61508-related low-demand safety system in relation to EN 50129.

THR (Railway—EN 50129)	SIL	$PFD_{avg} \times d$ (Generic—IEC 61508)
$\geq 10^{-9}$ to $< 10^{-8}$	4	$(\geq 10^{-5}$ to $< 10^{-4}) \times 10^{-4}$
$\geq 10^{-8}$ to $< 10^{-7}$	3	$(\geq 10^{-4}$ to $< 10^{-3}) \times 10^{-4}$
$\geq 10^{-7}$ to $< 10^{-6}$	2	$(\geq 10^{-3}$ to $< 10^{-2}) \times 10^{-4}$
$\geq 10^{-6}$ to $< 10^{-5}$	1	$(\geq 10^{-2}$ to $< 10^{-1}) \times 10^{-4}$

In the railway industry, with respect to the Durable and Reliable Tunnel Structures (DARTS) project, the initiating event frequency for fire used in the event tree of a fire in a train tunnel is 10^{-8} per year, which converts to about 10^{-11} per hour (DARTS, 2004; Vrouwenvelder & Krom, 2004). If this value is considered as the demand rate for a safety system designed based on IEC 61508, such a safety system also proves adequate robustness for railway application in relation to Table 4. This is consistent with the report of the International Railway Industry (IRA), wherein it is stated that systems of whatever demand mode can be modelled as continuous-demand-mode systems (TPD, 2019). This implies that a fire safety system designed as low-demand based on IEC 61508 could still be sufficient for the railway fire safety function, even though it had not been designed as continuous/high-demand based on EN 50129.

Based on the aforementioned analysis, it can be stated that given the PFD_{avg}, the factor that influences SIL equivalence in relation to IEC 61508 and EN 50129 is the demand rate. A demand rate of 10^{-4} per hour is a necessary and sufficient condition for establishing SIL equivalence.

4.2. Case 2: IEC 61508-related continuous/high-demand safety system

For a fire safety system developed as high-demand based on IEC 61508, the PFH is equal to the THR (Braband et al., 2009). This is evident in Table 5 which is adapted from the SIL tables in IEC 61508 (2010) and EN 50129 (2018). Hence, there is an obvious direct evidence of SIL equivalence between IEC 61508 and EN 50129 without the need for further analysis.

5. The influence of SIL-related input data sources on cross-acceptance

The reliability of the input data used to calculate the PFD_{avg} which is in turn used to determine the SIL is of paramount importance because an erroneous adoption of the failure rate leads to wrong values of PFD_{avg} and SFF. An incorrect PFD_{avg} may lead to an incorrect SIL claim, which further leads to an incorrect SIL equivalence claim between IEC 61508 and EN 50129, implying an incorrect basis for cross-acceptance.

Table 5. SIL equivalence table for IEC 61508-related continuous/high-demand safety system in relation to EN 50129.

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

Table 6. Fire and gas detectors input data from generic and manufacturer data sources.

ID	Generic data (PDS Data Handbook, 2013)	Manufacturer data (Certified by Exida)
Equipment	Flame detector	X33AF Multi-spectrum IR flame detector
Failure rate (DU)	5.0×10^{-7}/h	1.24×10^{-7}/h
Failure rate (DD)	1.2×10^{-6}/h	6.34×10^{-7}/h
Failure rate (Spurious)	3.8×10^{-6}/h	2.137×10^{-6}/h
Diagnostic coverage	0.70	0.84
SFF	91%	95.7%
β factor	0.07	–
Equipment	Gas detector, IR point	HC400 IR gas detector
Failure rate (DU)	6.0×10^{-7}/h	1.62×10^{-7}/h
Failure rate (DD)	1.9×10^{-6}/h	1.06×10^{-6}/h
Failure rate (Spurious)	2.2×10^{-6}/h	4.2×10^{-8}/h
Diagnostic coverage	0.75	0.87
SFF	87%	87.2%
β factor	0.07	–

In the following, a study of a fire and gas system (FGS) encompassing flame detectors, flammable gas detectors, and a logic solver is used to validate the influence of reliability input data sources on cross-acceptance and to guide practitioners on the prioritisation of such data.

5.1. Comparison of SIL-related input data sources for fire and gas system

In this section, generic input data collected from SINTEF's PDS Data Handbook (Håbrekke et al., 2013) and manufacturer data from the certification portfolio of Exida and TUV are compared in Tables 6 and 7.

5.2. Calculation and analysis of results

The average probability of failure on demand (PFD_{avg}) for a fire and gas system (FGS) can be generally expressed as:

$$PFD_{avg} = PFD_{avg(Sensor)} + PFD_{avg(Logic\,Solver)} \tag{6}$$

In this paper, a simplified method is chosen to calculate the PFD_{avg} for a fire and gas system consisting of flame detector sensors in 1oo2

Table 7. Fire and gas control panels input data from generic and manufacturer data sources.

ID	Generic data (PDS Data Handbook, 2013)	Manufacturer data (Certified by TUV)
Equipment	Control logic unit—programmable safety system	Fire and gas control panel (BS 420/BSD310)
Failure rate (DU)	8.0×10^{-7}/h (AI + CPU + DO)	Failure rate (*D*) $= 8.0 \times 10^{-8}$/h
Failure rate (DD)	7.2×10^{-6}/h (AI + CPU + DO)	
Failure rate (Spurious)	8.0×10^{-6}/h (AI + CPU + DO)	–
Diagnostic coverage	0.9	–
SFF	95%	96%
β factor	0.05	–
PFD$_{avg}$		3.57×10^{-5} (Given HFT $=$ 0, $\tau = 12$ months)

(i.e. 1-out-of-2) voting, a flammable gas detector sensor in 2oo3 (i.e. 2-out-of-3) voting and a logic solver in a 1oo1 (i.e. 1-out-of-1) configuration.

Using the flame detector (FD) sensor generic data,

$$PFD_{avg(FD\,Sensor)} = \frac{[(1-\beta_{FD}) \cdot \lambda_{FD,DU} \cdot \tau]^2}{3} + \frac{\beta_{FD} \cdot \lambda_{FD,DU} \cdot \tau}{2} = 1.59 \times 10^{-4} \tag{7}$$

Where:

- $PFD_{avg(FD\,Sensor)}$ denotes the average probability of failure on demand of the flame detector sensor.
- β_{FD} denotes the beta factor of the flame detector sensor.
- $\lambda_{FD,DU}$ denotes the rate of dangerous undetected failures in the flame detector sensor.
- τ denotes the test interval.

Using the gas detector (GD) sensor generic data,

$$PFD_{avg(GD\,Sensor)} = [(1-\beta_{GD}) \cdot \lambda_{GD,DU} \cdot \tau]^2 + \frac{\beta_{GD} \cdot \lambda_{GD,DU} \cdot \tau}{2} = 2.08 \times 10^{-4} \tag{8}$$

Where:

- $PFD_{avg(GD\,Sensor)}$ denotes the average probability of failure on demand of the gas detector sensor.
- β_{GD} denotes the beta factor of the gas detector sensor.
- $\lambda_{GD,DU}$ denotes the rate of dangerous undetected failures in the gas detector sensor.
- τ denotes the test interval.

Using the generic data of the logic solver (LS), a single unit without any voting structure,

$$PFD_{avg(LS)} = \frac{\lambda_{LS,DU} \cdot \tau}{2} = 3.5 \times 10^{-3} \tag{9}$$

Where:

- $PFD_{avg(LS)}$ denotes the average probability of failure on demand of the logic solver.
- $\lambda_{LS,DU}$ denotes the rate of dangerous undetected failures in the logic solver.
- τ denotes the test interval.

Therefore,

$$PFD_{avg} = PFD_{avg(FD\,sensor)} + PFD_{avg(GD\,sensor)} + PFD_{avg(LS)} = 3.87 \times 10^{-3} \quad (10)$$

If similar calculations are performed using manufacturer data, the results in Table 8 are realised. Table 8 shows the comparison of PFD_{avg} obtained from the different data sources. The calculation method is the same as the previous, but input data are changed. Beta-Factor from generic data is available for both.

As seen in Table 8, the PFD_{avg} calculated by using generic data is about 30 times that calculated by using manufacturing data. It is also seen that the former corresponds to SIL 2, whereas the latter corresponds to SIL 3 according to IEC 61508 (2010). The PFD_{avg} using generic date is higher, because the generic data considers both systematic failure and random hardware failure based on operational experience, whereas manufacturer data reflects only random failure. This is consistent with the observation by SINTEF of discrepancy in failure rate data between manufacturer/certificate source and operational data collection source (Ottermo et al., 2021), whereby the former lacks systematic failure contribution in addition to being exaggerated by manufacturers (Hauge et al., 2010).

The aforementioned analysis implies that using generic data is more robust for reliability quantification and compliance, whereas manufacturer data is well-suited for comparing reliability performance between similar equipment. In addition, it can be deduced that using manufacturer data only for calculating the PFD_{avg} of a system or product can lead to wrong decision-making on cross-acceptance. Furthermore, it can be concluded also that variation between corresponding data of similar equipment from different manufacturers can also add to cross-acceptance uncertainty.

Table 8. Comparison of PFD_{avg} and SIL calculated from generic and manufacturer data sources for fire and gas system.

ID	PFD_{avg} from generic data	PFD_{avg} from manufacturer data
Flame detector sensor	1.59×10^{-4}	3.85×10^{-5}
Gas detector sensor	2.08×10^{-4}	5.14×10^{-5}
Logic solver	3.50×10^{-3}	3.57×10^{-5}
Total	3.87×10^{-3}	1.26×10^{-4}
SIL (IEC 61508, 2010)	SIL 2	SIL 3

6. Discussion and recommendations

Data for calculating PFD_{avg} should be carefully chosen to suit the given purpose. Generic data is the better choice to reflect the uncertainty of installation and maintenance being expressed as DU failure, and hence should be used for research and development of a system since it offers more assurance for a finished product in use. Therefore, it should be used for cross-acceptance decision-making. However, manufacturer data can be used to select and procure the subsystems or parts and still be used for cross-acceptance decision-making, provided the test interval, Mean Time To Repair (MTTR), and Mean Repair Time (MRT) are taken into account when evaluating the PFD_{avg} (IEC 61508, 2010).

Besides, for cross-acceptance from IEC 61508 (2010) to EN 50129 (2018), establishing SIL equivalence alone for a fire safety system originally developed based on IEC 61508 (2010) is necessary, but not sufficient. SIL equivalence only expresses the random hardware integrity, a measure of the extent to which the safety system is dependable. Architectural constraints and systematic capability, which are other factors that influence SIL achievement and certification, must be considered in addition.

6.1. Architectural constraints

Architectural constraints, like SIL equivalence, also have the objective of reduction of random hardware failures. They are constraints that encompass hardware fault tolerance (HFT) and its safe failure fraction (SFF), which are imposed by functional safety standards to regulate the SIL that can be claimed for a safety function as shown in Table 9 (IEC 61508, 2010; Rausand & Høyland, 2004). HFT implies the ability to tolerate a given number of hardware failures based on the addition of a commensurate number of redundant elements, whereas SFF is the fraction of the total random hardware failure rate of a safety system that manifests as either a safe failure or a detected dangerous failure (Rausand & Høyland, 2004). Architectural constraints require that a minimum degree of redundancy is established for a subsystem based on its SFF to guarantee the required HFT (Rausand &

Table 9. The IEC 61508 architectural constraints on low complexity subsystems.

	HFT		
SFF	0	1	2
$<60\%$	SIL 1	SIL 2	SIL 3
60–90%	SIL 2	SIL 3	SIL 4
90–99%	SIL 3	SIL 4	SIL 4
$\geq 99\%$	SIL 3	SIL 4	SIL 4

Høyland, 2004). E.g. a 1oo1 (i.e. 1-out-of-1) safety architecture corresponds to HFT0 (i.e. hardware fault tolerance of 0), whereas a 1oo2 (i.e. 1-out-of-2) architecture corresponds to HFT1 (i.e. hardware fault tolerance of 1). There is no equivalent to SFF in the railway industry and by implication in EN 50129 (TPD, 2019), however, requirements do exist for the implementation of redundancy in processing channels depending on the SIL (Arriola et al., 2012).

Architectural constraints express (through redundancy) the quality of resilience, i.e. the ability to adapt to or recover from random failure events and acquire stability in the new state the system has transited to (Okoh & Haugen, 2015). Besides, they also help to compensate for the uncertainty associated with input reliability data and thus enhance the integrity of a safety system's design. As a recommendation, the induced resilience property and the reduction of uncertainty by limiting what SIL can be claimed offer reasonable benefits that should earn an IEC 61508-certified safety system some credits en route to EN 50129 certification.

6.2. Systematic capability

Both IEC 61508 and EN 50129 recognise the fact that safety system failures are not only caused by random technical factors, but also by human factors. The latter, also known as systematic failures, include human errors in the safety requirements specification, design, manufacture, installation, and use of hardware and software. Such failures are preventable through the application of procedural safety strategies (Amyotte et al., 2007), which include a quality management system and safety manual applicable to a typical safety case (Myklebust & Stålhane, 2018; Okoh, 2019). Decreasing systematic failures leads to increasing safety integrity. Meanwhile, systematic capability (SC) is a term used to express confidence in claiming a certain level of safety integrity (SIL) based on having strictly applied the procedural safety strategies required for reducing systematic failures (IEC 61508, 2010). Per standard definition, the systematic capability is 'a measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified Safety Integrity Level (SIL), in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element' (IEC 61508, 2010). Table 10 is one of several tables in IEC 61508 (2010), which shows how systematic capability is evaluated. The selection of any of these tables depends on the route to SC followed according as guided by the standard. Furthermore, with respect to Table 10, for example, if all the measures corresponding to say, SIL 2, are applied, then it can be declared that SC equals 2 for the given

Table 10. IEC 61508-2010 Table A.15—techniques and measures to control systematic failures caused by hardware design.

Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
Failure detection by on-line monitoring	A.1.1	HR low	HR low	HR medium	HR high
Tests by redundant hardware	A.2.1	HR low	HR low	HR medium	HR high
Standard test access port and boundary-scan architecture	A.2.3	HR low	HR low	HR medium	HR high
Code protection	A.6.2	HR low	HR low	HR medium	HR high
Diverse hardware	B.1.4	—–low	—–low	R medium	R high

Table 11. Measures extracted from EN 50129 for mitigation of systematic failures (copied from TPD, 2019 for illustration only).

Technique/measure	Ref	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
FMEA/FMECA	H.2.30.4 H.2.30.5 See Note 1	–	R	R	M	M
Bent pin analysis/cable failure matrix analysis	H.2.14.1	–	R	R	HR	HR
Electromagnetic compatibility analysis	H.2.14.2	–	R	R	HR	HR
Energy trace and barrier analysis	H.2.14.3	–	R	R	HR	HR
Materials compatibility analysis	H.2.31.1	–	R	R	HR	HR
Fault tree analysis	H.2.30.7 See Note 1	–	R	R	HR	HR

element/component. In Table 10, R and HR mean Recommended and Highly Recommended, respectively, whereas low, medium, and high express the impact.

In EN 50129, a corresponding approach is the implementation of similar tables. Table 11, an example of such tables, presents risk analysis techniques among others (e.g. FMEA, FTA, etc., classified as recommended, highly recommended, or mandatory for a given SIL) as measures to enhance confidence in making a given SIL claim (EN 50129, 2018; TPD, 2019). The use of risk analysis techniques implies that EN 50129 approach also contributes to the reduction of random hardware failure (TPD, 2019).

Based on the preceding study and discussion, supported by references to authorities, it can be deduced that IEC 61508 and EN 50129 are similar with respect to standard requirements for the detailed design architecture (Arriola et al., 2012; Smith & Simpson, 2011). Hence, for cross-acceptance of fire safety systems from IEC 61508 to EN 50129 domain, the demonstration of fulfillment of the following are recommended as the basis for approval: (1) SIL equivalence, (2) the original requirements of architectural constraints, (3) the original requirements of systematic capability, (4) the original safety case featuring the quality management, safety management, and technical safety reports, (5) a supplementary safety case accounting for any differences between the original and the target (Ruiz et al., 2017; TR 50506, 2007), and (6) safety manuals for the 'pre-existing' items (Filip, 2020). The framework recommended in this paper is consistent with the positions of BS PD CLC/TR 50506-1 (2007), Filip (2020), IRSE (1992), and Ruiz et al. (2017). The quality and safety management, which are normally reported, reduce the occurrence of human errors and thus minimise the risk of systematic faults, whereas the technical safety report presents technical evidence that the product is safe for its intended application, and the safety manuals contain information about equipment reliability data and recommended operating and environmental conditions of use as well as test and maintenance procedures. It is recommended to provide safety manuals for commercial-of-the-shelf (COTS) components and the finished product. The proposal by Filip (2020) of risk management with CSM-RA (if a significant change to the railway domain is expected) of a 'pre-existing' item is not necessary if the fire safety system is not integrated with a control system, since this is not expected to cause any disruption to the railway system.

7. Conclusion

This paper has established a framework for cross-acceptance of fire safety systems from the generic (based on IEC 61508) to the railway industry (based on EN 50129). Following a study of the aforementioned standards and several literature related to dependability, the concept of SIL equivalence was established and suggested together with architectural constraints, systematic capability, safety cases, and safety manuals as robust criteria for the fulfillment of cross-acceptance. The original safety case would consist of the quality management, the safety management, and the technical safety reports in relation to IEC 61508, whereas the supplementary safety case would address differences between IEC 61508 and EN 50129 provisions, and the safety manuals would encompass the safety manuals of individual COTS components and the whole system, which aligns with industry best-practice. The framework is based on international standards and is an improvement on the approach of MoU between a few countries that is unconventional, limited in scope, and not easily accessible to the wider public to promote universal uniformity. This paper is expected to give national railway authorities, notified bodies, and other stakeholders an alternative perspective for cross-acceptance, thus contributing to promoting globalisation and the ease of doing business across industrial sectors. In addition, the paper advised on the prioritisation and augmentation of SIL-related input data for optimal decision-making on cross-acceptance.

Nomenclature

AI	Analog Input
BS	British Standard
CCPS	Centre for Chemical Process Safety
CENELEC	European Committee for Electrotechnical Standardisation
CLC	CENELEC
COTS	Commercial off The Shelf
CPU	Central Processing Unit
CSM-RA	Common Safety Method for Risk Evaluation and Assessment
EBA	Federal Railway Authority, Germany
D	Dangerous (failure)
DARTS	Durable and Reliable Tunnel Structures
DD	Dangerous Detected (failure)
DO	Digital Output
DU	Dangerous Undetected (failure)
E/E/PE	Electrical/Electronic/Programmable Electronic
FGS	Fire and Gas System
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HR	Highly Recommended
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
IR	Infra-Red
IR_i	Individual Risk Index
IRSE	Institution of Railway Signal Engineers
ISO	International Organisation for Standardisation
M	Mandatory
MoU	Memorandum of Understanding
NJSPC	New Jersey State Planning Commission
PD	Published Document
PFD_{avg}	Average Probability of Failure on Demand
PFH	Frequency of Dangerous Failure
PLC	Public Liability Company
R	Recommended
SC	Systematic Capability
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
THR	Tolerable Hazard Rate
TPD	Technical Programme Delivery Ltd.
TR	Technical Report

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

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

References

Amyotte, P. R., Goraya, A. U., Hendershot, D. C., & Khan, F. I. (2007). Incorporation of inherent safety principles in process safety management. *Process Safety Progress*, *26*(4), 333–346. https://doi.org/10.1002/prs.10217

Arriola, A. V., Samper, J. M., & Lagunilla, J. M. (2012). Fault injection for on-board ERTMS/ETCS safety assessment. In F. Flammini (Ed.), *Railway safety, reliability and security: Technologies and systems engineering*. IGI Global.

Baufreton, P., Blanquart, J. P., Boulanger, J., Delseny, H., Derrien, J., Gassino, J., Ladier, G., Ledinot, E., Leeman, M., & Quéré, P. (2010). Multi-domain comparison of safety standards. In *ERTS2 2010*. Embedded Real Time Software & Systems. Retrieved from https://hal.archives-ouvertes.fr/hal-02264379

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). Hamburg: Springer.

CCPS (2001). *Layer of protection analysis: Simplified process risk assessment*. Wiley.

Coenraad, W. (2005). Proposed cross-acceptance process for railway signalling systems and equipment. Retrieved from https://eurailpress-archiv.de/SingleView.aspx?show=18981

DARTS (2004). *DARTS WP5 – Integrated design examples* (Report No. 141, Technical Report). European Commission.

EBA (2021). Cross acceptance. Retrieved from https://www.eba.bund.de/EN/TechnicalInformation/CrossAcceptance/crossacceptance_node.html

EN 50129 (2018). *Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling* (Technical Report). European Committee for Electrotechnical Standardization.

Filip, A. (2020). Certification of EGNOS safety-of-life service for ERTMS according to IEC 61508 and EN 50129. *WIT Transactions on the Built Environment*, *199*, 115–126. https://doi.org/10.2495/CR200111

Håbrekke, S., Hauge, S., & Onshus, T. (2013). *Reliability data for safety instrumented systems: PDS Data Handbook 2013 edition* (2013 ed.). Sintef Technology and Society.

Hauge, S., Lundteigen, M. A., Hokstad, P., & Håbrekke, S. (2010). *Reliability prediction method for safety instrumented systems – PDS method handbook 2010 edition* (2010 ed.). Sintef Technology and Society.

IEC 61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems* (Technical Report). International Electrotechnical Commission.

IRSE (1992). *ITC Report 01: System safety validation with regard to cross acceptance of signalling systems by the railways* (Technical Report). Institution of Railway Signalling Engineers.

IRSE (2003). *ITC Report 06: Proposed cross acceptance processes for railway signalling systems and equipment* (Technical Report). Institution of Railway Signalling Engineers.

IRSE (2020). *Cross acceptance of systems and equipment developed under different acceptance frameworks* (Technical Report). Institution of Railway Signalling Engineers. Retrieved from https://webinfo.uk/webdocssl/irse-kbase/ref-viewer.aspx?RefNo=1606493530&NextPrevious=YES

Kessell, C. (2020). *Cross acceptance of systems and equipment*. Retrieved from https://www.railengineer.co.uk/cross-acceptance-of-systems-and-equipment/

Li, J. (2018). SIL implementation on safety functions in mass transit system. *International Journal of Mathematical, Engineering and Management Sciences*, *3*(3), 258–270. https://doi.org/10.33889/IJMEMS.2018.3.3-018

Machrouh, J., Blanquart, J. P., Baufreton, P., Boulanger, J. L., Delseny, H., Gassino, J., Ladier, G., Ledinot, E., Leeman, M., Astruc, J. M., Quéré, P., Ricque, B., & Deleuze, G. (2012). Cross domain comparison of system assurance. In *ERTS2 2012*. Embedded Real Time Software & Systems.

Myklebust, T., & Stålhane, T. (2018). *The agile safety case*. Springer International Publishing. https://doi.org/10.1007/978-3-319-70265-0

NJSPC (2021). *What is cross-acceptance?* (Technical Report). New Jersey State Planning Commission. Retrieved from https://nj.gov/state/planning/assets/docs/publications/028-what-is-cross-acceptance.pdf

Okoh, P. (2019). Integrated logistics support and asset management (ILSAM). *Infrastructure Asset Management*, *6*(4), 245–257. https://doi.org/10.1680/jinam.17.00026

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). A study of maintenance-related major accident cases in the 21st century. *Process Safety and Environmental Protection*, *92*(4), 346–356. https://doi.org/10.1016/j.psep.2014.03.001

Okoh, P., & Haugen, S. (2015). Improving the robustness and resilience properties of maintenance. *Process Safety and Environmental Protection*, *94*, 212–226. https://doi.org/10.1016/j.psep.2014.06.014

Okoh, P., Onshus, T., Lycke, E., Winther-Larssen, E., & Sigmundstad, J. N. (2019). Independence classification, split logic and shared final element for all-electric subsea safety system. In *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*. Research Publishing Services. https://doi.org/10.3850/978-981-11-2724-3_0486-cd

Ottermo, M., Hauge, S., & Håbrekke, S. (2021). *Reliability data for safety equipment: PDS Data Handbook – 2021 edition* (2021 ed.). SINTEF Digital.

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.

Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). John Wiley & Sons.

Reder, H. J. (2006). Cross-acceptance of safety approvals in the rail industry: A manufacturer's viewpoint. In *2006 1st IET International Conference on System Safety*. IET.

Ruiz, A., Juez, G., Espinoza, H., Luis De La Vara, J., & Larrucea, X. (2017). Reuse of safety certification artefacts across standards and domains: A systematic approach. *Reliability Engineering & System Safety*, *158*, 153–171. http://www.opencoss-project.eu. https://doi.org/10.1016/j.ress.2016.08.017

Smith, D. J., & Simpson, K. G. (2011). Other industry sectors. In *Safety critical systems handbook*. Elsevier. https://doi.org/10.1016/B978-0-08-096781-3.10010-0

TPD (2019). *International engineering safety management good practice guidance: Application Note 9 safety integrity within engineering safety management* (Technical Report). International Railway Industry.

TR 50506 (2007). *Railway applications – Communication, signalling and processing systems – Application guide for EN 50129 – Part 1: Cross-acceptance* (Technical Report).

Vrouwenvelder, A., & Krom, A. H. M. (2004). Hazards and the consequences for tunnel structures and human life. In *Safe & reliable tunnels*. Innovative European Achievements. Retrieved from https://www.researchgate.net/publication/246360919_HAZARDS_AND_THE_CONSEQUENCES_FOR_TUNNEL_STRUCTURES_AND_HUMAN_LIFE