

Evaluation Process for the Hardware Safety Integrity Level

Sung Kyu Kim and Yong Soo Kim

Abstract—Safety instrumented systems (SISs) are becoming increasingly complex and the proportion of programmable electronic parts is growing. The IEC 61508 global standard was established to ensure the functional safety of SISs, but it was expressed in highly macroscopic terms. This study introduces an evaluation process for hardware safety integrity levels through failure modes, effects, and diagnostic analysis (FMEDA). FMEDA is widely used to evaluate safety levels, and it provides the information on failure rates and failure mode distributions necessary to calculate a diagnostic coverage factor for a given component. In our evaluation process, the components of the SIS subsystem are first defined in terms of failure modes and effects. Then, the failure rate and failure mechanism distribution are assigned to each component. The safety mode and detectability of each failure mode are determined for each component. Finally, the hardware safety integrity level is evaluated based on the calculated results.

Keywords—Safety instrumented system; Safety integrity level; Failure modes, effects, and diagnostic analysis; IEC 61508.

I. INTRODUCTION

COMPONENT and system reliability have been improving continuously. However, despite improved reliability, system failures still cause fatal accidents. Recently, computer systems have been widely applied to safety-related systems (SRSs) to achieve the desired safety functions. This trend forced the International Electro-technical Commission (IEC) to issue the IEC 61508 global standard related to the functional safety of SRSs [1].

IEC 61508, published in 2000, has been adopted by many countries as their national standard, and it is currently being updated. Two significant concepts, the safety life cycle and safety integrity level (SIL), appear in IEC 61508 [2].

Safety instrumented systems (SISs) are used in many industrial sectors to reduce the risk to human lives, the environment, and material assets. A SIS is installed to detect and respond to the onset of hazardous events by the use of electrical, electronic, or programmable electronic (E/E/PE) technology. In cars, the airbag and anti-lock braking systems are two examples of SIS applications. When a sensor detects that a car has collided, the airbag is activated. ABS prevents the wheels from locking during heavy braking so that the driver can

maintain control of the car. In the process industry, SISs are used to stop flow and isolate electrical equipment upon detected high pressures, high temperatures, fires, and gas leakages. One such SIS application is the high-integrity pressure protection system (HIPPS), which is used to prevent over-pressurisation in vessels and pipelines [3].

A SIL is not a property of a system, subsystem, element, or component. The correct interpretation of the phrase “SIL n SRS” (where n is 1, 2, 3, or 4) is that the system is potentially capable of supporting safety functions with a SIL up to n , where n corresponds to a range of safety integrity values. Safety integrity level 4 is the highest level, and safety integrity level 1 is the lowest [4].

The SIL is a criterion describing whether a component can meet the safety requirements of a SIS, derived from a risk analysis such as a hazard analysis and risk assessment. The SIL must include an evaluation of the related hardware and software. However, software SILs are difficult to evaluate quantitatively; instead, they are evaluated through a variety of qualitative techniques.

This article proposes an evaluation process for hardware SILs that is compliant with IEC 61508. The process applies failure modes, effects, and diagnostic analysis (FMEDA).

II. RELATED STUDIES

The safety lifecycle of IEC 61508 covers the development of a SIS, including all phases from “cradle to grave”. However, the standard is not very detailed when it comes to the product-development stages. To complement it, IEC 61508 can be combined with a reliability, availability, maintainability, and safety (RAMS) analysis. This approach covers all phases of the development process for a new product and is aimed at producers of complex products similar to SISs. A case study using a HIPPS was carried out by [3].

Given that the existing method based on merging rules suggested by IEC 61508 is straightforward to apply and does not take into account the value of the corresponding probability of failure on demand (PFD) of different subsystems, multiphase Markov modelling has been proposed to derive the SIL of a system [5]. Reference [6] describes an automatic transformed Markov model for reliability assessment of a SIS. Other methods used to determine SILs include a fuzzy probabilistic method [7] and a simple reliability block diagram method [2].

Hardware SILs are expressed by architectural constraints and the probability of failure. Architectural constraints are based on hardware fault tolerance (HFT) and safe failure fraction (SFF) concepts [8]. The probability of failure is classified into two reliability measures by demand rate.

Sung Kyu Kim is with the Department of Industrial and Management Engineering, Kyonggi University Graduate School, 154-42, Gwanggyosan-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, South Korea, (phone: +82 31-242-2872; fax: +82 31-244-3534; e-mail: kimsk@kgu.ac.kr).

Yong Soo Kim is an Assistant Professor of the Department of Industrial and Management Engineering, Kyonggi University, 154-42, Gwanggyosan-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, South Korea, (phone: +82 31-249-9771; fax: +82 31-244-3534; e-mail: kimys@kgu.ac.kr).

A variety of research on the role of architectural constraints has been carried out as follows. The SFF is not an adequate indicator of a component's reliability properties because two components with the same SFF may have quite different characteristics with respect to the rate of spurious operations, rate of dangerous failures, and diagnostic coverage (DC). Additionally, a high SFF does not always indicate a safe component, just as a low SFF is not always synonymous with an unsafe component. The SFF may give credit (in terms of increased SFF) to unsafe designs as well as punishment (in terms of unchanged or decreased SFF) to safe designs [9]. Reference [1] showed that the positive effect of SFF constraints on the hazardous event rate is almost negligible for a Type I system, i.e., one where the safe state is invariable. The negative effect of SFF constraints on safety is much stronger than the positive effects for a Type II system, i.e., one where the safe state is inherently variable and the trip is complete.

A study using the FMEDA method has been used to measure diagnostic coverage in programmable electronic systems [10]. Reference [11] described a safety assessment case study for a complex SIS using a FMEDA according to IEC 61508, assuming DC values of 0, 50, 75, and 100%. Reference [12] described how to increase the SIL of an emergency shutdown system (ESD) by applying a redundancy design to the switch and programmable logic controller (PLC). Reference [13] introduced a SIL estimation method for a safety assurance criterion and performed a case study using a flame scanner.

Other case studies have not used a FMEDA for a SIS. Reference [14] quantitatively analysed a complex guided transportation system [14] and a decay heat-removal system of a prototype fast breeder reactor [15] through a Monte Carlo simulation approach. Reference [16] describes the optimisation of proof-testing policies using genetic algorithms.

III. HARDWARE SIL CERTIFICATION PROCESS

A. Overview of the Safety Life Cycle of IEC 61508

According to IEC 61508, the safety life cycle determines the concept and scope of the SIS. The safety requirements are derived through a hazard and risk analysis. The standard verifies the safety requirements and designs of the SIS, as well as its realisation, installation, operation, and decommissioning (see Fig. 1).

Fig. 2 illustrates the realisation phase of the safety life cycle of an E/E/PE SRS. The realisation phase consists of system and software safety.

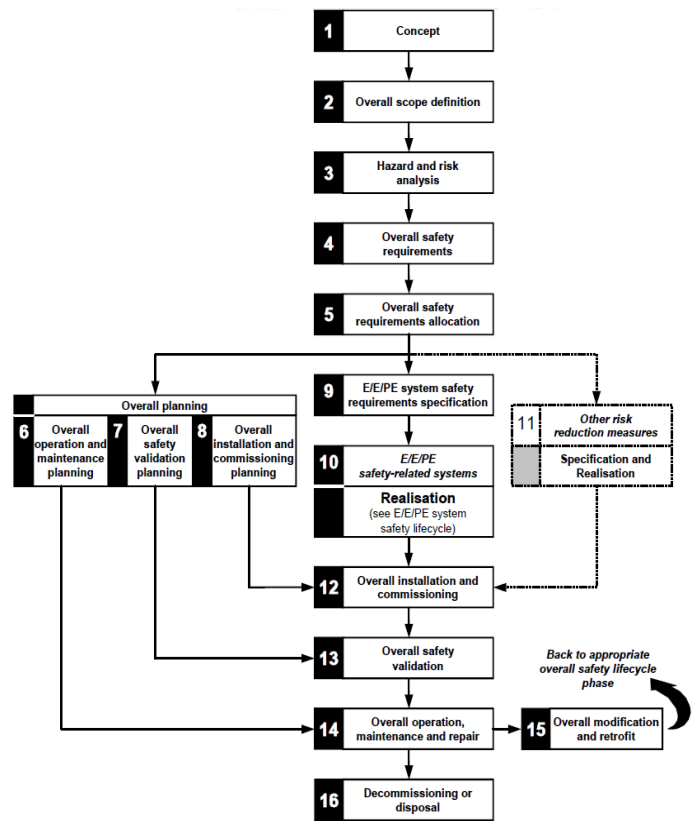


Fig. 1 Overall safety life cycle [17]

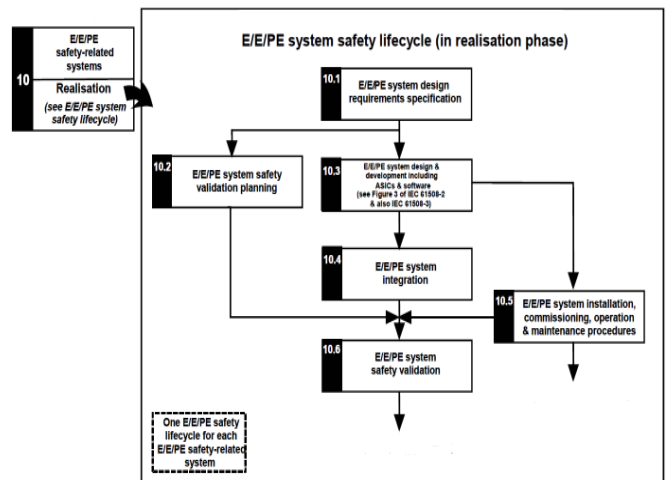


Fig. 2 E/E/PE system safety life cycle (in realisation phase) [17]

B. Safety Integrity Requirements

The first evaluation measure for a SIL is the architectural constraints that are defined in IEC 61508 and IEC 61511, as shown in Tables I and II for each type of component (A and B), based on combinations of the following aspects per subsystem. Tables I and II show the maximum allowable SIL for given HFTs and SFFs. Equation (1) gives the SFF as a ratio of the average rate of safe failures plus dangerous detected failures of the subsystem to the total average failure rate of the subsystem [8, 9], where λ_S is the safe failure rate, λ_{DD} is the dangerous

detected failure rate, and λ_{DU} is the dangerous undetected failure rate. The HFT is expressed as the minimum hardware fault tolerance for each subsystem of an E/E/PE SRS. If HFT '1' is specified, the selected configuration must tolerate one failure without affecting the safety instrumented function (SIF). Configurations that provide HFT '1' are, for example, 1oo2, 2oo3, and 3oo4, where a 'koon' system is functioning if at least k out of n components are functioning [9].

Type A components can be regarded as those we would like to achieve. For Type A components, the failure modes of all constituent components are well defined, and the behaviour of an element under fault conditions can be completely determined. Also, there are sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met. Otherwise, the component is regarded as type B [8].

TABLE I
ARCHITECTURAL CONSTRAINTS OF A TYPE A SUBSYSTEM [8]

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	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
≥99%	SIL 4	SIL 4	SIL 4

TABLE II
ARCHITECTURAL CONSTRAINTS OF A TYPE B SUBSYSTEM [8]

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
<60%	Not Allowed	SIL 1	SIL 2
60–<90%	SIL 1	SIL 2	SIL 3
90–<99%	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

$$SFF = \frac{\sum \lambda_s + \sum \lambda_{DD}}{\sum \lambda_s + \sum \lambda_{DD} + \sum \lambda_{DU}} \quad (1)$$

The SIL is a required reliability indicator for a SIF. Thus, the second measure used to evaluate a SIL is the probability of failure. This measure is classified into the average PFD for low-demand operation and the average frequency of dangerous failures per hour (PFH) for high-demand/continuous operation [4].

The mode of operation corresponds to the operational system's expected demand frequency on the safety system, and it can be further divided into low- and high-demand modes. The low-demand mode of operation implies irregular solicitations of the safety system, as is the case with a train's emergency braking system. To be considered lowdemand, the operational demand frequency can be no greater than once per year and no greater than twice the proof-test frequency. The high-demand/ continuous mode of operation has a greater demand frequency on the safety system [4], [18].

The PFD and PFH values defined by the SIL according to IEC 61508 are shown in Table III. The PFD and PFH can be calculated from Eqs. (2) and (4) for a single-channel (1oo1) system [19], where λ_D is the dangerous failure rate as the sum of λ_{DD} and λ_{DU} , t_{CE} is the channel equivalent mean downtime (hour), MRT is the mean repair time, and $MTTR$ is the mean time to restoration.

TABLE III
SAFETY INTEGRITY LEVELS – TARGET FAILURE MEASURES FOR A SAFETY FUNCTION OPERATING IN EACH DEMAND MODE [17]

Safety integrity level	Demand mode of operation	
	PFD	PFH
SIL 1	≥10 ⁻⁵ to <10 ⁻⁴	≥10 ⁻⁹ to <10 ⁻⁸
SIL 2	≥10 ⁻⁴ to <10 ⁻³	≥10 ⁻⁸ to <10 ⁻⁷
SIL 3	≥10 ⁻³ to <10 ⁻²	≥10 ⁻⁷ to <10 ⁻⁶
SIL 4	≥10 ⁻² to <10 ⁻¹	≥10 ⁻⁶ to <10 ⁻⁵

$$PFD_{1oo1} = \left(\sum \lambda_{DD} + \sum \lambda_{DU} \right) t_{CE} \quad (2)$$

$$t_{CE} = \sum \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MRT \right) + \sum \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (3)$$

$$PFH_{1oo1} = \sum \lambda_{DU} \quad (4)$$

C. Hardware SIL Certification Process Based on a FMEDA

A FMEDA is an extension of the well-proven failure modes and effects analysis (FMEA) technique, and it can be used on electrical or mechanical products. It combines standard FMEA techniques with extensions to identify online diagnostic techniques. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, and dangerous undetected) in safety models [10]. A FMEDA sheet consists of several columns that include the component number, type of component, failure mode, failure distribution, possible failure, failure effect, failure rate, safe mode, detectability, diagnostic method, safe detected failure rate, safe undetected failure rate, dangerous detected failure rate, and dangerous undetected failure rate.

This article proposes an evaluation process for hardware SILs through an eight-stage process using FMEDA (see Fig. 3).

In step 1, the parts list is constructed using a bill of materials (BOM), schematic drawing, and block diagrams. Additionally, all components are categorised into subsystems.

Step 2 involves a FMEA. This step is performed by interviewing engineers about the failure modes and the effects of each component.

In Step 3, the failure rate is assigned to each component based on field failure data. If field failure data do not exist, a variety of guidebooks such as Telcordia Standards SR-332, RIAC HDBK 217F, IEC 62380, or SN 29500 are used. Additionally, failure in time (FIT) is used as a unit failure rate expressed as the number of failures per 1 billion hours.

In step 4, the failure mechanism distribution is assigned to each component based on field failure data. As many manufacturers do supply field failure data, guidelines such as RIAC FMD-97 and IEC 62061 are often used.

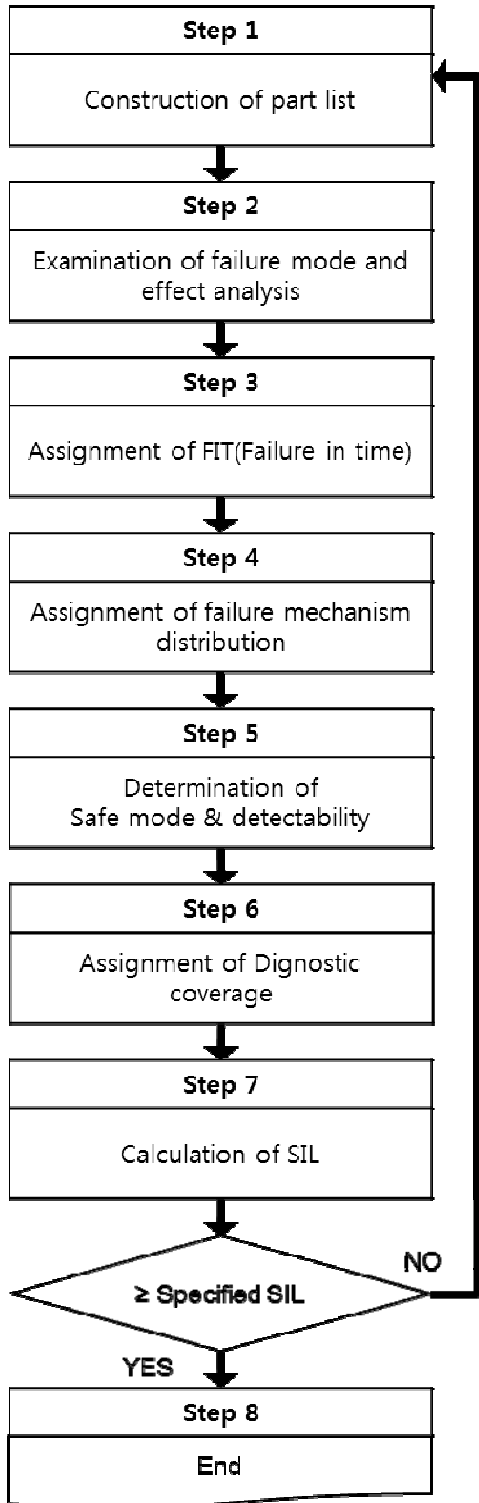


Fig. 3 Hardware SIL certification evaluation process based on aFMEDA [13]

In step 5, the safe mode and detectability of each failure

mode are determined by standards or engineers' opinions. Additionally, we consider that a dangerous failure prevents a safety function from operating when required or causes a safety function to fail such that the equipment under control (EUC) is put into a hazardous or potentially hazardous state according to IEC 61508-4 [4]. If a failure can be detected, the detection method must be defined.

In step 6, the DC for detected failure method is determined by referencing the component specifications and IEC 61508-2. Failure rates are then assigned to safe detected failure rates, safe undetected failure rates, dangerous detected failure rates, and dangerous undetected failure rates based on the safety mode, detectability, and DC (see Fig. 4).

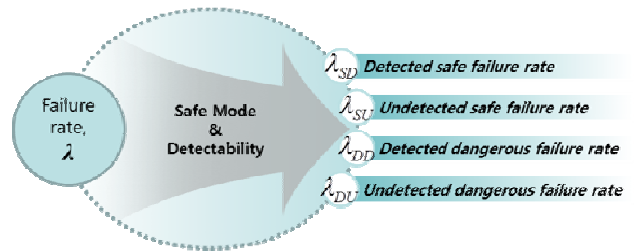


Fig. 4 Failure rate based on safety mode and detectability

In step 7, the SIL is calculated using the PFD (or PFH), HFT, and SFF based on the outcomes obtained from steps 1 to 6. If the requirement of the specified SIL with respect to the safety function of the specified element can be met, then the process ends. If not, the design of the system and/or equipment will be improved.

IV. CONCLUSION

IEC 61508 is a basic global safety standard that requires one to specify the safety function and SIL to be achieved by a SRS. The highest SIL that can be claimed for the safety function of a subsystem of a SRS is limited by architectural constraints [1]. However, the existing evaluation process of the safety life cycle is not very detailed when it comes to evaluation stages for hardware SILs.

This study describes an eight-step process based on a FMEDA method that can be used to evaluate hardware SILs for reliability verification of a SIS. This process defines the components of the SIS subsystems, failure modes, and failure effects. It assigns a failure mechanism distribution and failure rate to each component and determines the safety mode as well as the detectability of each failure mode. Hardware SILs can be evaluated from these results. This procedure is expected to be useful when evaluating hardware SILs for a SIS.

ACKNOWLEDGMENT

This work was supported by Kyonggi University Research Grant 2012.

REFERENCES

- [1] I. Yoshimura, and Y. Sato, "Safety achieved by the safe failure fraction (SFF) in IEC 61508," *IEEE Trans. Reliability*, vol. 57, no. 4, pp. 662–669, Dec. 2008.
- [2] H. Guo and X. Yang, "A simple reliability block diagram method for safety integrity verification," *Reliability Engineering and System Safety*, vol. 92, no. 9, pp. 1267–1273, Sep. 2007.
- [3] M. A. Lundteigen, M. Rausand, and I. B. Utne, "Integrating RAMS engineering and management with the safety life cycle of IEC 61508," *Reliability Engineering and System Safety*, vol. 94, no. 12, pp. 1894–1903, Dec. 2009.
- [4] IEC 61508-4, "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations," 2nd ed., Apr. 2010.
- [5] Y. Langeron, A. Barros, A. Grall and C. Bérenguer, "Combination of safety integrity levels (SILs): A study of IEC61508 merging rules," *Journal of Loss Prevention in the Process Industries*, vol. 21, no. 4, pp. 437-449, July 2008.
- [6] H. Guo and X. Yang, "Automatic creation of Markov models for reliability assessment of safety instrumented systems," *Reliability Engineering and System Safety*, vol. 93, no. 6, pp. 829–837, June 2008.
- [7] M. Sallak, C. Simon, and J.-F. Aubry, "A fuzzy probabilistic approach for determining safety integrity level," *IEEE Trans. Fuzzy Systems*, vol. 16, no. 1, pp. 239–248, Feb. 2008.
- [8] IEC 61508-2, "Functional safety of electrical/electronic/programmable electronic safety-related systems–Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems," 2nd ed., Apr. 2010.
- [9] M. A. Lundteigen and M. Rausand, "Architectural constraints in IEC 61508: do they have the intended effect?," *Reliability Engineering and System Safety*, vol. 94, no. 2, pp. 520–525, Feb. 2009.
- [10] W.M. Goble and A.C. Brombacher, "Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems," *Reliability Engineering and System Safety*, vol. 66, no. 2, pp. 145–148, Nov. 1999.
- [11] M. Catelani, L. Ciani and V. Luongo, "The FMEDA approach to improve the safety assessment according to the IEC61508," *Microelectronics Reliability*, vol. 50, no. 9-11, pp. 1230-1235, Sep.-Nov. 2010.
- [12] J. J. Sammarco, "Programmable electronic and hardwired emergency shutdown systems: A quantified safety analysis," *IEEE Trans. Industry Applications*, vol. 43, no. 4, pp. 1061–1068, July-Aug. 2007.
- [13] S. K. Kim and Y. S. Kim, "A study on FMEDA process for SIL certification - A case study of a flame scanner -," *IE Interfaces*, vol. 25, no. 4, pp.422-430, Dec. 2012.
- [14] J. Beugin, D. Renaux and L. Cauffriez, "A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems," *Reliability Engineering and System Safety*, vol. 92, no. 12, pp. 1684–1700, Dec. 2007.
- [15] T. S. Mathews, M. Ramakrishnan, U. Parthasarathy, A. J. Arul and C. S. Kumar, "Functional reliability analysis of safety grade decay heat removal system of indian 500 MWe (PFBR)," *Nuclear Engineering and Design*, vol. 238, no. 9, pp. 2369–2376, Sep. 2008.
- [16] A.C. Torres-Echeverría, S. Martorell and H. A. Thompson, "Modelling and optimization of proof testing policies for safety instrumented systems," *Reliability Engineering and System Safety*, vol. 94, no. 4, pp. 838–854, Apr. 2009.
- [17] IEC 61508-1, "Functional safety of electrical/electronic/programmable electronic safety-related systems–Part 1: General requirements," 2nd ed., Apr. 2010.
- [18] H. Jin, M. A. Lundteigen and M. Rausand, "Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation," *Reliability Engineering and System Safety*, vol. 96, no. 3, pp. 365–373, March 2011.
- [19] IEC 61508-6, "Functional safety of electrical/electronic/programmable electronic safety-related systems–Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3," 2nd ed., Apr. 2010.