International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 3 (2017) pp. 359-364

A Case Study on an Evaluation Procedure of Hardware SIL for Fire Detection System

Sung Kyu Kim
Department of Industrial and Management Engineering,
Kyonggi University Graduate School, Gyeonggi 16227, Republic of Korea.

Yong Soo Kim*
Department of Industrial and Management Engineering,
Kyonggi University, Gyeonggi 16227, Republic of Korea.

Abstract
Safety integrity is a core concept at the standards to indicate credibility and reliability levels of safety-related functions. It is measured based on that the function being able to perform when demanded. Several requirements in the IEC 61508 should be satisfied to evaluate hardware SIL of safety related system. Especially, probability measures and architectural constraints should be achieved at the same time to meet target SIL. This study presented evaluation procedure for the hardware SIL and performed the case study about evaluating the hardware SIL of the fire detection system. Consequently, the PFD and the architectural constraints of all safety functions were calculated and decided. The final outcomes which achieved SIL 2 were drawn.

Keywords: Hardware Safety integrity level, Safety related System, Fire Detection System, Safety function.

INTRODUCTION

Functional safety is a concept to prevent and control risks which cause accidents by systematic dangerous failures for product life cycle. Since functional safety standards was established, IEC 61508 [1] have been a general standard as that presents concepts, requirements, and approaches for functional safety of electrical/electronic/programmable electronic safety related systems.
Safety integrity is a core concept at the standards to indicate credibility and reliability levels of safety-related functions. It is measured based on that the function being able to perform when demanded. In addition, safety integrity is divided to three categories which are hardware, software, and systematic safety integrity. Hardware safety integrity among the categories deal with the random hardware failure in a dangerous mode of failure.

Safety integrity levels (SILs) are defined to four grades (between 1 and 4). The highest level of SILs is SIL 4, and it should be qualified to meet all requirements [1, 2].
Thus, this paper describes evaluation procedure of hardware SIL and performs a case study for a safety related system. Particularly, the case study is to demonstrate that a fire detection system (FDS) is capable of achieving target SIL in terms of hardware safety integrity.

EVALUATION PROCEDURE

Probability criteria for hardware SIL
Several requirements in the IEC 61508 should be satisfied to evaluate hardware SIL of safety related system. Especially, probability measures and architectural constraints should be achieved at the same time to meet target SIL. Figure 1 shows two measures on probability and architecture of safety system (and/or function) and required values during SIL evaluation analysis.

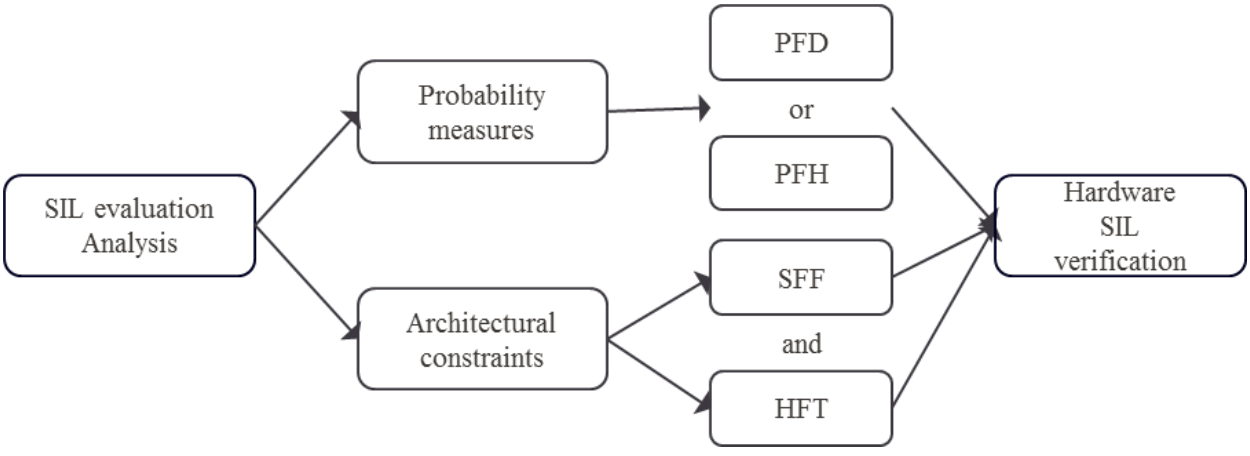

Figure 1: An analysis process for hardware SIL verification

In this paragraph, probability measures and criteria to evaluate hardware SIL were described based on IEC 61508 standards. The probability measures are classified to probability of failure on demand (PFD) or probability (or frequency) of failure per hour (PFH) by frequency of demands. The PFD is applied for low demand operation mode in case of the frequency of demands less than once per year. On the other hand, the PFH is adopted to calculate the probability measure for hardware SIL evaluation [1].

In this paper, the PFD and PFH formulations are presented for a case that system architecture consists of single-channel as follows.

$$PFD = \sum \lambda_{DU} \left(\frac{T_P}{2} + MRT \right) + \sum \lambda_{DD} \cdot MTTR \quad (1)$$

$$PFH = \sum \lambda_{DU} \quad (2)$$

where λ_{DD} is the dangerous detected failure rate, λ_{DU} is the dangerous undetected failure rate, T_P is the proof-test interval time (hours), *MRT* is the mean repair time (hours), and *MTTR* is the mean time to restoration (hours) [1].

The SIL in term of probability measures is decided by calculated PFD or PFH value of target safety related system. *MRT* and/or *MTTR* can be assumed by 8 hours, if their values cannot be procured. Table 1 shows criteria of SIL based on the PFD and PFH.

Table 1: Definitions of the safety integrity levels based on operating mode of safety related system [1].

SIL	Probability measure	
	PFD	PFH
SIL 4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
SIL 3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
SIL 2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
SIL 1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

Architectural constraints for hardware SIL

Architectural constraints are a one of measures to evaluate the hardware SIL with above probability measures. In IEC 61508, the Architectural constraints are decided by values of safe failure fraction (SFF) and hardware fault tolerance (HFT). In addition, the Architectural constraints of each safety function (or subsystem) are determined for the SIL of target safety system.

First, SFF means a ratio of total failure rates to the failure rates without dangerous undetected failure rates. It is formulated as below [1, 3].

$$SFF = 1 - \frac{\sum \lambda_{DU}}{\sum \lambda_T} \quad (3)$$

where, λ_T is the total failure rate.

A level of hardware redundancy which how many failures the system (or subsystem) can tolerate, is required for determination of HFT. Thus, $HFT = n$ is that the system and safety function should continue to work normally until occurrence of $n+1$ and more failures. In addition, component type is determined to `A` or `B` based on IEC 61508. To classify type A, expected risks as well as all failure modes and effects of components are well defined. And if not, component type is determined as `B` [1, 2]. Thus, the Architectural constraints are evaluated as follows (See Table 2).

Table 2: The architectural constraints by safe failure fraction and hardware fault tolerance [1].

SFF	HFT					
	Type A			Type B		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	-	SIL 1	SIL 2
60 to < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 to < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 4	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

An approach to evaluate hardware SIL

According to the IEC 61508, several failure rates which are divided by safe mode (safety or dangerous failure) and detectability (detected or undetected failure) are required to evaluate hardware SIL. Thus, failure rates should be classified into safe detected failure rate (λ_{SD}), safe undetected failure rate (λ_{SU}), dangerous detected failure rate, and dangerous undetected failure rate to calculate the formulations mentioned-above.

A failure modes, effects, and diagnostic analysis (FMEDA) is that failure modes and effects analysis (FMEA) is extended. In addition, it also deals with all possible failure modes of components are listed and drawn with respect to their effects on the safety functions of the system. Studies that the FMEDA was applied have performed as one of the useful approaches when failure rates are separated [4-6].

The FMEDA sheet consists of several columns that include the component ID, type of component, quantity of component, failure mode, failure distribution, failure effect (local and final), safe mode (SM), detectability (DE), diagnostic coverage (DC), diagnostic method (DM), and the four failure rates. Each step of analysis process is summarized to fill in the blanks of the sheet (See Table 3).

Table 3: The FMEDA analysis process and activity for each step

Step	Activity
1	Involved examining the parts list, bill of materials, and schematic drawing of target system, and creating a block diagram that matched the system functions to modules and components.

2 The failure rate was assigned based on failure rate data books such as MIL-HDBK-217, Telcordia SR-332 [7], and the specification of each component.

3 Assigned the failure mechanism distribution based on failure mechanism and distribution data book such as the Reliability Information Analysis Center (RIAC) FMD-2013 [8], defined as the ratio of the probability of each failure mode to the total failure probability.

4 Failure effects were identified separately for local and final effects (via interviews and workshops between engineers and experts)

5 Determined the SM and DE by either referencing IEC-61508 or engineering judgment. Each failure mode was classified as either 'Safe' or 'Dangerous'. Further, the failure mode can be either 'Detected' or 'Undetected'. In case the failure mode is detectable, the DM should be specified.

6 The DC was determined by reviewing the installed fault detection methods and attempting to match them to those in the IEC-61508.

A CASE STUDY: FIRE DETECTION SYSTEM

The FDS of this case study is a safety related system in maritime industry to prevent accident risks such as fire and a gas leak that cause huge losses of both life and property. It consists of main and sub-panels, detectors, loops, and interface subsystems and performs consistent detection functions (See Figure 2).

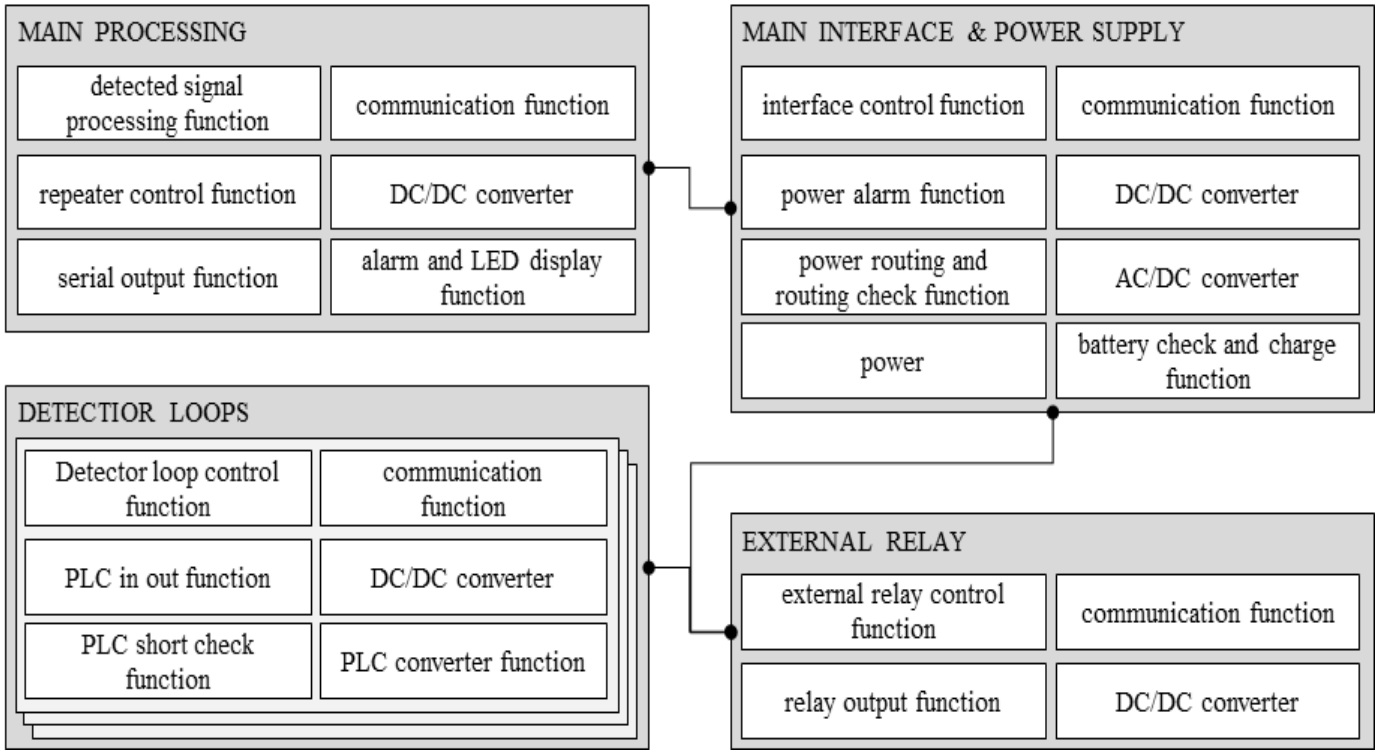

Figure 2: Functional block diagram of the FDS

For evaluating hardware SIL of the FDS, safety-related functions are classified after all of functions were defined by interviewing related engineers and experts. Thus, four safety functions were selected among all basic functions of the system (Step 1). In addition, all components of each defined function were listed and then, generic failure rates (λ_G), modes and distribution were allocated to suitable components (Step 2 and 3). In Step 4, we drawn local and final failure effects of each failure mode by interviewing development engineers. Table 4 shows a part of the FMEDA sheet which was filled through the analysis process.

Table 4: A part of the FMEDA sheet of the FDS by the step 1-4 [7, 8]

Subsystem/ Module	component	Failure Mode	Failure Distribution	Qty.	λ_G (FIT)	Local Effect	Final effect
Main Processing Function	Capacitor	Drift	65.55	6	0.10	No effect on signal processing function	No effect on fire detecting function
		Shorted	28.17			No signal processing	System down
		Opened	6.28			No effect on signal processing function	No effect on fire detecting function
	Capacitor	Drift	65.55	1	0.10	Signal processing error	loss of detecting function of fire
		Shorted	28.17			No signal processing	System down
		Opened	6.28			No signal processing	System down
	Capacitor	Drift	65.55	2	0.10	Occurrence of firmware error	Occurrence of wrong signal
		Shorted	28.17			Occurrence of firmware error	Occurrence of wrong signal
		Opened	6.28			Occurrence of firmware error	Occurrence of wrong signal

In this study, Telcordia SR-332 as failure rate data book was applied to allocate failure rate for each component. The following assumptions have been made in this study, during allocation of failure rates.

i. Failure rates are constant (failure distribution of all components is assumed as exponential distribution), wear-out and early (or initial) failure mechanisms are not included
ii. Failure rates of non-safety related subsystems and/or functions are not included;
iii. Failure rate of each component is applied as steady-state failure rate, it is calculated by black box technique (BBT) of Telcordia SR-332 issue 3.
iv. Quality factor and environment factor of BBT are respectively designate 1.0 and 1.5.
v. Failure in time (FIT) that 1 FIT equals one failure per 10^9 hours is used as unit of failure rate.

$$\lambda_{SS} = \lambda_G \pi_S \pi_T \pi_Q \pi_E \quad (4)$$

where, λ_{SS} is steady-state failure rate, λ_G is mean generic steady-state failure rate for component, π_S is electrical stress factor (1.0 at 50 % electrical stress), π_T is Temperature factor (1.0 at 40 ℃), π_Q is quality factor, π_E is environment factor [7].

All generic failure rates of components were adjusted by the BBT. To do this, we measured temperature and electrical stresses such as applied DC voltage, contact current, etc. based on the Telcordia SR-332. In addition, SM, DE, DM, and DC the detection methods and diagnostic coverages were defined to the four failure rate categories. Table 5 and 6 show a part of results of step 5-6 and defined failure detection methods, respectively.

Table 5: A part of the FMEDA sheet of the FDS by the step 5-6

Subsystem/ Module	component	Final effect	SM	DE	DC	DM	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Main Processing Function	Capacitor	No effect on fire detecting function	1	0			0.00	0.10	0.00	0.00
		System down	0	0			0.00	0.00	0.00	0.04
		No effect on fire detecting function	1	0			0.00	0.01	0.00	0.00
	Capacitor	loss of detecting function of fire	0	1	99	DM-02	0.00	0.00	0.01	0.00

	System down	0	0			0.00	0.00	0.00	0.01
	System down	0	0			0.00	0.00	0.00	0.00
Capacitor	Occurrence of wrong signal	0	1	99	DM-01	0.00	0.00	0.03	0.00
	Occurrence of wrong signal	0	1	99	DM-01	0.00	0.00	0.01	0.00
	Occurrence of wrong signal	0	1	99	DM-01	0.00	0.00	0.00	0.00

Table 6: A part of defined failure detection methods for the case study

ID	DC (%)	Description	DM in IEC-61508
DM-01	99	Possible to monitor the fire and gas signal from the display	Monitoring
DM-02	99	Fire alarm is output to Sound and Light	Multi-channel parallel output
DM-03	60	Possible to see the LED status with the naked eye	Analog signal monitoring

As the HFT is '0' and all the type of each function is classified as 'B' according to the IEC 61508, the architectural constraints of each safety function of the FDS is determined as in Table 2. In addition, the architectural constraints of the FDS were decided by that minimum level among the architectural constraints of all functions was adopted depending on merging rule in IEC 61508. Table 7 shows the calculated SFF and the architectural constraints of the FDS and each safety function. In Table 8, the PFD from the evaluation procedure for the target safety system were calculated based on several proof test intervals. Furthermore, the MRT and MTTR were assumed by 8 hours. Therefore, the final SIL of the FDS was determined as SIL 2 by the PFD and the architectural constraints.

Table 7: Determination of the architectural constraints of the FDS and each safety function

System/Function	Total failure rate (FIT)	SFF	Architectural constraints
Fire detection system	5289.79	95.82	SIL 2
Main processing function	1973.65	90.89	SIL 2
Main interface and power supply function	507.17	97.09	SIL 2
Detector loop function	2728.40	99.05	SIL 3
External relay function	80.56	99.55	SIL 3

Table 8: Calculation of the PFD based on proof test intervals

PFD	Proof test interval (T_P)	Determination of SIL by probability measure
1.11×10^{-4}	One month (730 h)	SIL 3
5.14×10^{-4}	Six month (4380 h)	SIL 3
9.98×10^{-4}	One year (8760 h)	SIL 3
1.97×10^{-3}	Two years (17520 h)	SIL 2
9.71×10^{-3}	Ten years (87600 h)	SIL 2

CONCLUSIONS

This study presented evaluation procedure for the hardware SIL and performed the case study about evaluating the hardware SIL of the FDS. In addition, several measures for the hardware SIL were effectively drawn using the FMEDA. All failure modes and effects of all included components should be examined from filling the FMEDA sheet. In addition, failure rates were adjusted based on operation environment such as operating temperature and electrical stress to be close to the realistic analysis.

Consequently, the PFD and the architectural constraints of all safety functions were calculated and decided. The final outcomes which achieved SIL 2 were drawn. We are expecting that this study will be usefully applied for evaluating and verifying the hardware SIL of safety related systems.

ACKNOWLEDGEMENT

This work was supported by Kyonggi University`s Graduate Research Assistantship 2017.

REFERENCES

[1] Functional safety of electrical/electronic/programmable electronic safety-related systems; IEC 61508; IEC: Geneva, Switzerland, April 2010.

[2] Kosmowski, K. T., 2005, "Functional safety concept for hazardous systems and new challenges", *Journal of Loss Prevention in the Process Industries*, 19(2-3), pp.298-305.

[3] Yoshimura, I., and Sato, Y., 2008, "Safety achieved by the safe failure fraction (SFF) in IEC 61508", *IEEE Transactions on Reliability*, 57, pp.662-669.

[4] Goble, W. M., and Brombacher, A. C., 1999, "Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems", *Reliability Engineering and System Safety*, 66, pp.145-148.

[5] Catelani, M., Ciani, L., and Luongo, V., 2010, "The FMEDA approach to improve the safety assessment according to the IEC61508", *Microelectronics Reliability*, 50, pp.1230-1235.

[6] Kim, S. K., and Kim, Y. S., 2013, "An evaluation approach using a HARA & FMEDA for the hardware SIL", *Journal of Loss Prevention in the Process Industries*, 26, pp.1212-1220.

[7] Reliability prediction procedure for electronic equipment; Telcordia SR-332 Issue 3; Telcordia Technologies, Inc.: New Jersey, USA, 2011.

[8] Failure mode/ mechanism distributions; FMD-2013; Reliability Information Analysis Center (RIAC): New York, USA, 2013.