An Optimal Design Procedure based on the Safety Integrity Level for Safety-related Systems

Sung Kyu Kim[1] and Yong Soo Kim[2*]
[1] Department of Industrial and Management Engineering, Kyonggi University Graduate School, Suwon, Republic of Korea
[e-mail: kimsk@kgu.ac.kr]
[2] Department of Industrial and Management Engineering, Kyonggi University, Suwon, Republic of Korea
[e-mail: kimys@kgu.ac.kr]
*Corresponding author: Yong Soo Kim

Received March 24, 2018; revised May 13, 2018; accepted June 10, 2018; published December 31, 2018

Abstract

Safety-related systems (SRSs) has widely used in shipbuilding and power generation to prevent fatal accidents and to protect life and property. Thus, SRS performance is a high priority. The safety integrity level (SIL) is the relative performance level of an SRS with regard to its ability to operate reliably in a safe manner. In this article, we proposed an optimal design procedure to achieve the targeted SIL of SRSs. In addition, a more efficient failure mode and effects diagnostic analysis (FMEDA) process and optimization model were developed to improve cost efficiency. Based on previous IEC 61508 diagnostic analyses that revealed unnecessary costs associated with excessive reliability, the new approach consists of two phases: (i) SIL evaluation by FMEDA, and (ii) solution optimization for achieving the target SIL with minimal cost using integer-programming models. The proposed procedure meets the required safety level and minimizes system costs. A case study involving a gas-detection SRS was conducted to demonstrate the effectiveness of the new procedure.

Keywords: Safety-related system, safety integrity level, gas detector, FMEDA, integer programming

1. Introduction

Industrial facilities, such as those associated with shipbuilding or power generation, require high-level safety protocols to prevent injuries to workers or those in surrounding communities, as well as to prevent or minimize damage to the facility. Accordingly, many safety-related systems (SRSs), involving electrical/electronic technologies, have been installed at these sites to perform safety diagnostics.

The safety integrity level (SIL) was established to ensure the stability and reliability of Safety Requirements Specifications (SRS) based on the requirements, criteria, and formulations of international standards, such as IEC 61508 [1]. According to the standard, the applicable SRS safety grade is assigned to one of four SILs. In addition, hardware and software must be verified individually to determine the SIL of an SRS.

Thus, several methodologies were developed to improve the accuracy and efficiency of SIL verification, and an optimal reliability design procedure was presented to achieve the required hardware SIL. This procedure consists of an SIL evaluation process and an optimal design model, and is described below.

In this study, we proposed an optimal reliability design procedure for achieving the hardware SIL and minimizing system cost using integer programming. For this, we modified the evaluation process [2] of the hardware SIL using failure modes effects and diagnostic analysis (FMEDA). First, adjusted failure rates are considered based on factors that influence the condition of components to determine practical failure rates; then, the analytical process is revised via comparison with the previous process.

We also developed two optimal design models to minimize cost using integer programming. These models address two key issues presented by commonly used testing procedures. The first issue occurs when the evaluated SIL of a SRS is less than the target SIL. In this case, the SRS cannot achieve the required SIL without replacement of conventional parts with other parts that have higher reliability. Additionally, the target SIL can be achieved by adding a novel fault checking module to some subsystem of the SRS since the failure detection rate can be improved. The second issue arises when the evaluated SIL is greater than the target SIL. In this case, the unit cost of production may be higher than necessary.

Finally, we conducted a case study of a gas detection system to demonstrate the effectiveness of the proposed optimal reliability design procedure. This case study was selected because sensors play a key role in SRS for signal scanning and gas detection and are usually equipped with various logic solvers and actuators. As a result, our approach achieved the target SIL for the gas sensor at minimal cost.

2. Related Works

For the evaluation of hardware SIL, the required failure rates are divided into the following categories: safe-detected, safe-undetected, dangerous-detected, and dangerous-undetected. FMEDA is highly useful when four failure rates are defined. Goble and Brombacher [3] described a procedure to calculate the diagnostic coverage (DC) based on FMEDA results. Catelani et al. [4] performed a case study for a safety assessment of a complex system using FMEDA and compared the approach to that outlined by IEC 61508 standards. Additionally,

Kim and Kim [2] proposed an FMEDA process to evaluate the hardware SIL and performed a case study on a flame scanner system.

Generally, the evaluation of hardware SILs is specified in IEC 61508 to determine the architectural constraints (AC) and the probability of failure [1]; several measurements are used to resolve these criteria. The safe failure fraction (SFF), which is one of the criteria used for evaluating the SIL, has been studied with respect to its positive effects on the hazardous event rate [5]. A Markov model with common cause failures was applied to calculate probability of failure on demand (PFD) for determination of SIL [6]. Several studies have compared common calculation methods and the reliability block diagram (RBD) to assess the PFD [7]. Ding et al. [8] developed an SIL verification approach using the RBD based on system redundancy and degradation. Hu et al. [9] proposed a reliability prediction model based on the evidential reasoning algorithm and used the model in a case study of turbocharged engine systems. Human factors during machine operation were accounted for qualitatively and quantitatively to verify the SIL of the SRS using quantitative risk analysis (QRA) and integrated dynamic decision analysis (IDDA) in [10]. In term of the risk analysis, Piesik et al. [11] proposed extending the risk graph approach by the frequency of accident scenarios, as well as existing resk gragh of IEC 61508, to evaluate required SIL grade.

A variety of reliability prediction models, such as the MIL-HDBK-217, Telcordia SR-332, IEEE STD 1413, EPRD, and NPRD95 standards, have been established and revised by several international organizations and companies. These models have been widely used to estimate the reliability of a system and its components. In addition, these methods assume that the times to failure of the parts follow an exponential distribution. Telcordia SR-332 [12] is applied by many commercial electronics manufacturers; it provides generic failure rates for components with standard adjustment factors for generic parts, with factors for quality and temperature, environmental, and electrical stresses.

Goel and Graves [13] collected and analyzed several reliability prediction models for electronic systems and evaluated the models by calculating the system failure rates. Cassanelli et al. [14] proposed a novel reliability prediction methodology to minimize the problems of traditional methods, using different approaches to assess the reliability of the electronics during the design phase. Brissaud et al. [15] developed an evaluation method for failure rates with influencing factors; e.g., temperature, pressure, fluid, and material properties, for the processing industry.

System reliability predictions and component allocation are important issues for achieving target reliability levels and assembling units. Many studies have examined these safety-related issues and proposed solutions using optimization and heuristic methods. Jang and Kim [16] considered a redundancy allocation problem (RAP) in series-parallel to select optimal redundancy solution for components and modules of a system by tabu search. Gheraibia et al. [17] solved an automotive SIL allocation problem by applying an ant colony algorithm to maximize safety requirements and minimize costs. Yildiz [18] presented a comparative study of state-of-the-art optimization techniques, such as the hybrid technique, for solving multi-pass turning operation problems. Torres-Echeverría et al. [19] described the design optimization of SRSs using a multi-objective genetic algorithm based on RAMS+C measures. Torres-Echeverría et al. [20, 21] also presented a new approximation method for time-dependent probability to optimize proof-testing policies by genetic algorithms, and proposed the optimization of design and test policies for SRSs using several redundancies through the use of a multi-objective genetic algorithm. Marseguerra et al. [22] proposed a multiple-objective optimization approach by combining genetic algorithms and Monte Carlo simulations for network system design optimization. Amari et al. [23] described the optimal

design of a k-out-of-n structure, based on subsystems subjected to imperfect fault coverage. Safari [24] developed a methodology to solve a novel mathematical model for multi-objective RAP using a variant of the non-dominated sorting genetic algorithm (NSGA-II). Sharifi et al. [25] also considered a RAP based on k-out-of-n system structural using heuristic algorithms. Bakkiyaraj and Kumarappan [26] developed an optimal reliability-planning algorithm using particle swarm optimization in a composite electric power system. In addition, Elegbede et al. [27] solved optimal RAPs through cost minimization in parallel-series systems.

3. Development of an Optimal Reliability Design Procedure

3.1 Evaluation of Hardware SIL using FMEDA

3.1.1 FMEDA Process for SIL Evaluation

In the IEC 61508 standards, several measures to evaluate hardware SIL are described. These measures consist of hardware construct and probability failure of each subsystem and/or system, which can be classified into four categories according to the safe mode and detectability, described earlier.

FMEDA, introduced by Kim and Kim [2], is a recommendation method for system analysis based on each failure mode of the system's components. This method defines the failure distribution, failure effect, safe mode, detectability, detection method, and diagnostic coverage (DC), as well as the failure rate of the components. Thus, it draws on numerous measures for hardware SIL evaluation.

In this study, we modified the sequence and activity of the original FMEDA process to improve hardware SIL evaluation. In the proposed method, the failure rates of each component were adjusted, based on the quality factors and usage environmental factors of the system, such as the temperature and electrical stress. The steps of the modified FMEDA process are given below [2, 3].

- Step 1: Define the subsystems as safety- or non-safety-related, using a functional block diagram (FBD). In addition, all components of the system should be assigned to suitable subsystems, based on the bill of materials (BOM) and schematic diagrams.
- Step 2: Determine the failure rate of each component using field failure data and/or reliability data handbooks. Where field failure data are unavailable, the failure rate should be defined based on reliability data handbooks (preferably using a single handbook for consistency). Additionally, the adjustment methods described in the handbooks should be applied to more accurately predict the failure rate of components [12].
- Step 3: Determine the failure modes and distributions of each component using field failure data and/or related literature, which may include RIAC FMD-2013 [28] and IEC 62061 standards, for example.
- Step 4: Define the failure effects of each assigned failure mode by interviewing engineers regarding the effects of the failure modes on system or subsystem failure.
- Step 5: Classify each failure mode as safe or dangerous, based on its failure effects and definitions of both failures in the IEC 61508 standards. According to these standards, if the occurrence of any failure reveals that the safety function did not function properly when required, then it is categorized as a dangerous failure; otherwise, the failure is classified as a safe failure [1].

- Step 6: Specify the component failure modes and the detection methods for the component failure/safe modes. The failure rate of each category is based mainly on the detectability. Detectability is divided into detected failure and undetected failure. If any failure mode of the components can be detected, then its detection method must be specified. If a fraction of the dangerous failure is detected (i.e., DC), then this should also be defined using the IEC 61508 standards and component specification [1].
- Step 7: Assign the failure rates for the hardware SIL to one of the four categories: safe-detected, safe-undetected, dangerous-detected, and dangerous-undetected, based on the failure rate, failure distribution, safety mode, detectability, and the DC. The hardware SIL of the system is then evaluated by the probability and architectural measurements, given the failure rate and hardware construct.
- Step 8: If the target SIL is not achieved, then the system and/or individual subsystem design must be improved by replacing the components in question and/or by changing the system design.

3.1.2 Hardware SIL Criteria based on IEC 61508 Standards

In this section, we describe the criteria used to decide the hardware SIL, based on IEC 61508 standards. Probability and architectural measurements are required to evaluate hardware SIL. The probability measurements are classified into the PFD and frequency of dangerous failures per hour (PFH), according to the operational demand frequency. The PFH are used in a same sense as probability of failure per hour at several literatures. If the operational demand frequency is no greater than once per year and no greater than twice the proof-test frequency, then the component operates in a low-demand mode. A high-demand/continuous mode has a greater demand frequency than a low-demand mode [1].

The PFD and PFH for single-channel (1oo1) architecture can be expressed as

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

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

$$PFH_{1oo1} = \sum \lambda_{DU} \tag{3}$$

where λ_{DD} is the dangerous detected failure rate, λ_{DU} is the dangerous undetected failure rate, λ_D is the dangerous failure rate or the sum of λ_{DD} and λ_{DU}, t_{CE} is the channel equivalent mean downtime (hours), T_1 is the proof-test interval, MRT is the mean repair time, and $MTTR$ is the mean time to restoration [1]. In $\lambda_D = \lambda_{DD} + \lambda_{DU}$, Eq. (1) can be rewritten as

$$PFD_{1oo1} = \sum \lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + \sum \lambda_{DD} MTTR \cdot$$

Table 1 shows the evaluation of the hardware SIL by probability measurement.

Table 1. Evaluation of the hardware safety integrity levels (SILs) by probability of failure in each demand mode [1]

Safety integrity level	Demand of operation	
	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 $<10^{-5}$

The architectural measurement refers to the AC or maximum allowable SILs in the system structure. The AC is determined by the SFF and the hardware fault tolerance (HFT). The SFF is calculated by taking the safe failure rate and the dangerous detected failure rated divided by the total failure rate for each subsystem as follows

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \tag{4}$$

where, λ_S is the safe failure rate [1].

The HFT is based on hardware redundancy and an understanding of the components and subsystems. Hardware redundancy which is 'HFT n' refers to the minimum number of failures that can be permitted without system failure and/or malfunction of the safety function. Additionally, the component type is defined as 'Type A' or 'Type B' to indicate the AC. If the failure modes and effects of a component are well defined, this component is regarded as 'Type A'; otherwise, the component is classified as 'Type B'. In addition, if just one component in a subsystem is defined as 'Type B', then the entire subsystem is classified as 'Type B'; otherwise, the subsystem is classified as 'Type A'. **Table 2** shows the determination of the AC or maximum allowable SIL, given the SFF and HFT [1].

All of the formulations quoted above are specified in IEC 61508 and most are recommended. Therefore, we used these formulations and criteria to evaluate hardware SIL and to establish optimal models.

Table 2. Determination of architectural constraints (ACs) based on the safe failure fraction (SFF) and hardware fault tolerance (HFT) [1]

Safe failure fraction (SFF)	Hardware fault tolerance (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

3.2 Optimization for Achieving the Target SIL based on Minimum Cost

3.2.1 Problems during the Hardware SIL Evaluation for Developed SRSs

SRSs are based on various requirements related to design, production, maintenance, repair, and disposal. SRS development can be difficult. In an attempt to effectively manage SRSs, the

IEC developed guidelines (the IEC 61508 standards) that describe the safety lifecycle of a system, from the concept phase to the production phase. However, SRSs already in operation have limited safety lifecycle requirements, due to the difficulty associated with changing the existing system design [1, 2].

For verification of the hardware SIL, first, the safety requirements of the SRS should be identified via hazard analysis and risk assessment. In this study, the target SIL for the SRS considered was defined based on the requirements cited to prevent hazardous events and system malfunction. As such, the SRS should be designed and developed with a target SIL in mind, based on the hardware structure and probability failure of the system. With system safety and reliability at the forefront of functional safety protocol, the system design considerations should also include the total cost incurred by the system components and modules for safe, reliable, and efficient operation.

Given these considerations, the developed SRS meets one of three outcomes, described in terms of the hardware SIL and the total cost of the system design (see **Fig. 1**). For Case 1, the evaluated SIL does not meet the target SIL, and the design or components must be changed. For Case 2, the target SIL is met with a cost that is less than the default design. Case 2 is optimal, due to its lower cost. For Case 3, the default design greatly exceeds the target SIL, resulting in unnecessary additional cost. Changing the components has a direct effect on the actual SIL, due to the costs involved in making the change and the difference in the failure rate of the replaced parts (i.e., higher quality components have lower failure rates). In summary, we wish to avoid designs corresponding to Cases 1 or 3. The optimal solution satisfies the target SIL using a minimum cost design.

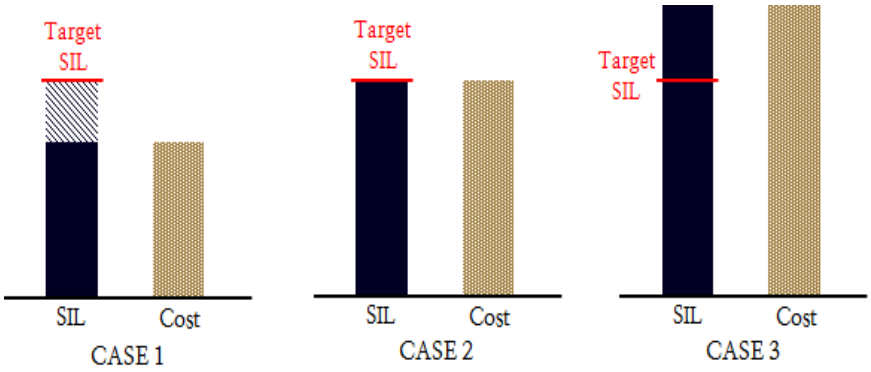

Fig. 1. Three cases representing the trade-off between hardware safety integrity level (SIL) and total cost

3.2.2 Optimization Models for Achieving the Target SIL at Minimal Cost by Integer Programming

As one of several optimization methods in operations research, integer programming is applied to solve problems in which the decision variables are represented as integers. This paper examined a problem that optimizes the design of SRS to achieve the target SIL at minimum cost, based on selecting components and adding diagnostic coverage modules. Integer programming is the most suitable method for this because the number of components that are decision variables is an integer.

Here, we developed optimization models to minimize the cost to achieve a target SIL using integer programming. Optimization Model I focused on component replacement to meet the

SIL. The other model (optimization Model II) considered component replacement (Model I) as well as additional fault checking modules to satisfy SIL requirements. These models assumed the following: (i) the structural design of the SRS did not change; (ii) the total number of components chosen was equal to or greater than the default quantity in the same category; (iii) DC by additional detection methods refers to all subsystem components of the installed fault checking module; and (iv) the entire system had a 1oo1 structure.

Optimization Model I consists of decision variable and 14 constants (see **Table 3**). The objective function, Eq (5), of this model was to minimize the total component cost. According to hardware SIL criteria, the constraints are given in Eqs. (6), (7), and (10). Eq. (6) or (10) can be used depending on the safety function demand. Eq. (6) should be selected if the system is evaluated by PFD; otherwise, Eq. (10) should be included in the model without Eq. (6). Eq. (7) determines the SFF of each subsystem, as defined by Eq. (4). Eq. (8) ensures the jth component quantity of the default design in the same subsystem. Additionally, Eq. (9) defines the integer constraint and the non-negative constraint of the decision variable.

Table 3. Parameters used in the optimization Model I

Parameter	Notation	Description
Variable	x_{ijk}	Quantity rate for *k* category of *j*th component on *i*th subsystem.
Constant	c_{ijk}	Cost for *k* category of *j*th component on *i*th subsystem.
	$\lambda_{DU_{ijk}}$	Undetected dangerous failure rate for *k* category of *j*th component on *i*th subsystem.
	$\lambda_{DD_{ijk}}$	Detected dangerous failure rate for *k* category of *j*th component on *i*th subsystem.
	$\lambda_{S_{ijk}}$	Safe failure rate for *k* category of *j*th component on *i*th subsystem.
	T_1	Proof test interval (hour).
	MRT	Mean repair time (hour).
	$MTTR$	Mean time to restoration (hour).
	PFD_{Target}	Criterion of the PFD based on the target SIL in 1oo1 system.
	PFH_{Target}	Criterion of the PFH based on the target SIL in 1oo1 system.
	SFF	Criterion of the SFF based on the target SIL.
	q_{ij}	Default quantity for the *j*th component on *i*th subsystem
	n	A number of subsystems.
	m	Maximum number of component type (*j*) among all subsystems
	l	A number of alternative components.

$$\text{Minimize} \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} c_{ijk}\, x_{ijk} \tag{5}$$

$$\text{Subject to} \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} \lambda_{DU_{ijk}}\, x_{ijk}\left(\frac{T_1}{2}+MRT\right)+\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} \lambda_{DD_{ijk}}\, x_{ijk}\, MTTR \le PFD_{Target} \tag{6}$$

$$\left(1-\frac{\sum_{j=1}^{m}\sum_{k=1}^{l}\lambda_{DU_{ijk}}x_{ijk}}{\sum_{j=1}^{m}\sum_{k=1}^{l}\lambda_{S_{ijk}}x_{ijk}+\sum_{j=1}^{m}\sum_{k=1}^{l}\lambda_{DD_{ijk}}x_{ijk}+\sum_{j=1}^{m}\sum_{k=1}^{l}\lambda_{DU_{ijk}}x_{ijk}}\right)\geq SFF \tag{7}$$

$$\sum_{k=1}^{l}x_{ijk}\geq q_{ij},\forall i,j \tag{8}$$

$$x_{ijk}\geq 0,\ \text{integer},\forall i,j,k \tag{9}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l}\lambda_{DU_{ijk}}x_{ijk}\leq PFH_{Target} \tag{10}$$

Optimization Model II was formulated to consider additional fault checking modules, as well as changing components. Unlike the previous model, the decision variables y_{ijk}, y'_{ijk}, and z_i were added to reflect additional fault checking modules and function linearity. y_{ijk} corresponds to the system components having a DC less than the DC of the additional fault checking modules. Thus, the components that do not have to consider additional DCs are included in x_{ijk}. y'_{ijk} is added to realize a linear model. z_i accounts for whether or not an additional fault checking modules for the ith subsystem is installed or not. In total, optimization Model II includes 23 constants (see **Table 4**).

Table 4. Parameters used in the optimization Model II

Parameter	Notation	Description
Variable	x_{ijk}	Quantity rate for *k* category of *j*th component on *i*th subsystem for non-considering additional DC.
	y_{ijk}	Quantity rate for *k* category of *j*th component on *i*th subsystem for considering additional DC.
	y'_{ijk}	y_{ijk} `s dummy variable for linearity of model.
	z_i	1 if the additional fault checking modules is installed in the *i*th subsystem, and 0 otherwise.
Constant	c^x_{ijk}	Cost for *k* category of *j*th component on *i*th subsystem for *x*.
	c^y_{ijk}	Cost for *k* category of *j*th component on *i*th subsystem for *y*.
	c^{dm}	Cost of additional fault checking modules.
	λ_{DU_i}	Total undetected dangerous failure rate for *i*th subsystem.
	λ_{DD_i}	Total detected dangerous failure rate for *i*th subsystem.
	$\lambda^x_{DU_{ijk}}$	Undetected dangerous failure rate for *k* category of *j*th component on *i*th subsystem for *x*.
	$\lambda^x_{DD_{ijk}}$	Detected dangerous failure rate for *k* category of *j*th component on *i*th subsystem for *x*.
	$\lambda^x_{S_{ijk}}$	Safe failure rate for *k* category of *j*th component on *i*th subsystem for *x*.
	$\lambda^y_{D_{ijk}}$	Dangerous failure rate for *k* category of *j*th component on *i*th subsystem for *y*.

dc_{ij}	Default diagnostic coverage of *j*th component on *i*th subsystem for *y*.
dc_a	Diagnostic coverage by additional fault checking modules.
T_1	Proof test interval (hour).
MRT	Mean repair time (hour).
MTTR	Mean time to restoration (hour).
PFD_{Target}	Criterion of the PFD based on the target SIL in 1oo1 system.
PFH_{Target}	Criterion of the PFH based on the target SIL in 1oo1 system.
SFF	Criterion of the SFF based on the target SIL.
q_{ij}	Default quantity for the *j*th component on *i*th subsystem.
n	A number of subsystems.
m	Maximum number of component type (*j*) among all subsystems for *x*.
m'	Maximum number of component type (*j*) among all subsystems for *y*.
l	A number of alternative components.
M	Very big constant for linearity of model

As the objective function of Model II, Eq. (11) can be used to minimize the total cost, and is defined as the sum of the total component cost and additional fault checking modules costs. Eq. (12) or (21) can be used to determine the probability; this evaluation depends on the frequency dictated by the safety function demand. Eq. (13) defines the constraints for the SFF, similar to Eq. (7). According to decision variables x_{ijk} and y_{ijk}, Eqs. (14) and (15) ensure the jth component quantity of the default design in the same subsystem for each variable. Eqs. (16–18) are inserted in the model to retain the linearity of the objective function and its constraints. Eq. (19) defines the integer constraint and the non-negative constraint of x_{ijk}, y_{ijk}, and y'_{ijk}. Finally, z_i is constricted by (20).

$$\text{Minimize } \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} c_{ijk}^{x} x_{ijk} + \sum_{i=1}^{n}\sum_{j=1}^{m'}\sum_{k=1}^{l} c_{ijk}^{y} y_{ijk} + \sum_{i=1}^{n} z_i c^{dm} \tag{11}$$

$$\text{Subject to } \sum_{i=1}^{n} \lambda_{DU_i}\left(\frac{T_1}{2} + MRT\right) + \sum_{i=1}^{n} \lambda_{DD_i} MTTR \le PFD_{Target} \tag{12}$$

where $\lambda_{DU_i} = \sum_{j=1}^{m}\sum_{k=1}^{l} \lambda_{DU_{ijk}}^{x} x_{ijk} + \sum_{j=1}^{m'}\sum_{k=1}^{l}\left[\left(1-dc_{ij}\right)\lambda_{D_{ijk}}^{y} y_{ijk} - \left(\left(1-dc_{ij}\right)-\left(1-dc_a\right)\right)\lambda_{D_{ijk}}^{y} y'_{ijk}\right]$ and

$\lambda_{DD_i} = \sum_{j=1}^{m}\sum_{k=1}^{l} \lambda_{DD_{ijk}}^{x} x_{ijk} + \sum_{j=1}^{m'}\sum_{k=1}^{l}\left[dc_{ij}\lambda_{D_{ijk}}^{y} y_{ijk} - \left(DC_{ij} - DC_a\right)\lambda_{D_{ijk}}^{y} y'_{ijk}\right]$.

$$\frac{\sum_{j=1}^{m}\sum_{k=1}^{l} \lambda_{S_{ijk}}^{x} x_{ijk} + \lambda_{DD_i}}{\sum_{j=1}^{m}\sum_{k=1}^{l} \lambda_{S_{ijk}}^{x} x_{ijk} + \lambda_{DD_i} + \lambda_{DU_i}} \ge SFF, \forall i \tag{13}$$

$$\sum_{k=1}^{l} x_{ijk} \geq q_{ij}^{x}, \forall i, j \tag{14}$$

$$\sum_{k=1}^{l} y_{ijk} \geq q_{ij}^{y}, \forall i, j \tag{15}$$

$$y'_{ijk} \leq y_{ijk} \tag{16}$$

$$y'_{ijk} \leq z_i M \tag{17}$$

$$y'_{ijk} \geq y_{ijk} + (z_i - 1)M \tag{18}$$

$$x_{ijk}, y_{ijk}, y'_{ijk} \geq 0, \text{ integer}, \forall i, j, k \tag{19}$$

$$z_i = 0 \text{ or } 1, \forall i \tag{20}$$

$$\sum_{i=1}^{n} \lambda_{DU_i} \leq PFH_{Target} \tag{21}$$

4. A Case Study for a Gas Detector

4.1 Hardware SIL Evaluation of the Gas Detector using the FMEDA Process

We have performed a case study of a gas detector using our FMEDA process. As one of the SRSs, the gas detector was installed at several industrial sites to prevent accidents by leakage of toxic gas. The detection system consisted of 10 subsystems, including a toxic gas sensor, signal processor, communicator, and power manager, as defined in Step 1 of the FMEDA process.

In this paper, Telcordia SR-332 was applied to assign component failure rates. These failure rates assume that the times to failure of the parts are exponentially distributed. We used failure in time (FIT), where the unit failure rate was defined as one failure per one billion hours. Additionally, we selected the black box technique of Telcordia SR-332 to adjust the failure rates. The black box technique reflects the temperature, electrical stress, quality, and equipment operation environment, according to Eq. (22):

$$\lambda_{SS} = \lambda_G \pi_Q \pi_S \pi_T \pi_E \tag{22}$$

where λ_{ss} is the steady-state failure rate of the component, λ_G is the generic steady-state failure rate of the component, π_Q is the quality factor of the component, π_S is the electrical stress factor of the component based on the percent electrical stress, π_T is the temperature factor of the component based on the normal operating temperature during the steady state, and π_E is an environmental factor. If the electrical stress and temperature are unknown, then π_S and π_T are set to 1, which assumes 50% electrical stress and a temperature of 40°C [12]. **Table 5** shows a part of steady-state failure rates of components for the gas detector based on Telcordia SR-332.

Table 2. A part of steady-state failure rates of components based on the adjustment factors [12]

No.	Component	π_s	π_t	π_Q	π_E	λ_G	λ_{SS}
1	Thermistor sensor	1.00	4.40	1.00	1.50	5.10	33.66
2	Chip resistor	0.52	1.50	1.00	1.50	0.08	0.09
3	Chip ceramic capacitor	0.13	1.10	1.00	1.50	0.10	0.02
4	Lead connector	1.00	4.40	1.00	1.50	11.00	72.60
5	Ferrite bead inductor	1.00	1.50	1.00	1.50	0.10	0.23
6	Chip resistor	0.52	1.50	1.00	1.50	0.08	0.09
7	Dip switch	0.52	4.40	1.00	1.50	5.86	20.22
8	Chip resistor	0.52	1.50	1.00	1.50	0.08	0.09
9	Axial resistor	0.52	1.50	1.00	1.50	0.08	0.09
10	Chip resistor	0.52	1.50	1.00	1.50	0.08	0.09
11	Chip ceramic capacitor	0.13	1.10	1.00	1.50	0.10	0.02
12	Linear IC	1.00	13.58	1.00	1.50	0.24	4.89
13	Chip FET	0.30	1.80	1.00	1.50	11.00	8.97
14	Regulator/LDO IC	1.00	13.37	1.00	1.50	0.31	6.22
15	Chip ceramic capacitor	0.16	1.10	1.00	1.50	0.10	0.03
16	Chip resistor	0.59	1.50	1.00	1.50	0.08	0.11
17	ADC/DAC IC	1.00	13.41	1.00	1.50	0.34	6.84
18	Chip ceramic capacitor	0.19	1.10	1.00	1.50	0.10	0.03
19	Chip resistor	0.52	1.50	1.00	1.50	0.08	0.09
20	Ferrite bead inductor	1.00	1.50	1.00	1.50	0.10	0.23

We also considered the failure mode and distribution for all of the gas detector's components. In this paper, RIAC FMD-2013 [28] was selected to assign the failure mode and distribution. If a component had numerous failure modes, then three high-ranked failure modes were selected. The failure distribution for the selected failure modes was scaled such that the sum of the distribution was 100% [28].

We defined the failure effects of each failure mode after determining the failure mode and distribution for each component. The safe mode and detectability were determined based on interviews with engineers, as well as the IEC 61508 standards. The detectability was assigned a '1' if a fault checking module existed for the system component. The DCs for these fault checking modules were resolved using the same techniques specified in the IEC 61508 standards. **Table 6** shows a sample of the FMEDA results for the case study [1].

Table 3. A sample FMEDA sheet for the gas detector

Sub System	Component	Failure distribution (%)	Failure mode	Failure effect	Failure rate (FIT)	SM	DE	DC	λ_{SD} (FIT)	λ_{SU} (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)
S1	THERMISTOR SENSOR	71.07	opened	wrong temperature value sensed	35.88	1	0		0	35.88	0	0
		28.93	drift	exceed the value of the temperature sensing accuracy	14.61	1	0		0	14.61	0	0
	CHIP RESISTOR	81.15	opened	wrong temperature value	0.12	1	0		0	0.12	0	0

				detected								
		13.71	high value	wrong temperature value detected	0.015	1	0		0	0.015	0	0
		5.14	shorted	wrong temperature value detected	0	1	0		0	0	0	0
	CHIP CERAMIC CAPACITOR	37.62	opened	no effect on the system	0.015	1	0		0	0.015	0	0
		62.38	shorted	wrong temperature value detected	0.015	1	0		0	0.015	0	0
S2	LEAD CONNECTOR	33.33	opened	no gas detection	36.3	0	1	99	0	0	35.94	0.36
		33.33	shorted (except power pin)	no detection of gas	36.3	0	1	99	0	0	35.94	0.36
		33.33	power pin shorted	no gas detection	36.3	0	1	99	0	0	35.94	0.36
	FERRITE BEAD INDUCTOR	59.75	opened	no gas detection	0.195	0	0		0	0	0	0.195
		40.25	Shorted	no effect on the system	0.135	1	0		0	0.135	0	0
	FERRITE BEAD INDUCTOR	59.75	opened	no gas detection	0.195	0	0		0	0	0	0.195
		40.25	shorted	no effect on the system	0.135	1	0		0	0.135	0	0
	FERRITE BEAD INDUCTOR	59.75	opened	no gas detection	0.195	0	0		0	0	0	0.195
		40.25	shorted	no effect on the system	0.135	1	0		0	0.135	0	0
	CHIP RESISTOR	81.15	opened	no reading of sensor output signal	0.12	1	1	99	0.12	0	0	0
		13.71	high value	no reading of sensor output signal	0.015	1	1	99	0.015	0	0	0
		5.14	shorted	no reading of sensor output signal	0	1	1	99	0	0	0	0
	DIP SWITCH	100.00	opened	no gas detection	30.33	0	1	99	0	0	30.015	0.3
	CHIP RESISTOR	81.15	opened	no gas detection	0.12	0	1	99	0	0	0.12	0
		13.71	high value	no gas detection	0.015	0	1	99	0	0	0.015	0
		5.14	shorted	no effect on the system	0	1	0		0	0	0	0

The probability measurement was determined as the PFD in that the operational demand frequency of the gas detector was no greater than once per year. This decision was based on the operating records of the gas detector. However, *MRT* and *MTTR* were assumed to be 8 hours, based on IEC 61508 standards.

The PFD of the gas detector was calculated according to the failure rates outlined by FMEDA and Eq. (1). The HFT and SFF were defined by the FMEDA process and Eq. (4). The HFT for all of the subsystems was assigned a '0' and 'Type B', because this detector was a single structure and used 'Type B' components. **Table 7** shows a summary of the case study, based on the proposed process.

Table 4. Summary of the calculated parameters for the gas detector and individual subsystems

System/ subsystem	SFF (%)	HFT	Architectural constraints	DC (%)	$\sum \lambda_S$ (FIT)	$\sum \lambda_D$ (FIT)	$\sum \lambda_{DD}$ (FIT)	$\sum \lambda_{DU}$ (FIT)
Gas detector	99.41	B, N=0	SIL 2	98.90	6592.45	7546.26	7463.01	83.25
S1	100.00	B, N=0	SIL 3	100.00	33.78	0.00	0.00	0.00
S2	98.34	B, N=0	SIL 2	98.21	9.88	123.63	121.42	2.21
S3	95.44	B, N=0	SIL 2	95.32	0.20	7.23	6.89	0.34
S4	99.05	B, N=0	SIL 3	99.00	93.84	1911.73	1892.58	19.15
S5	96.18	B, N=0	SIL 2	95.79	8.37	82.31	78.85	3.46
S6	99.12	B, N=0	SIL 3	98.78	3.17	7.98	7.88	0.10
S7	99.18	B, N=0	SIL 3	99.00	26.74	122.95	121.72	1.23
S8	99.95	B, N=0	SIL 3	99.00	248.59	12.86	12.74	0.13
S9	98.94	B, N=0	SIL 2	98.93	75.08	5253.89	5197.50	56.39
S10	100.00	B, N=0	SIL 3	99.00	6092.81	23.68	23.44	0.24

The PFD of the gas detector was calculated to be 4.25×10^{-4} when the proof test interval was assumed as 1 year. The AC of the system level was determined as a merging rule, based on IEC 61508 standards. The merging rule considers the AC of the subsystem level. If the system structure is serial, then the AC of the system is determined to be the minimum AC of the subsystems. Thus, the AC of the gas detector was SIL 2 (see **Fig. 2**). As a result, the hardware SIL of the gas detector was evaluated as SIL 2, based on the PFD and AC.

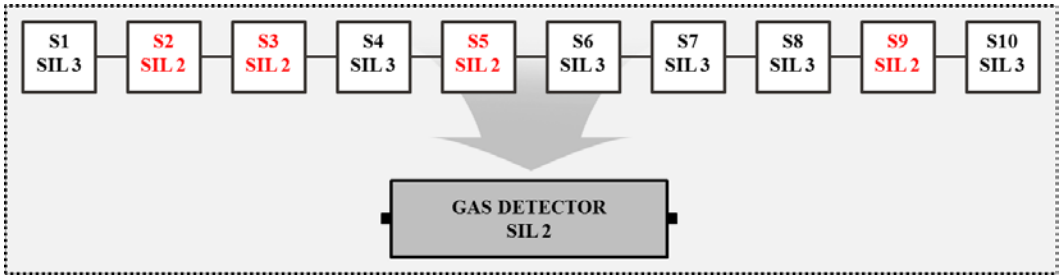

Fig. 1. Architectural constraints (ACs) of the gas detector using the merging rule

4.2 Optimal Design for the Gas Detector to Achieve the Minimum Cost and Target SIL

4.2.1 Considering Only Changing the Components of the Gas Detector

The target SIL of the gas detector in this case study was SIL 2, as determined by hazard analysis and risk assessment. Therefore, the gas detector must satisfy SIL 2 using the FMEDA process. The components were divided into 90 categories, based on their location, specifications, and functions. All categories of the components had four alternatives. The failure rates and cost of alternatives are adjusted based on the Telcordia SR-332 quality factor and assumed costs ratio (see **Table 8**). In this paper, the default failure rate and cost were

established for k = 2. The failure rates and costs of the alternatives (k = 1, 2, 4) were calculated by multiplying the default values by the quality factors and cost ratios for the same k. The cost of the default components that corresponds to quality level II was obtained from Mouser.com, an online component vendor.

Table 5. Quality factors and cost ratios used based on *k* [12]

k	Quality level	Quality factor	Cost ratio
1	III	0.8	1.5
2	II	1.0	1
3	I	3.0	0.75
4	0	6.0	0.5

Integer programming was carried out using the 'ILOG CPLEX' software package to derive the optimal solution. The difference between the PFDs obtained from the optimization Model I and the FMEDA process was due to the assumptions listed in the section above. For the default design, the calculated PFD was 4.25×10^{-4} and the total cost of the components was 250.46 US dollars ($). If the components with the lowest failure rates were chosen, then the PFD was 3.32×10^{-4} and the total cost was $375.70. Thus, the actual gas detector has a greater margin than the default design, but the cost was higher than that of a conventional gas detector. If the components with the highest failure rates were chosen, then the PFD was 2.49×10^{-3} and the total cost was $125.23 (see **Fig. 3**). However, this optimal solution can be changed by revising information on, for example, the failure rate, costs, and operating factors. In this case, expected benefit is $ 125.23 by the proposed procedure (see **Table 9**).

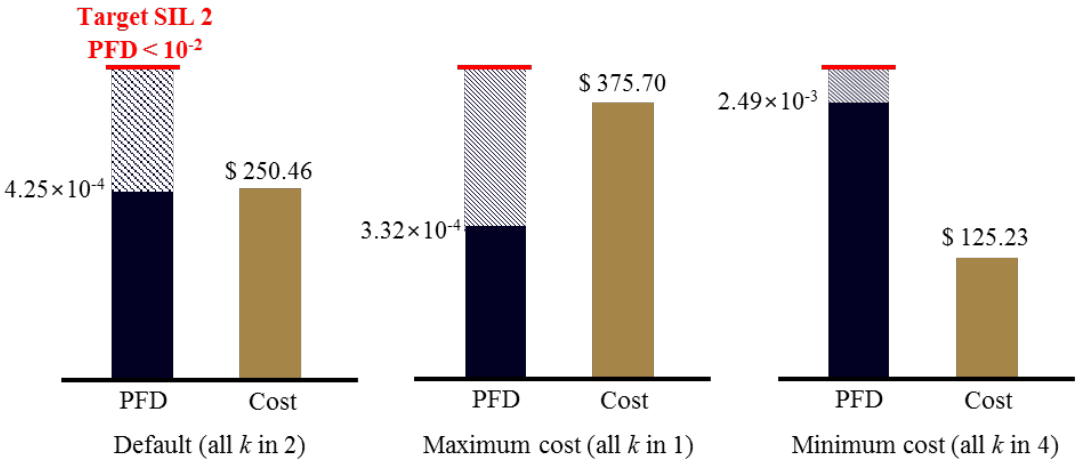

Fig. 2. PFD and cost comparison among default, maximum cost and minimum cost cases based on *j* for target SIL 2

Table 9. Performance comparison between the default and optimal solutions for SIL 2

Performance	Default (A)	Optimal (B)	Expected benefit (A-B)
Cost ($)	250.46	125.23	125.23

As a result, the optimal solution was the case in which the lowest-quality components were selected among the assumed alternatives, because this case had a sufficient margin in terms of its probability measurement. However, if the target SIL was set to SIL 3 instead of SIL 2, then the target SIL could not be achieved, due to the AC of subsystems S2, S3, S5, and S9. Thus, Section 4.2.2 considers additional fault checking modules to improve the SFF of these subsystems.

4.2.2 Changing the Components and using Additional Fault Checking Modules to Achieve the Target SIL

Given a target SIL of 3, additional fault checking modules were considered to achieve the target SIL. Hence, the additional fault checking module was assumed to have 99% DC and a \$100 cost. The AC of subsystems S2, S3, S5, and S9 were determined to be SIL 2 in the default design of the gas detector. Subsystems S2 and S9 could be improved to SIL 3 by converting to higher-quality components. However, subsystems S3 and S5 could not achieve SIL 3 simply by changing the components.

In this section, we reconfigured the optimal design for the gas detector, based on optimization Model II. To apply this model, we classified the components that improved the DC as decision variable y_{ijk}. Accordingly, some of the components associated with subsystems S2, S3, S5, and S9 were assigned to y_{ijk}.

Following the above assumptions, the hardware SIL of the gas detector achieved SIL 3 using the new model. The total cost for the gas detector was \$371.34 as the minimum cost, and the PFD of the new optimal design was 9.99×10^{-4} FIT. In this optimal solution, an additional fault checking module was added to subsystems S3 and S5. As a result, a cost benefit of \$79.12 was expected based on the proposed procedure when two fault checking modeles were added (**Fig. 4** and **Table 10**).

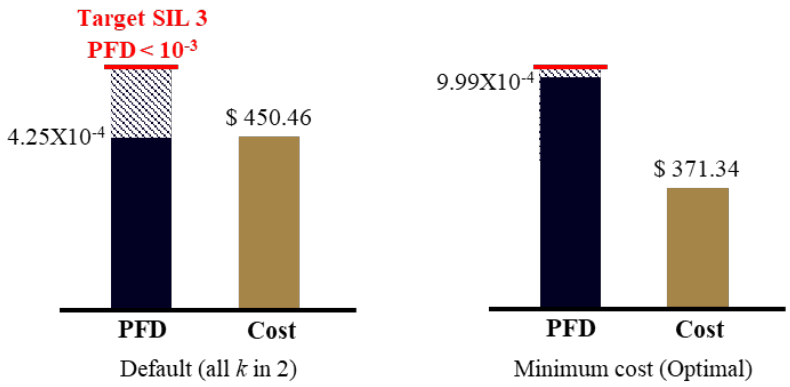

Fig. 4. PFD and cost comparison between default and optimal cases for target SIL 3

Table 10. Performance comparison between the default and optimal solutions for SIL 3

Performance	Default (A)	Optimal (B)	Expected benefit (A-B)
Cost (\$)	450.46	371.34	79.12

5. Conclusion

This study proposed an optimal reliability design procedure using the FMEDA process and integer programming, to achieve the target hardware SIL of SRS at minimal cost. In addition, to demonstrate its effectiveness, we applied the newly developed procedure to a case study of a gas detector.

For applying the procedure, an FMEDA process was performed to evaluate the hardware SIL and/or reliability of the SRS. This process was used to assign failure rates, failure modes, and the failure mechanism distribution of each component. Additionally, failure effects, safety mode, and detectability of each failure mode were defined. The proposed optimization modeling was performed using integer programming when the output of the FMEDA process was calculated. For concurrently achieving minimum component cost and the target SIL, the models provided the optimum solution by selecting the appropriate alternative components and/or fault checking modules. The models were formulated from probability and structural measures to evaluate the hardware SIL in terms of IEC 61508 standards.

The proposed method was applied to a case study of a gas detector. For evaluation of the hardware SIL, we complied with the evaluation criteria of the SIL outlined by IEC 61508. Failure rates were assigned using Telcordia SR-332. The failure rates of each component were modified by multiplying the generic failure rates by adjustment factors, based on the black box technique of Telcordia SR 332. These adjustment factors were determined by the operating temperature, electrical stress, quality level, and environment conditions of the SRS installation. We also assigned failure modes and distributions to each component based on the FMD-2013. As a result, the hardware SIL of the gas detector was determined to be SIL 2 from evaluation criteria, based on both architectural and probability constraints.

Given this SIL assignment, default designs were developed for this gas detector. The optimal reliability design of the gas detector considered two cases. The first case assumed only a change in the components. The second case included a change in components, in addition to the inclusion of additional fault checking modules. Our proposed method successfully optimized the reliability design of the gas detector via integer programming and achieved the targeted SIL for minimal total cost.

As a result, the proposed procedure can be applied when an optimal design that achieves both the target SIL and minimum cost of SRS is required. The SIL hardware of SRS is evaluated more effectively, and the optimal design of the SRS is provided, based on the information given by the procedure.

Acknowledgement

This work was supported by the GRRC program of Gyeonggi province. [GRRC KGU 2018-B05, Smart Manufacturing Application Technology Research].

References

[1] “Functional safety of electrical/electronic/programmable electronic safety-related systems, 2.0 Edition. IEC 61508,” *International Electrotechnical Commission (IEC)*, Geneva, Switzerland, 2010. Article (CrossRef Link).

[2] S. K. Kim and Y. S. Kim, “An evaluation approach using a HARA and FMEDA for the hardware SIL,” *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 6, pp. 1212-1220, 2013. Article (CrossRef Link).

[3] 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, 1999. Article (CrossRef Link).
[4] 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, 2010. Article (CrossRef Link).
[5] I. Yoshimura and Y. Sato, "Safety achieved by the safe failure fraction (SFF) in IEC 61508," *IEEE Transactions on Reliability*, vol. 57, no. 4, pp. 662-669, 2008. Article (CrossRef Link).
[6] R. Pilch, "Extending the Possibilities of Quantitative Determination of SIL–a Procedure Based on IEC 61508 and the Markov Model with Common Cause Failures," *Quality and Reliability Engineering International*, vol. 33, no. 2, pp. 337-346, 2017. Article (CrossRef Link).
[7] 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, 2007. Article (CrossRef Link).
[8] L. Ding, H. Wang, J. Jiang and A. Xu, "SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram," *Reliability Engineering and System Safety*, vol. 165, pp. 170-187, 2017. Article (CrossRef Link).
[9] C. H. Hu, X. S. Si and J. B. Yang, "System reliability prediction model based on evidential reasoning algorithm with nonlinear optimization," *Expert Systems with Applications*, vol. 37, no. 3, pp. 2550-2562, 2010. Article (CrossRef Link).
[10] M. Demichela, R. Pirani and M. C. Leva, "Human Factor Analysis Embedded in Risk Assessment of Industrial Machines: Effects on the Safety Integrity Level," *International Journal of Performability Engineering*, vol. 10, no. 5, pp. 487-496, 2014. Article (CrossRef Link).
[11] E. Piesik, M. Śliwiński and T. Barnert, "Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects," *Reliability Engineering and System Safety*, vol. 152, pp. 259-272, 2016. Article (CrossRef Link).
[12] "Reliability prediction procedure for electronic equipment," *Telcordia Technologies*, Inc.,. Telcordia SR-332 Issue 4, Jersey, USA, 2016. Article (CrossRef Link).
[13] A. Goel and R. J. Graves, "Electronic system reliability: collating prediction models," *IEEE Transactions on Device and Materials Reliability*, vol. 6, no. 2, pp. 258-265, 2006. Article (CrossRef Link).
[14] G. Cassanelli, G. Mura, F. Cesaretti, M. Vanzi and F. Fantini, "Reliability predictions in electronic industrial applications," *Microelectronics Reliability*, vol. 45 no. 9-11, pp. 1321-1326, 2005. Article (CrossRef Link).
[15] F. Brissaud, D. Charpentier, M. Fouladirad, A. Barros and and C. Bérenguer, "Failure rate evaluation with influencing factors," *Journal of Loss Prevention in the Process Industries*, vol. 23, no. 2, pp. 1000-1009, 2010. Article (CrossRef Link).
[16] K. -W. Jang and J. -H. Kim, "A Tabu Search for Multiple Multi-level Redundancy Allocation Problems in Series-Parallel Systems," *International Journal of Industrial Engineering: Theory, Applications and Practice*, vol. 18, no. 3, pp. 120-129, 2011. Article (CrossRef Link).
[17] Y. Gheraibia, K. Djafri and H. Krimou, "Ant colony algorithm for automotive safety integrity level allocation," *Applied Intelligence*, vol. 48, no. 3, pp. 555-569, 2018. Article (CrossRef Link).
[18] A. R. Yildiz, "A comparative study of population-based optimization algorithms for turning operations," *Information Sciences*, vol. 210, pp. 81-88, 2012. Article (CrossRef Link).
[19] A. C. Torres-Echeverría, S. Martorell and H. A. Thompson, "Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse," *Reliability Engineering and System Safety*, vol. 94, no. 2, pp. 162-179, 2009. Article (CrossRef Link).
[20] 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, 2009. Article (CrossRef Link).

[21] A. C. Torres-Echeverría, S. Martorell and H. A. Thompson, "Multi-objective optimization of design & testing of safety instrumented systems with MooN voting architectures using a genetic algorithm," *Reliability Engineering and System Safety*, vol. 106, pp. 45-60, 2012. Article (CrossRef Link).
[22] M. Marseguerra, E. Zio, L. Podofillini and D. W. Coit, "Optimal design of reliable network systems in presence of uncertainty," *IEEE Transactions on Reliability*, vol. 54, no. 2, pp. 243-253, 2005. Article (CrossRef Link).
[23] S. V. Amari, H. Pham and G. Dill, "Optimal design of k-out-of-n:G subsystems subjected to imperfect fault-coverage," *IEEE Transactions on Reliability*, vol. 53, no. 4, pp. 567-575, 2004. Article (CrossRef Link)
[24] J. Safari, "Multi-objective reliability optimization of series-parallel systems with a choice of redundancy strategies," *Reliability Engineering and System Safety*, vol. 108, pp. 10-20, 2012. Article (CrossRef Link).
[25] M. Sharifi, G. Cheragh, K. D. Maljaii, A. Zaretalab and A. V. F. Daei, "Reliability optimization of a series-parallel k-out-of-n system with failure rate depends on working components of system," *International Journal of Industrial Engineering: Theory, Applications and Practice*, vol. 22, no. 4, pp. 438-453, 2015. Article (CrossRef Link).
[26] R. A. Bakkiyaraj and N. Kumarappan, "Optimal reliability planning for a composite electric power system based on Monte Carlo simulation using particle swarm optimization," *International Journal of Electrical Power and Energy Systems*, vol. 47, pp. 109-116, 2013. Article (CrossRef Link).
[27] C. Elegbede, C. Chu, K. H. Adjallah and F. Yalaoui, "Reliability allocation through cost minimization," *IEEE Transactions on Reliability*, vol. 52, no. 1, pp. 106-111, 2003. Article (CrossRef Link).
[28] "Failure mode/ mechanism distributions," *Reliability Information Analysis Center (RIAC)*, FMD-2013, New York, USA, 2013. Article (CrossRef Link).

Sung Kyu Kim received M.S. degree from Kyonggi University, Republic of Korea in 2014. He is a Ph.D. candidate in Industrial and Management Engineering, Kyonggi University, Republic of Korea. His research interests include reliability engineering, optimization and functional safety.

Yong Soo Kim is an associate professor at the Department of Industrial and Management Engineering, Kyonggi University, Korea. He received B.S., M.S. and Ph.D degree from KAIST, respectively. His research interests include data mining and reliability.