Korean J. Chem. Eng., 34(3), 619-627 (2017)
DOI: 10.1007/s11814-016-0321-1

pISSN: 0256-1115
eISSN: 1975-7220

FTA-FMEA-based validity verification techniques for safety standards

Chung Keun Chae† and Jae Wook Ko

Department of Chemical Engineering, Kwangwoon University, 20 Kwangwoon-ro, Nowon-gu, Seoul 01897, Korea
(*Received 12 April 2016 • accepted 20 November 2016*)

Abstract−Scientific and technological advances have yielded a plethora of benefits, but the associated risks have increased as well. Although numerous safety standards have been established for various applications, these standards have not been adequately verified. In this study, a method is proposed for prioritizing safety standard priorities on the basis of minimal cut sets. In addition, safety standards obtained through fault tree analysis are applied to the breakdown modes and accident cause removal methods of failure mode and effects analysis to develop a validity verification method for safety standard sets. The developed method was applied to a gas-boiler exhaust system as a case study, and the validity of the safety standard sets and improvements in the safety standards were verified on the basis of the established safety standard priorities.

Keywords: Safety Standard, Failure Mode and Effects Analysis, Fault Tree Analysis, Minimal Cut Set, Safety Priority, Gas Boiler

INTRODUCTION

With progress in science and technology, living is becoming increasingly convenient; however, the various risks associated with the products of these advances are also increasing [1], especially in developing and newly industrialized countries. Therefore, safety standards for various applications, benchmarked to those in developed countries, have been established; however, the validity of these standards has not been adequately verified. This is concerning because safety standards that are not valid in their designed environments might result in unnecessary social costs without any reduction in risks.

Numerous studies have proposed methods for developing safety standards. Ma et al. [2] presented a method for developing safety standards for incineration systems by applying hazard and operability (HAZOP) techniques. Rhie and Kim [3] proposed a method for developing safety standards for hydrogen gas filling facilities by applying HAZOP and failure mode and effects analysis (FMEA) techniques. And Mun [4] presented a method for developing an efficient safety management plan for facilities at a high risk of accidents by using a fuzzy-FMEA technique. However, no study has yet verified the validity of all safety standards for a system.

Typically, a complex system follows the Pareto principle, also called the 80 : 20 principle: at least 80% of the risks result from 20% of the risk scenarios or complex system elements [5]. With this principle as its basis, the validity verification technique for safety standards developed in this study is aimed at identifying and overcoming the drawbacks of safety standards for a certain system to make the standards more comprehensive.

†To whom correspondence should be addressed.
E-mail: chae@meri.co.kr

THEORY

1. Fault Tree Analysis and Minimal Cut Set

The fault tree analysis (FTA) approach was originally developed as part of the US Army's intercontinental ballistic missile plan in 1961. Currently, FTA is widely applied in nearly all engineering domains and facilities, such as in nuclear power plants, petrochemical plants, and air traffic control centers [6]. FTA uses a logic diagram that infers the cause of system breakdown in a top-down order by using two types of logic gates: AND and OR. Thus, FTA can be easily understood visually and is useful for logically identifying the cause of an accident. A fault tree is drawn from the top event; thus, fault trees drawn from different top events differ and hence a system may have multiple fault trees [7]. Fig. 1 shows samples of seven basic events when FTA was implemented for a system with two top events.

A set of accidents occurring in a system is called a cut set, and a set of accidents with redundancies removed is called a minimal

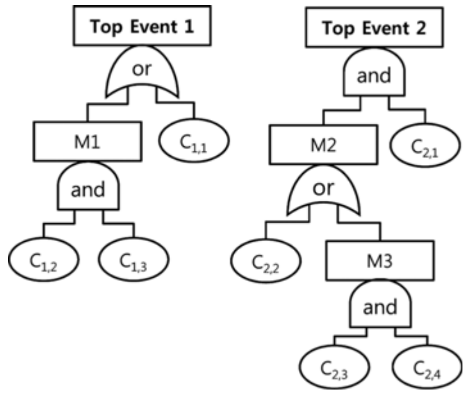

Fig. 1. Sample of FTA.

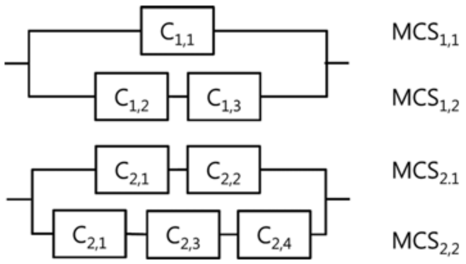

Fig. 2. Reliability block diagram.

cut set (MCS). When multiple accident causes within an MCS are simultaneously triggered, an accident occurs; however, if any of these causes are not present, no accident occurs [8]. A system with many MCSs is a relatively unsafe system, whereas a system with one MCS that contains many accident causes is a relatively safe system [8]. As shown in Fig. 2, the results of the MCS analysis for the FTA samples presented in Fig. 1 is $\{C_{1,1}\}$, $\{C_{1,2}, C_{1,3}\}$, $\{C_{2,1}, C_{2,2}\}$, and $\{C_{2,1}, C_{2,3}, C_{2,4}\}$.

Boolean algebra is used to mathematically express and calculate the AND and OR gates of a fault tree, whose probability is between 0 and 1 [9]. Risk is defined as the product of the consequence of a top event and its frequency [10]. Severity is a type of consequence, and occurrence is a type of frequency. The factors are related as shown in Eq. (1); individual risks have low probabilities [11].

$$\begin{aligned}\text{Risk}\left(\frac{\text{Fatalities}}{\text{Year}}\right) &= \text{Consequence}\left(\frac{\text{Fatalities}}{\text{Accidents}}\right)\times\text{Frequency}\left(\frac{\text{Accidents}}{\text{Year}}\right) \\ &= \text{Severity}\left(\frac{\text{Fatalities}}{\text{Accidents}}\right)\times\text{Occurrence}\left(\frac{\text{Accidents}}{\text{Year}}\right)\end{aligned} \quad (1)$$

Thus, the basic event for each MCS in the block diagram illustrated in Fig. 2 is related to an AND gate. The probability of the total frequency of each MCS is defined as Q_k and that of the frequency of a basic event is q_m. The number of basic events in an MCS is n. Accordingly, the probability can be calculated using Eq. (2). Similarly, the MCS for each top event is related to an OR gate; the probability of the total frequency of each top event is defined as Q_{TE}, and the number of MCSs in that top event is n. Accordingly, the probability can be calculated using Eq. (3).

$$Q_k = q_1 \cdot q_2 \cdots q_m = \Pi_{m=1}^{n} q_m \quad (2)$$

$$Q_{TE} = 1 - \Pi_{k=1}^{n}(1 - Q_k) \quad (3)$$

The principle of prioritizing safety standards using MCSs was examined under the assumption that the severity of top events 1 and 2 was 10^{-3} and 10^{-2}, respectively, and that the frequency of the

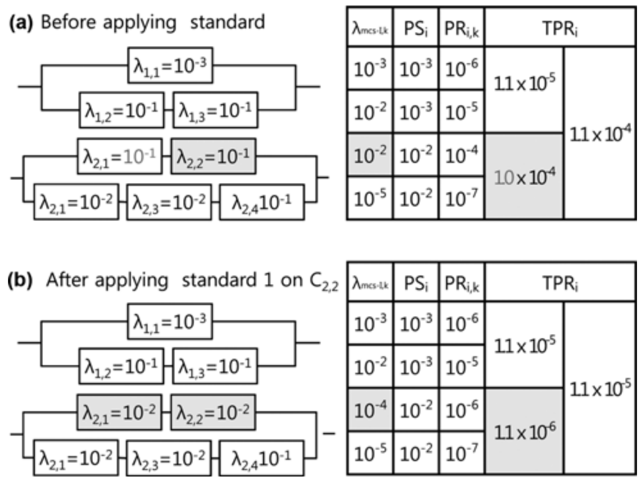

Fig. 3. Priority of risk reduction.

block diagram shown in Fig. 2 (or failure rate) was as shown in Fig. 3(a). Because the risk value of each MCS is 10^{-6}, 10^{-5}, 10^{-4}, and 10^{-7}, respectively, the highest-frequency MCS is $MCS_{2,1}$, whose risk value is 10^{-4}. Thus, the safety standards that can reduce the risk of $MCS_{2,1}$ are assigned the top priority. Under the assumption that applying safety standards to $C_{2,1}$ and $C_{2,2}$ reduces the risk to 10^{-6}, the second-highest-frequency MCS is $MCS_{1,2}$. Thus, the prioritization of the safety standards considering each accident cause can be derived. However, in practice, obtaining data on the severity and occurrence of events and applying it to each safety standard item is difficult; thus, the discussed principle cannot be applied directly. Therefore, this study applied FTA in combination with the FMEA technique.

2. Failure Mode and Effects Analysis

FMEA was first used in the mid-1960s during NASA's Apollo space mission program. Since the 1970s, it has been used in various industrial sectors, for example, to solve business deficits in the automotive industry and in response to the Product Liability Act [12]. FMEA is used to estimate severity, occurrence, and detection of a failure mode based on experts' evaluation as well as to establish priorities of accident cause removal methods in terms of the risk priority number (RPN), which is the product of these three factors [12]. Table 1 shows a commonly used FMEA worksheet [13].

FTA accounts for the correlation among the undesired factors; by contrast, FMEA considers the effect of each factor. In addition, FTA may combine each factor's probability of occurrence, whereas FMEA cannot combine the probability of upper event occurrence [13]. Despite these differences, FTA and FMEA are complementary. FTA is an empirical, a priori, deductive technique, and it is integrated to the back of FMEA, an empirical, inductive technique,

Table 1. Generic FMEA worksheet

Item	Function	Potential failure mode	Potential effect(s) of failure	Severity	Potential cause(s) of failure	Occurrence	Current design controls (prevention)	Current design controls (detection)	Detection	RPN	Recommended action(s)

to understand the fracture mode in FMEA and the correlation between causes and results [12-16].

Kim et al. [17] conducted a fault analysis of an IC card payment system by using FTA and proposed a method to evaluate and improve the security of the system through FMEA of the identified defects. Jang [18] proposed a method to determine the RPN through FMEA of the breakdown cause of a hierarchical structure determined using FTA. These studies have integrated FMEA to the back of FTA, unlike existing methods [19-21].

PROPOSED VALIDITY VERIFICATION TECHNIQUE

1. Procedure of Validity Verification Technique

This study proposes a validity verification technique for safety standards by integrating FMEA to the back of FTA. In addition to including the safety standards as an evaluation target, the proposed method differs from those in the literature primarily in its ability to prioritize the safety standards in multiple stages (i.e., for MCS→ for each accident cause→for each safety standard); this is realized by applying the MCS of accident causes identified through the FTA into the failure mode of an FMEA. The proposed method thus extends the conventional FTA-FMEA integrative method by one step.

As explained earlier, FTA is used to logically identify the accident causes within a system, whereas FMEA is used to prioritize the removal of accident causes in terms of the RPN of the causes. Thus, by integrating FTA and FMEA, the safety standards applied to remove accident causes can be prioritized; subsequently, the MCS can be linked, which enables the relative evaluation of the adequacy of the safety standards for an accident-cause group, thus allowing validity verification of a safety standard set (i.e., a group of safety standards established for ensuring the safety of a system).

The proposed method entails the following steps: FTA execution, FTA and FMEA connection, and FMEA execution (Fig. 4). In the FTA execution step, the target system for safety management is selected, the top event is decided, and FTA is executed to determine the MCS. In the FTA and FMEA connection step, the MCS is applied to the potential failure mode of a common FMEA worksheet, and the accident causes that belong to that MCS are applied to the potential cause(s) of failure to produce an FMEA worksheet specifically designed for safety standards validity verification. In the FMEA execution step, safety standards are applied to the current design controls (prevention); $S_{i,j}$, $O_{i,j}$, and $\Delta O_{i,j}$ are entered, and the validity of safety standards is verified using a safety standard prioritization tool. In this technique, evaluation elements with low effectiveness, such as detection, are removed from the worksheet.

Generally, in FMEA, severity and occurrence are rated on a scale of 1-10 [12]. However, to facilitate the use of the RPN for comparing priorities between MCSs in an FMEA worksheet, the RPNs must be expressed as a probability (Fig. 3). Hence, priorities are determined based on the total probability of risk (TPR), which is the product of the RPNs of multiple accident causes. The severity and occurrence scale can be converted into a probability scale by using Eq. (4) [22], where Gr is the magnitude (1-10) of severity and occurrence.

$$\mathrm{Pr} = \frac{1}{10^{(10-Gr)}} \tag{4}$$

2. Principle of Validity Verification Techniques

Table 2 shows an example worksheet in which the priorities of the safety standards are determined by applying FMEA to accident causes that are based on the FTA samples shown in Fig. 1, assuming 12 safety standards. A single safety standard may be applicable to multiple accident causes; this characteristic is reflected in the worksheet.

Before applying the listed safety standards, the TPRs of $MCS_{1,1}$, $MCS_{1,2}$, $MCS_{2,1}$, and $MCS_{2,2}$ were 10^{-9}, 10^{-10}, 10^{-9}, and 10^{-10}, respectively. Although both $MCS_{1,1}$ and $MCS_{2,1}$ were 10^{-9}, $MCS_{1,1}$ has a higher frequency of occurrence and fewer accident causes. Thus, the safety standard S001 for $C_{1,1}$ is assigned the top priority. Moreover, as S001 is applicable to $C_{1,3}$ as well, the TPR of $MCS_{1,2}$ also decreases. In brief, when multiple MCSs have the same $PR_{i,j}$, the MCS whose S_i has a larger $PR_{i,j}$ is considered a higher risk and thus must be given a higher priority; if the S_i of these MCSs are equal as well, the MCSs are prioritized randomly.

Higher-frequency MCSs can be prioritized in terms of level of

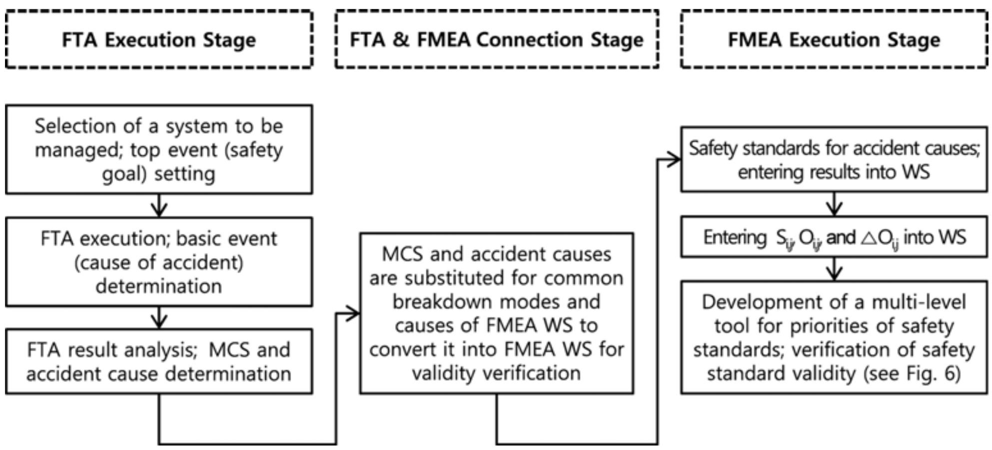

Fig. 4. Procedure of validity verification techniques.

Table 2. Worksheet for priority deduction

$MCS_{i,k}$	$C_{i,j}$	S_i	PS_i	Sn	$O_{i,j}$	$\Delta O_{i,j}$	No standard				No standard 1				No standard 2				No standard 3				No standard 4				Priority
							-	-	RPN		-	-	RPN		-	-	RPN		-	-	RPN		-	-	RPN		
							$\Delta O_{i,j}$	$PO_{i,j}$	$PR_{i,j}$	$TPR_{i,k}$	$\Delta O_{i,j}$	$PO_{i,j}$	$PR_{i,j}$	$TPR_{i,k}$	$\Delta O_{i,j}$	$PO_{i,j}$	$PR_{i,j}$	$TPR_{i,k}$	$\Delta O_{i,j}$	$PO_{i,j}$	$PR_{i,j}$	$TPR_{i,k}$	$\Delta O_{i,j}$	$PO_{i,j}$	$PR_{i,j}$	$TPR_{i,k}$	
				No standard			3				3				3				3				3				
				S001		1	0				1				1				1				1				1
$MCS_{1,1}$	$C_{1,1}$	8	1E-02	S002	3	1	0	1.E-07	1.E-09	1.E-09	0	1.E-08	1.E-10	1.E-10	0	1.E-08	1.E-10	1.E-10	1	1.E-09	1.E-11	1.E-11	1	1.E-10	1.E-12	1.E-12	3
				S003		1	0				0				0				0				1				4
				S004		1	0				0				0				0				0				
				No standard			7				7				7				7				7				
	$C_{1,2}$	8	1E-02	S010	7	1	0	1.E-03	1.E-05		0	1.E-03	1.E-05		0	1.E-03	1.E-05		0	1.E-03	1.E-05		0	1.E-03	1.E-05		
				S007		1	0				0				0				0				0				
$MCS_{1,2}$				S005		1	0			1.E-10	0			1.E-12	0			1.E-14	0			1.E-15	0			1.E-15	
				No standard			7				7				7				7				7				
	$C_{1,3}$	8	1E-02	S006	7	2	0	1.E-03	1.E-05		0	1.E-05	1.E-07		2	1.E-07	1.E-09		2	1.E-08	1.E-10		2	1.E-08	1.E-10		2
				S001		2	0				2				2				2				2				1
				S002		1	0				0				0				1				1				3
				No standard			6				6				6				6				6				
	$C_{2,1}$	9	1E-01	S010	6	1	0	1.E-04	1.E-05		0	1.E-04	1.E-05		0	1.E-04	1.E-05		0	1.E-04	1.E-05		0	1.E-04	1.E-05		
				S007		1	0				0				0				0				0				
$MCS_{2,1}$				S005		1	0			1.E-09	0			1.E-09	0			1.E-11	0			1.E-11	0			1.E-12	
				No standard			7				7				7				7				7				
	$C_{2,2}$	9	1E-01	S006	7	2	0	1.E-03	1.E-04		0	1.E-03	1.E-04		2	1.E-05	1.E-06		2	1.E-05	1.E-06		2	1.E-06	1.E-07		2
				S008		2	0				0				0				0				0				
				S003		1	0				0				0				0				1				4
				No standard			6				6				6				6				6				
	$C_{2,1}$	9	1E-01	S010	6	1	0	1.E-04	1.E-05		0	1.E-04	1.E-05		0	1.E-04	1.E-05		0	1.E-04	1.E-05		0	1.E-04	1.E-05		
				S007		1	0				0				0				0				0				
				S005		1	0				0				0				0				0				
				No standard			8				8				8				8				8				
$MCS_{2,2}$	$C_{2,3}$	9	1E-01	S010	8	3	0	1.E-02	1.E-03	1.E-10	0	1.E-02	1.E-03	1.E-10	0	1.E-02	1.E-03	1.E-10	0	1.E-02	1.E-03	1.E-10	0	1.E-02	1.E-03	1.E-12	
				S009		2	0				0				0				0				0				
				No standard			9				9				9				9				9				
	$C_{2,4}$	9	1E-01	S003	9	2	0	1.E-01	1.E-02		0	1.E-01	1.E-02		0	1.E-01	1.E-02		0	1.E-01	1.E-02		2	1.E-03	1.E-04		4
				S011		1	0				0				0				0				0				
				S012		1	0				0				0				0				0				

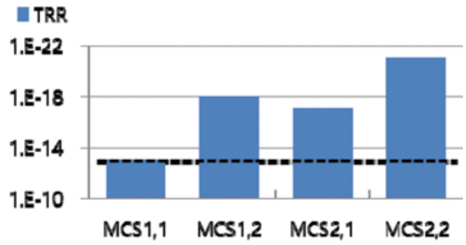

Fig. 5. Safety level of the $MCS_{i,k}$.

reduction in the safety standards for each MCS. The safety standards for the TPR of $MCS_{1,1}$ were reduced at 10^{-13} (Fig. 5). Thus, if the safety standards for $MCS_{1,1}$ are maintained the same and if those for the other MCSs are improved, the overall safety of the system would not largely improve. Thus, additional safety standards applicable to $MCS_{1,1}$ must be developed to enhance system safety.

3. Development of Validity Verification Tool

For a low number of MCSs and safety standards, the safety standards can be prioritized manually, as shown in Table 2. However, as the number of MCSs and standards increases, automation, such as algorithm presented in Fig. 6, become necessary.

CASE STUDY

1. Executing FTA

More than 13 million gas boilers have been installed and are in use in Korea. The safety standards (e.g., separation distance, materials, structures, and durability) pertaining to the installation of gas boilers are specified in the Korea Gas Safety Code KGS FU551 ("Facility/Technical/Inspection Code for Urban Gas Using Facility"). Accidents occur despite these specification: during 2010-2014, 19 people died and 105 were injured from CO gas poisoning accidents involving gas boilers.

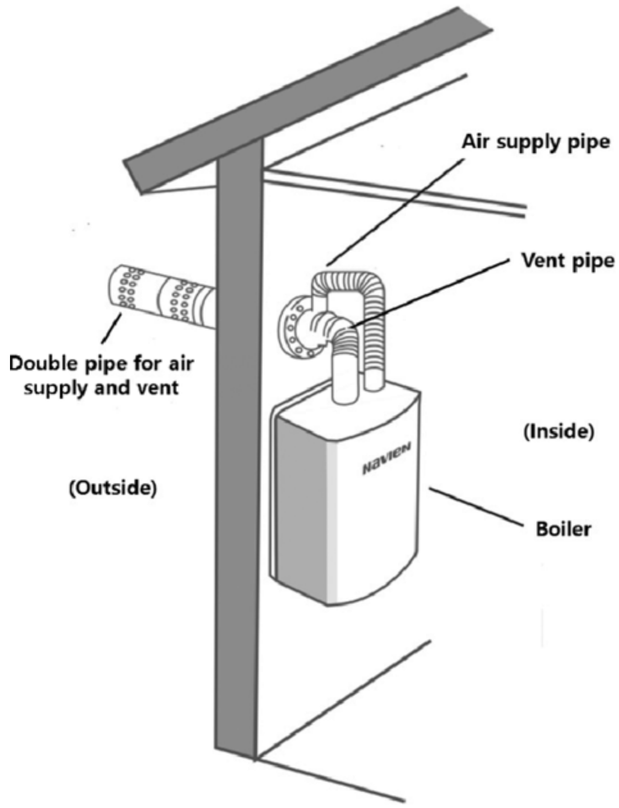

Fig. 7. Gas boiler system.

In the proposed method, FTA is implemented to identify potential accident causes and the corresponding MCSs. Potential acci-

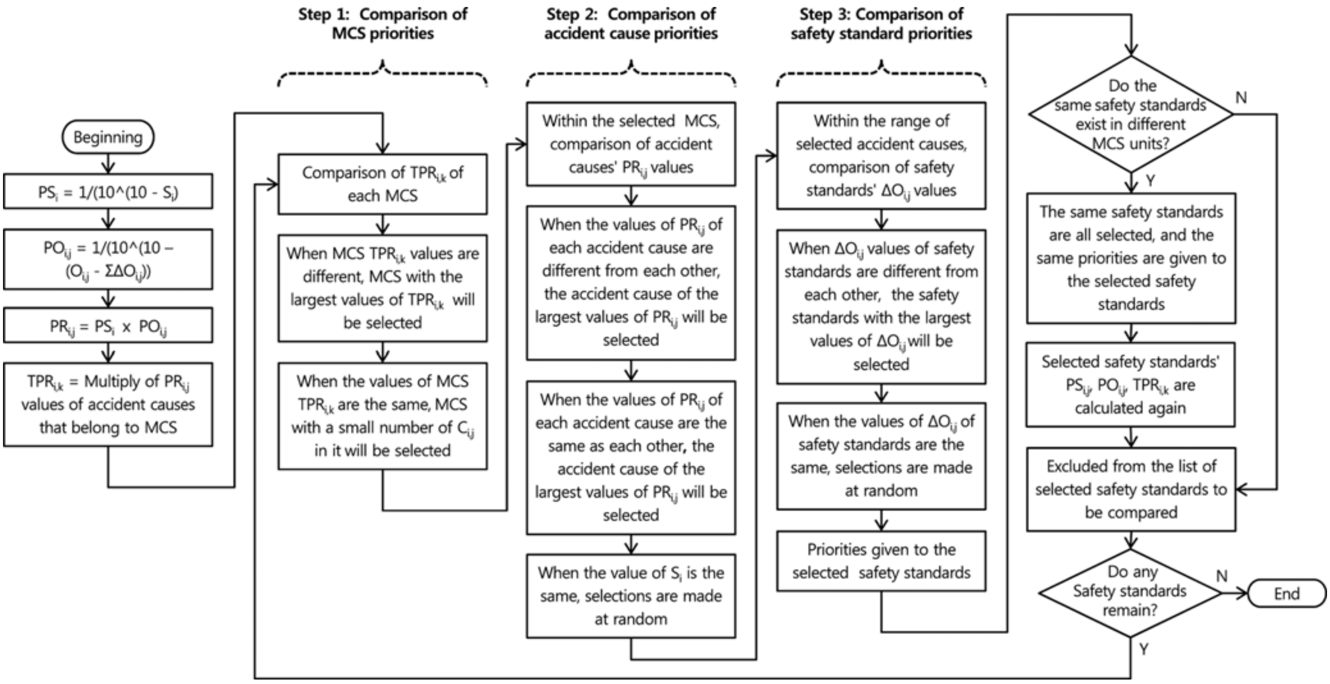

Fig. 6. Algorithm for priority deduction of safety standards.

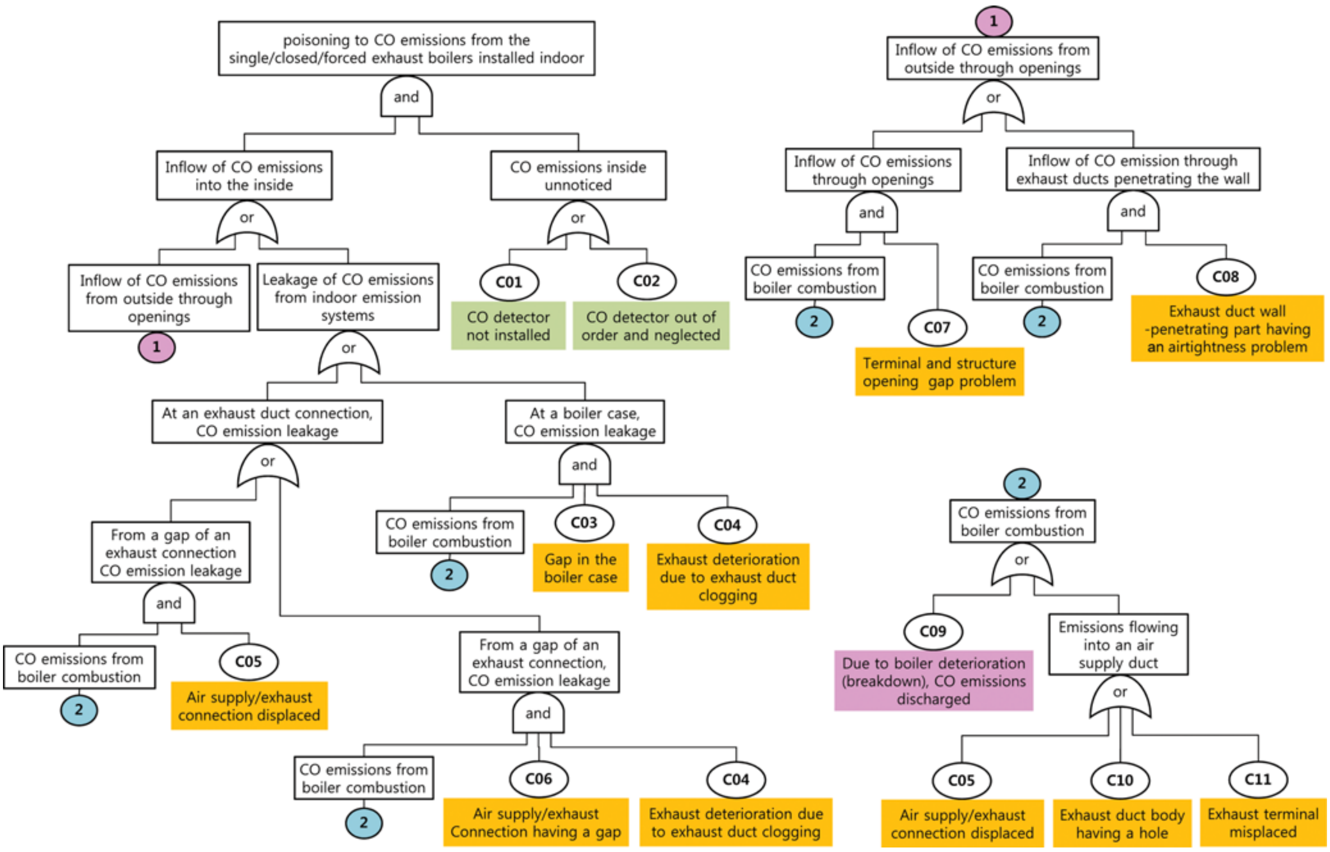

Fig. 8. Fault tree analysis of gas boiler system.

dents in gas-boiler exhaust systems include overheating-induced fire and CO poisoning due to system leakage. However, technological advances in the manufacturing and installation of gas boilers have largely precluded fire accidents; hence, CO poisoning is focused on in this case study, where the FTA target is a gas-boiler exhaust system for family use (forced exhaust boilers) (Fig. 7). FTA is executed as follows: First, "poisoning due to CO emissions from a single/closed/forced exhaust boiler installed indoor" is set as a top event. Second, FTA is implemented (Fig. 8), and accident causes are drawn (Table 3). Third, the MCS (40) of the accident causes is derived using the algorithm (Fig. 6).

Table 3. Gas boiler accident cause of CO addiction

Item	Cause of accident
C01	CO detector not installed
C02	CO detector out of order and neglected
C03	Gas boiler case having a crack
C04	Exhaust deterioration due to exhaust duct clogging
C05	Ventilation duct connection displaced
C06	Ventilation duct connection having a crack
C07	Terminal and structure opening gap problem Exhaust
C08	duct wall-penetrating part having an airtightness problem
C09	CO emissions due to gas boiler deterioration (breakdown)
C10	Exhaust duct body having a hole
C11	Exhaust duct terminal misplaced

2. Executing FMEA

On the basis of the accident causes and the MCS derived through the FTA, an FMEA must be implemented to prioritize the safety standards, as follows: First, the types (20) of safety standards specified in KGS FU551 are drawn. Second, these standards are distributed as the 11 accident cause removal methods derived through the FTA. Third, an FMEA worksheet (Table 4) is completed by using the severity, occurrence, and occurrence reduction probability listed in Table 5 [17]. Finally, the priorities are calculated using the worksheet (Fig. 6; Table 6).

3. Validity Analysis

According to the analyses, the safety standards for MCS19 and MCS20 were prioritized as third (Table 6). In addition, MCS19 and MCS20 were found to have high frequencies of occurrence, indicating the low validity of these safety standards. To compensate for these ineffective standards, the four new standards listed in Table 7 were added; subsequently, the validities were recalculated (Table 8). With the addition of these new standards, the reduction priority of safety standards for MCS19 and MCS20 decreased from third to sixth and to seventh, respectively, thus increasing the overall validity of the safety standards.

The standards for Sn stated in Table 8 are presented in Table 9. Among the 20 listed safety standards, the first, second, and third priorities were "installation of combination-type exhaust ducts," "leakage check during operation," and "service provider's safety check," respectively. The fourth and fifth priorities were "installation of a

Table 4. FMEA worksheet for priority deduction of gas boiler safety standards

$MCS_{i,k}$	$C_{i,j}$		S_i	Sn	Standards	$O_{i,j}$	$\Delta O_{i,j}$
Omitted							
MCS19	C01	CO detector not installed	2			10	
	C05	Ventilation duct connection misplaced	10	2.1.3.5	Exhaust duct to be connected in a screw type, flange type, or clamp type	6	2
				3.1.2.1	Combusted waste gas leakage checking by the user during the operation		1
				3.1.2.2	Exhaust system safety checking to be conducted by the gas service provider during the operation in accordance with specified regulations		2
MCS20	C02	CO detector out of order and neglected	3			8	
	C05	Ventilation duct connection displaced	10	2.1.3.5	Exhaust duct to be connected in a screw type, flange type, or clamp type	6	2
				3.1.2.1	Combusted waste gas leakage checking by the user during the operation		1
				3.1.2.2	Exhaust system safety checking to be conducted by the gas service provider during the operation in accordance with specified regulations		2
The rest below is omitted							

Table 5. Values range of severity and occurrence

Classification	Range of values
Severity	$0 \le S < 1$: No criticality $1 \le S < 3$: Low level of criticality $3 \le S < 6$: High level of criticality $6 \le S < 9$: Seriously high level of criticality $9 \le S < 10$: Extremely critical
Occurrence	$0 \le O < 1$: No probability $1 \le O < 3$: Almost no probability $3 \le O < 6$: Occasionally probable $6 \le O < 9$: High probability $9 \le O < 10$: Quite high probability

Table 6. Priority before strengthening the standards

$MCS_{i,k}$	$C_{i,j}$	Sn	Priority	Exhausted
MCS19/20	C05	2.1.3.5	1	
MCS19/20	C05	3.1.2.1	2	
MCS19/20	C05	3.1.2.2	3	●/◎
MCS7	C11	2.2.3.6	4	
MCS7	C07	2.2.3.11.(1)	5	⊙
MCS15	C11	2.2.3.8	6	
MCS15	C08	2.1.3.10	7	
MCS15	C11	2.2.3.9	8	
MCS15	C08	2.2.3.3	9	
The rest is omitted				

CO detector indoors" and "service provider's check of CO detectors," respectively, indicating the necessity of the newly added safety standards.

CONCLUSION

We have proposed an FMEA worksheet-based method for determining the priorities of safety standards by integrating FTA and FMEA and for quantitatively verifying the validity of safety standard sets. In addition, we have presented an algorithm for prioritizing the safety standard priorities. Because FMEA is applied to MCSs according to an FTA, multilevel priorities can be established for each MCS, each accident cause, and each standard.

In the proposed method, the validity of the safety standards is verified as follows. First, the accident causes of the target system and the associated MCSs are determined through FTA. Second, MCSs are applied to the breakdown mode of the FMEA worksheet, and safety standards for accident cause removal in each MCS are applied to this worksheet. Third, $S_{i,j}$, $O_{i,j}$, and $\Delta O_{i,j}$ (as determined by experts) are entered in the worksheet. Fourth, the safety standards are prioritized using an engineering tool based on the presented algorithm. Fifth, the validity (balance among MCSs) of all safety standards is verified using the order of the MCS safety standard reduction as the index. Finally, the safety standards for weak areas of the system are improved by strengthening the safety standards for accident causes present in higher-frequency MCSs. The proposed method was demonstrated by applying it to a gas-boiler exhaust system for family use as a case study.

A future study can explore expanding the proposed method to determine both safety and economic feasibility by applying the fig-

Table 7. FMEA worksheet for priority deduction of gas boiler safety standards

$MCS_{i,k}$	$C_{i,j}$		S_i	Sn	Standards	$O_{i,j}$	$\Delta O_{i,j}$
Omitted							
MCS19	C01	CO detector not installed	2	New 01	Install a CO detector indoors	10	4
				New 02	Install a dual sensor CO detector indoors		4
	C05	Ventilation duct connection misplaced	10	2.1.3.5	Combine the exhaust duct in a screw type, flange type, or clamp type	6	2
				3.1.2.1	Combusted waste gas leakage checking by the user during the operation		1
				3.1.2.2	Exhaust system safety checking to be conducted by the gas service provider during the operation in accordance with specified regulations		2
MCS20	C02	CO detector out of order and neglected	3	New 03	Safety checking for the CO detector to be conducted by the gas service provider in accordance with specified regulations	8	3
				New 04	Install a device that suspends the gas boiler operation upon CO detector breakdown		4
	C05	Ventilation duct connection displaced	10	2.1.3.5	Combine the exhaust duct in a screw type, flange type, or clamp type	6	2
				3.1.2.1	Combusted waste gas leakage checking by the user during the operation		1
				3.1.2.2	Exhaust system safety checking to be conducted by the gas service provider during the operation in accordance with specified regulations		2
The rest below is omitted							

Table 8. Priority after strengthening the standards

$MCS_{i,k}$	$C_{i,j}$	Sn	Priority	Exhausted
MCS19/20	C05	2.1.3.5	1	
MCS19/20	C05	3.1.2.1	2	
MCS19/20	C05	3.1.2.2	3	
MCS19	C01	New 01	4	
MCS20	C02	New 03	5	
MCS19	C01	New 02	6	●
MCS20	C02	New 04	7	◎
MCS7	C11	2.2.3.6	8	
MCS7	C07	2.2.3.11.(1)	9	⊙
The rest is omitted				

ure of economic feasibility as a detection item in the FMEA. Further, for estimating $S_{i,j}$, $O_{i,j}$, and $\Delta O_{i,j}$, the accuracy of the experts' evaluation can be improved by adopting an analytic hierarchy process or by automating the estimation process by using a fuzzy theory-based expert system.

ACKNOWLEDGEMENT

This study was a part of a research project conducted with funding from the Ministry of Trade, Industry and Energy (20132010500030).

NOMENCLATURE

$C_{i,j}$: accident cause j of top event i
$MCS_{i,k}$: MCS k of top event i
Q_k : total frequency probability of $MCS_{i,k}$
q_m : probability of basic event frequency
Q_{TE} : total frequency probability of top event i
$\lambda_{i,j}$: failure rate of $C_{i,j}$
$\lambda_{MCS\text{-}i,k}$: failure rate of $MCS_{i,k}$

Table 9. Priority of gas boiler safety standards

Sn	Description
2.1.3.5	Combine the exhaust duct in a screw type, flange type, or clamp type
3.1.2.1	Combusted waste gas leakage checking by the user during the operation
3.1.2.2	Exhaust system safety checking to be conducted by the gas service provider during operation
New 01	Install a CO detector indoors
New 03	CO detector safety checking to be conducted by the gas service provider
New 02	Install a dual-sensor CO detector indoors
New 04	Install a device that suspends the gas boiler operation upon CO detector breakdown
2.2.3.6	Take measures to protect exhaust ducts and terminals that involve the risk of damage to the external parts
2.2.3.11.(1)	No indoor inflow opening to be installed within 60 cm of the terminal

WS : worksheet
Gr : magnitude (1-10) of severity and occurrence
Pr : probability (0-1) of severity and occurrence
S_i : severity of top event i
PS_i : severity probability of top event i
$PR_{i,j}$: risk probability of $C_{i,j}$
$TPR_{i,k}$: total probability of risk of $MCS_{i,k}$
TPR_i : total probability of risk of top event i
$O_{i,j}$: occurrence of $C_{i,j}$
$\Delta O_{i,j}$: occurrence reduction probability of $C_{i,j}$ by standard n
$PO_{i,j}$: occurrence probability of $C_{i,j}$
Sn : standard number (where n=1, 2, 3…)

REFERENCES

1. K. R. Lee, Innovation Strategy to Mitigate Major Risks of the Korean Society, Science & Technology Policy Institute (2003).
2. B. C. Ma, H. M. Kwon and Y. C. Kim, *J. Korean Soc. Saf.*, **27**(6), 64 (2012).
3. K. W. Rhie and T. H. Kim, *Korea Saf. Manage. Sci.*, **14**(1), 95 (2012).
4. B. K. Mun, A Study on Efficient Safety Management of Disaster Risk Facility, Ph.D. Dissertation, Chonnam National University, Chonnam, Korea (2014).
5. M. Mohammad, *Risk Analysis in Engineering*, CRC Press, Boca Raton, Florida (2006).
6. J. B. Nicholas, *System Safety Engineering and Risk Assessment*, 2nd Ed., CRC Press, Boca Raton, Florida (2014).
7. T. T. Michael, *Risk-Based Reliability Analysis and Generic Principles for Risk Reduction*, Elsevier, London (2007).
8. D. J. Kim, H. C. Kim and J. O. Kim, *Trans. Korean Inst. Electr. Eng.*, **58**(1), 27 (2009).
9. U.S. Nuclear Regulatory, *Fault Tree Handbook* (1981).
10. M. Modarres, *Risk Analysis in Engineering*, CRC Press, Boca Raton, Florida (2006).
11. H. Y. Kim, W. So, D. I. Shin and I. S. Yoon, *Korean J. Chem. Eng.*, **28**(6), 1322 (2011).
12. M. H. Kim and I. S. Woo, *J. Korean Soc. Saf.*, **28**(4), 81 (2013).
13. S. C. Carl, *Effective FMEAs*, Wiley, Hoboken, New Jersey (2012).
14. D. H. Stamatis, *Failure Mode and Effect Analysis*, ASQ, Milwaukee, Wisconsin (2003).
15. K. H. Moon, S. H. Kim, J. H. Choi and J. K. Kim, *J. Korean Soc. Aviation Aeronautics*, **21**(4) (2013).
16. S. I. Lee, B. S. Chu and D. J. Chang, *Int. J. Precision Eng. Manufacturing*, **15**(2), 331 (2014).
17. M. H. Kim, E. J. Jin and M. G. Park, *J. Korea Multimedia Soc.*, **16**(1), 87 (2013).
18. H. A. Jang, Risk Evaluation of Hierarchical Failure Causes in FMEA, Ph.D. Dissertation, Pukyong National University, Busan, Korea (2015).
19. E. J. Jin, M. H. Kim and M. G. Park, *KIPS Trans. Software Data Eng.*, **2**(1), 7 (2013).
20. M. H. Kim, W. Toyib and M. G. Park, *KIPS Trans. Computer Communication Systems*, **2**(12), 541 (2013).
21. W. Toyib, An Integrative Method of FTA and Software FMEA for Security Analysis of a Smartphone, ME Dissertation, Pukyong National University, Busan, Korea (2012).
22. D. J. Kim, J. O. Kim and H. C. Kim, *Railway J.*, **12**(3), 342 (2009).