DOI: http://dx.doi.org/10.14248/JKOSSE.2015.11.2.125
ISSN 1738-480X (Print)
ISSN 2288-3592 (Online)
Journal of the Korea Society of Systems Engineering

Improvement of FTA for Completeness, Review and Knowledge Transfer - Introducing Strategy and Context Nodes in GSN and Reason Node -

Nasa Yoshioka*, Seiko Shirasaka
Graduate School of System Design and Management Keio University, Japan

Abstract : Various methods have been used for safety and reliability as it becomes more difficult to ensure safety owing to the increasing complexity and scale of systems. This study aims at making it easier and more efficient to discuss risks and countermeasures for completeness, review, and knowledge transfer by improving methods to create fault tree analyses which focus on the GSN [1], which are among the methods used to describe assurance cases. More specifically, the purpose of this study is to incorporate strategy and context, GSN concepts, along with reason, which is a new concept, into FTA; the study focuses on three points. One point is support for the safety designer to draw a mutually exclusive and collectively exhaustive (MECE) FTA. The second is to make it easier to understand diagrams and meanings of FTA compared with the usual methods. The third is to make creating an FTA more efficient and to pass on existing know-how. Eventually, FTA can achieve completeness, review, and knowledge transfer.
An introduction is provided in the first section. Next, the methodology covered in this paper is explained in the second section. The third section describes the proposed notation method based on two proposals made in this paper. In the fourth and fifth sections, results and discussion are provided, respectively. Finally, in the sixth section, conclusions are described.

Key Words : System engineering, System Safety, System Assurance, GSN, FTA

* 교신저자 : Nasa Yoshioka, momonunsong3iikanzi@keio.jp

1. Introduction

Various methods have been used for safety and reliability as the increasing complexity and scale of systems makes it more difficult to ensure safety. Fault tree analysis (FTA) is a method for analyzing channels, causes, and probabilities of occurrences for the purpose of reliability and safety assessment through describing a top-down analysis; using a tree diagram, undesirable factors or factors that must be prevented are identified. When the hazard's causes and channel of occurrence are drawn on a diagram, engineers take into account various environments. However the current FTA descriptive method is based on people's experiences. Therefore, there is a possibility that a MECE FTA is not obtained. In addition, there is another problem concerned with FTA: it is not plain or simple enough to be easily understood by people who do not have engineering knowledge. Therefore, it takes more time for them to decipher. This may cause not only unnecessarily extended discussion time about safety design but also progression of the design without the full understanding of the project members. It is impossible to deny that some accidents occur because of such misunderstandings. These two problems have also emerged in prior studies. [8] [9]

Moreover, from the viewpoint of improving safety design, problems occur because there is no log of the concepts or thoughts of the engineers during FTA creation. These problems include, for example, cases where the FTA could not be understood by a project member who does not draw FTAs or their successors. Therefore, even if the engineer succeeds in creating an FTA perfectly, there is the possibility that it is not taken advantage of by successors or that know-how is not passed onto successors.

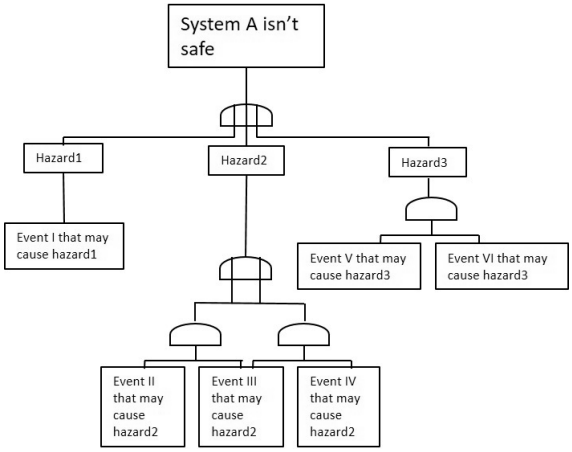
Accordingly, this study aims at improving the method used to describe FTAs by adding two Nodes of goal-structuring notation (GSN), which is a method for describing an assurance case, and one new Node. By modifying the description method, we aim at three purposes: (1) support for the safety designer to draw an MECE FTA; (2) making it easier to understand the diagrams and meaning of FTA than the usual methods used; and (3) making it more efficient to hand down the know-how for creating FTAs than it was before. Success is evaluated in terms of understandability, usability, and effectiveness through creating an FTA for an electric pot.

2. Methods

In this section, we describe the methodology covered in this paper.

2.1 FTA

An example of an FTA is shown in Figure 1. FTA is the analysis method used to determine whether a fault mode occurs through a lower item, an external event, or a combination of items and events. This structure is formed as a tree. We can analyze the processes, causes, and event probabilities by using the FTA tree [7]. The failure being analyzed has a possibility of occurring in the top event. Proceeding to lower events, there are different kinds of gates and lower events under the gates. From the lowest event the causes and effects of the



[Figure 1] An example of an FTA

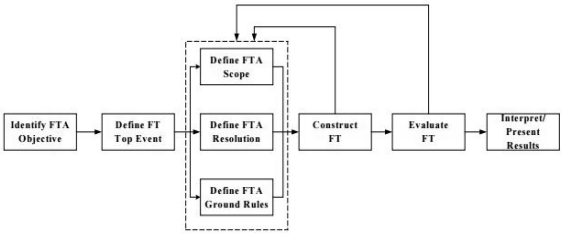
<Table 1> The role of each gate

Name	Gate structure	Role
And Gate		The upper event occurs when all the lower events occur.
Or Gate		The upper event occurs when one of the lower events occurs.

top event are identified. The possibility of the top event occurring is also evaluated. In the event, component hardware events, human errors, and any other pertinent events are described [6].

The gates, which are used when the upper event is divided, are explained below.

The steps of FTA are also defined as in Figure 2 [5].



[Figure 2] Fault tree analysis steps [6]

2.2 Assurance Case

The assurance case is the general term for the safety case or security case that assures the system to the system certifier and users by discussing the safety of the system based on the results of testing or verification. Its definition is "a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment."[2] Usually an assurance case is described in natural language and is shown in a graphical repre-sentation. There are different kinds of description methods. These are GSN, developed by the University of York, the British MOD, and claim argument evidence (CAE) developed by the City University London and Adelard.

2.3 GSN

This method is one of the assurance case description methods. GSN was developed by T.Kelly.

Four points are outlined below [2]:

· Structured notation for stakeholder agreements based on discussion and evidence.

· Management support for making an agreement with stakeholders.

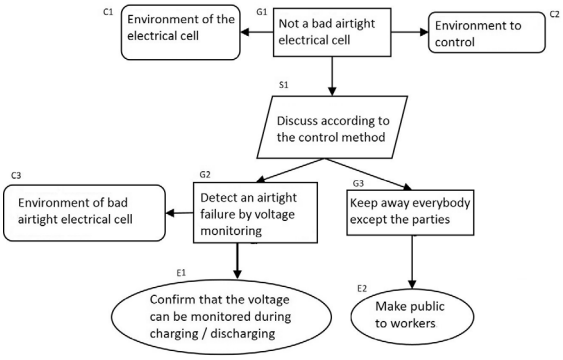
· Monitoring support to achieve the goal during operation (a monitor Node).

· Integrity checking support to describe the agreement.

A GSN consists of different kinds of Nodes which have roles and relationships with other Nodes. An example and the types of Nodes are explained below in Table 2. An example is shown in Figure 3.

<Table 2> Main description content for each Node

Node Name	Description Content
Goal	Proposition, what should be assured
Context	The background for deciding the goal
Strategy	The reasons or view point to divide goal to sub goal
Evidence	Actual way to achieve the goal
Monitor	Monitoring information of operational condition



[Figure 3] The example of GSN

3. Proposed Notation Method

In this section, we describe the details of the proposals, improvement of the FTA (which we term "IoFTA).

The purpose of this paper is three-fold: (1) make it easy to understand how to structure FTAs logically. This helps engineers and project members to discuss safety design efficiently and effectively. (2) Improve the accuracy of the safety design by improving the accuracy of FTAs. (3) Pass the skills to create FTAs down to successors or to the next generation of workers. By handing down description skills to successors, the skills needed to maintain reliability and dependability are also handed down.

Purposes (1) and (2) are achieved by Strategy Nodes and Context Nodes. (3) is achieved by Reason Nodes. Strategy, context, and Reason Nodes are explained in sections 3.1, 3.2, and 3.3, respectively.

These three Nodes should be drawn in the diagram at the same time as drawing the IoFTA. We do not recommend drawing these Nodes after creating an FTA diagram.

3.1 Strategy Nodes

A Strategy Nodes shows the viewpoint of dividing the upper event into lower events. Therefore, it is used for making it easy to understand the reasons why events are described or divided. In other words, it helps to divide the events in order to obtain a MECE FTA. The mechanisms that make FTA to be MECE are described in the following section.

FTA is usually made based on the experience of engineers. Because there is no rule how an upper event are divided into lower events, engineers try to find out lower events as much as possible. During this activity, the engineers don't have rules to find out the lower events. That's why in many cases lower events are identified from various viewpoints. By introducing "Strategy Node", the engineers can focus on one viewpoint on each step. The engineers need more steps to divide the upper event into the lower events. However, the engineers can make MECE FTA because the viewpoint works as the rule to find the lower events. In addition, it is also expected to assist the stakeholders to understand FTA.

An example of content is "classification with the original function lost." The describing rule for a Strategy Node is the same as in GSN. Therefore, the structure is a parallelogram. In

this Node, the description content includes the reasons for dividing the upper event into lower events. This means that we can understand the viewpoint for dividing the upper event into lower events.

3.2 Context Nodes

A Context Node shows the environment, specifications, or requests as constraints. When the upper event is divided into lower events, a Context Node makes the constraints for decomposing the upper event clear. This helps project members to understand any unspoken arguments. Moreover, this helps engineers who draw FTAs to remove factors that threaten MECE by making the constraints to which they should pay most attention documented and clear.

A Context Node is also used for making it easy to understand the reasons why events are described or divided. This Node supports the Strategy Node because it provides the background or environmental situation for determining the Strategy Node. This means that a Context Node explains the division of the upper event into lower events. An example of content is "the requirements for the system are…" The description rule for a Context Node is the same as in GSN. Therefore, the structure is a square with rounded corners.

3.3 Reason Nodes

A Reason Node is a completely novel Node which does not exist in GSN. The content of a Reason Node includes the concepts or thoughts of engineers during creation of an IoFTA. Consequently, a Reason Node shows the reason for the design. Therefore, Reason Nodes help successors to understand easily and contribute to the tradition of know-how. The content of a Reason Node includes the reason why the design is chosen from among alternatives. An example of the content is "even though physical damage is done, burns will not occur without functional damage." The structure of a Reason Node is a pentagon.

<Table 3> The relationship between Node types

Node Name	Content
Strategy Node	The result or viewpoint chosen from many candidates
Context Node	Constraints of the upper event
Reason Node	If several candidates which can be described in concomitant Nodes exists, the reason why one of these is selected is described

3.4 Relationships between Nodes

The relationships between strategy, context, and Reason Nodes are explained in Table 3.

In fact, when the upper event is divided into the lower events, the reason for division is described in a Strategy Node. However, in a Reason Node, the Reason described in the Strategy Node should be explained.

4. Results

4.1 Test Results

In this paper, an electric pot is used as an example for verifying the understandability, usability, and effectiveness of the proposed method. The top event is "a burn caused by the electric pot." After a trial test, an interview is performed. Participant details are shown in Table 4.

Each person draws an FTA and an IoFTA.

<Table 4> Participant details

	Person 1	Person2
Identification	SDM student	SDM student
Major	System assurance	Biological information
Design experience	Low	Low

<Table 5> Diagram labels according to participant and method

	Person 1	Person 2
FTA	Fig. 4	Fig. 6
IoFTA	Fig. 5	Fig. 7

After drawing, they respond to the interview. Incidentally, the top event of the FTA drawn by Person 1 is "Electric pot is not safe." However, the top event of the IoFTA drawn by Person 1 was changed to "Burn caused by electric pot." This occurred because the IoFTA is too large to draw, so Person 1 focused on one of the outcomes of the top event.

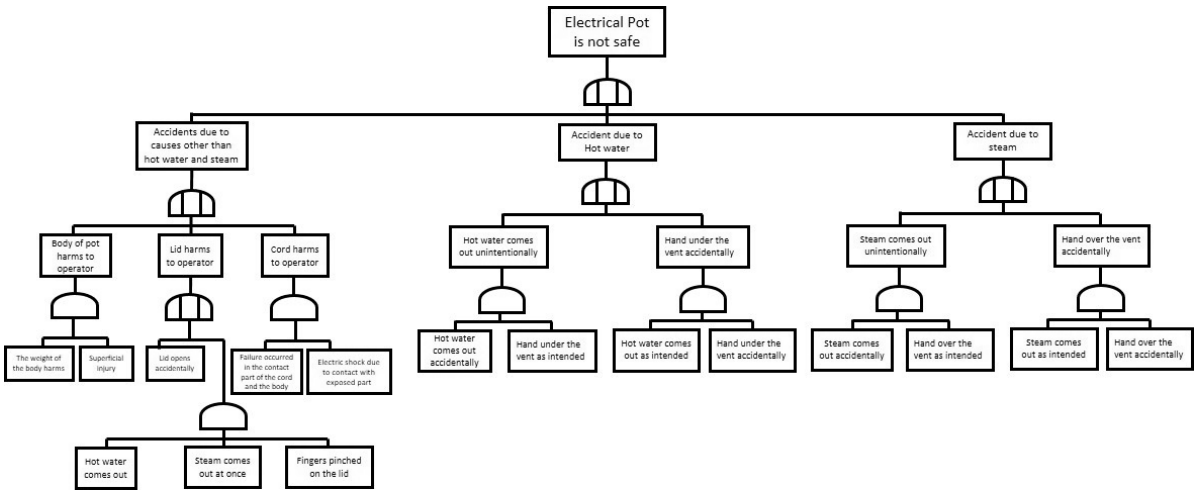
First the Nodes drawn in Figure 5 and Figure 7. Rounded rectangles have a role of Context Node. Parallelograms have a role of Strategy Node and Pentagons have a role of Reason Node.

Table 5 shows diagram labels corresponding to both participants using both methods.

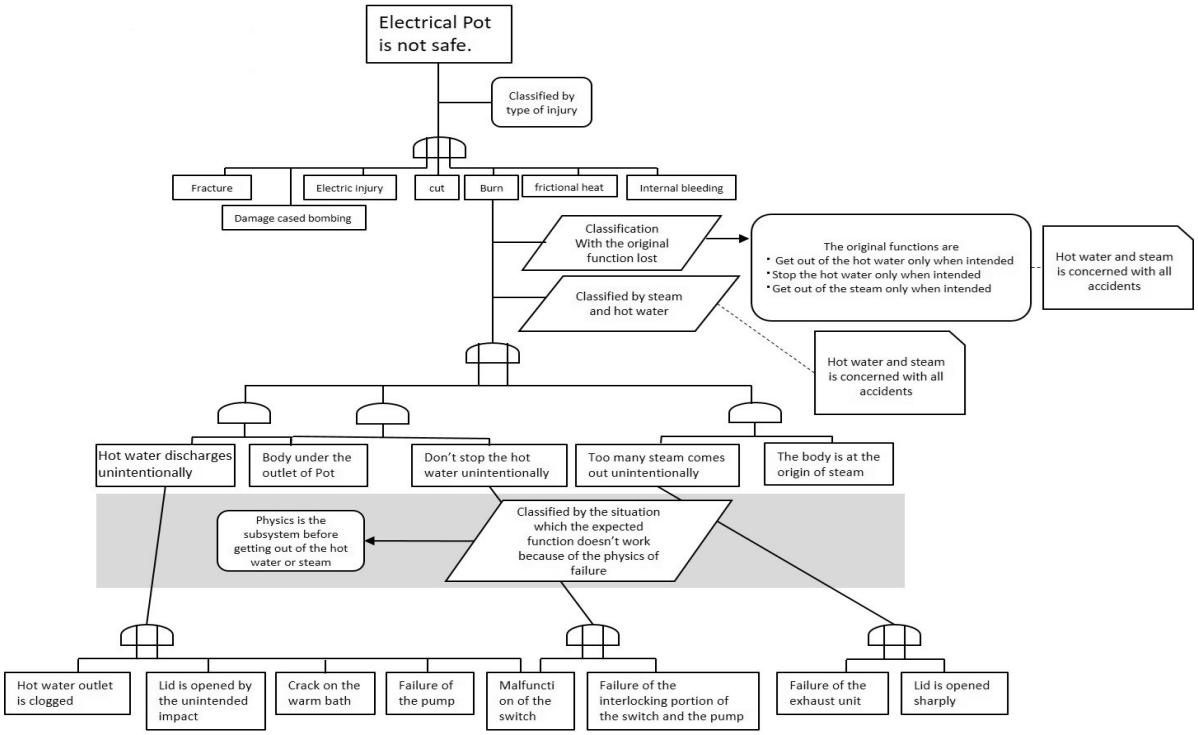
Figure 4 shows the FTA drawn by Person 1. The top goal, "electric pot is not safe," is divided into three events. These are "accident caused by hot water," "accident caused by steam," and "accident by other causes."

Figure 5 shows the IoFTA drawn by Person 1. The top goal is "burn by electric pot" and this is divided based on two viewpoints: "the original function lost" and "steam and water." The original function is explained in a Context Node. The reasons why the top goal is divided by the viewpoint "steam and hot water" is described in the Reason Node. That is, "hot water and steam are concerned in all burn accidents."

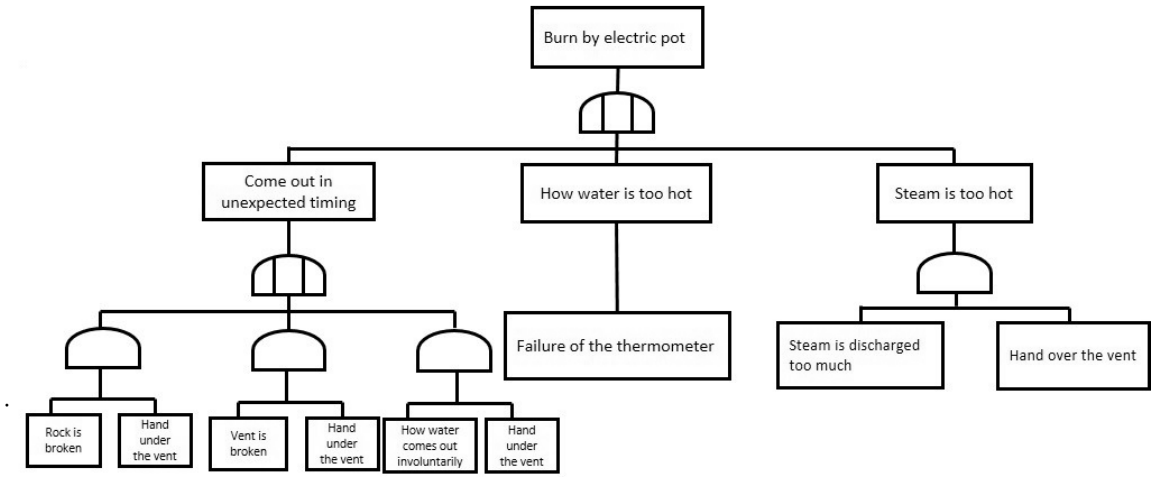
Figure 6 shows the FTA drawn by Person 2. The top goal is "burn by electric pot" and is divided into three points: "come out in unexpected timing," "hot water is too hot," and "steam is too hot." Below these are some of their



[Figure 4] FTA drawn by Person 1



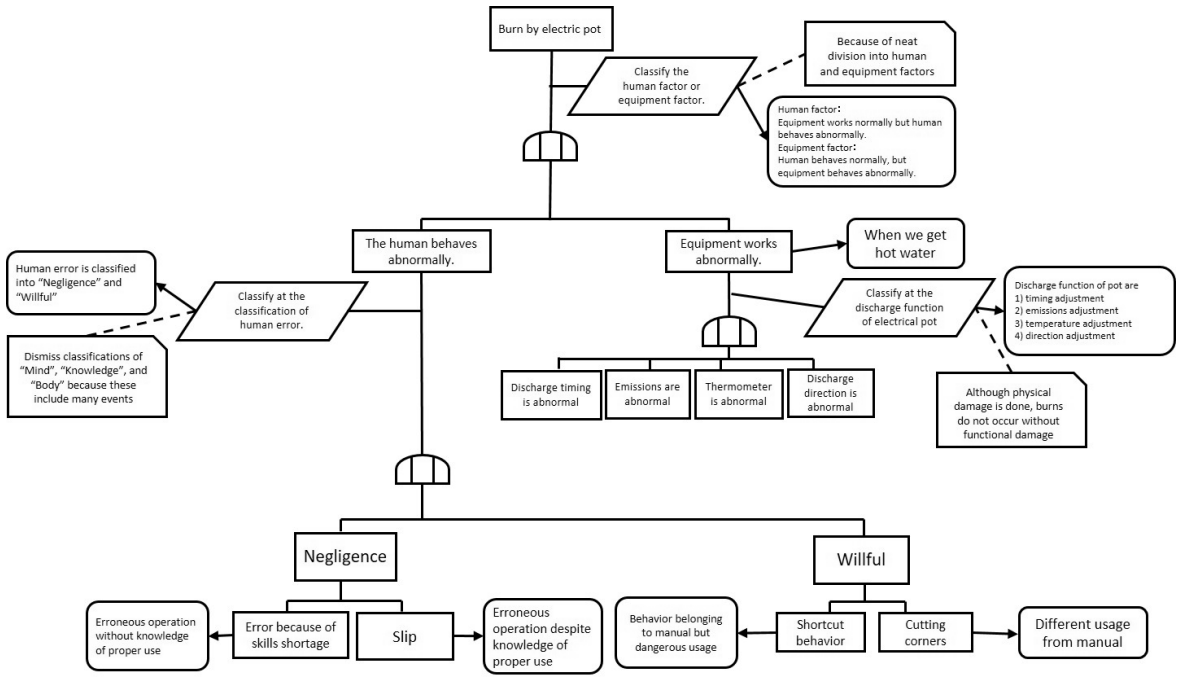
[Figure 5] IoFTA drawn by Person 1



[Figure 6] FTA drawn by Person 2

causes.

Figure 7 is the IoFTA drawn by Person 2. The top goal is "burn by electric pot," and this is divided based on one viewpoint which is "human factor or equipment factor." Therefore, the lower events are "human behaves abnormally" and "equipment behaves abnormally." In the Context Node are the details of the lower event. In the Reason Node is the reason why the top goal is divided into "human factors" and "equipment factors," which is "because of neat division into human and equipment factors." Human factors are classified based on the kind of human error. Equipment factors are classified



[Figure 7] IoFTA drawn by Person 2

based on the discharge function of the electric pot. The reason why the equipment factor is divided based on this is described in the Reason Node. This is: "even though physical damage is done, burns will not occur without functional damage." Moreover, the discharge function of the electric pot is explained in the Context Node. Moreover, the constraint of discharging the hot water is described in another Context Node.

4.2 Interview Results

The interview is done based on three points: understandability, usability, and effectiveness. Viewpoints for obtaining opinions are two-fold: (1) To describe method of IoFTA. This refers to the opinion from the experience of drawing the IoFTA. (2) Visibility, meaning the opinion from the experience of seeing or discussing the IoFTA objectively. In Table 6, each opinion is described.

5. Discussion

The discussion is based on verification in the interview.

First, understandability is discussed; in terms of the IoFTA method' s intelligibility, it was found that there are variations from person to person. Therefore, the contents enhanced clarity by confirming the described method. Using this work, the understandability of the method of IoFTA will be improved. In addition, the understandability of the content in IoFTA is better than in FTA according to results from comparison of diagrams from FTA and IoFTA.

Next discussed was usability. Both participants reported that it took a very long time to create a IoFTA relative to engineers who draw IoFTAs. It is assumed that this can be solved

<Table 6> Opinions from the participants

	Person 1			Person2		
Understandability	①	It is difficult to understand the differences between each Node.	X	①	It is easy to understand how to use these Nodes.	○
	②	It is easier to understand than FTA.	○	②	It is easy to see and understand the logic of IoFTA.	○
Usability	①	It takes a long time, so there is the possibility of stopping the use of each Node in the middle.	X	①	• It is difficult to comprehend the sentences. • It takes a longer time than FTA.	△
	②	There is the possibility of making complete design shorter.	○	②	It is easy to understand because the classification has become clear.	○
Effectiveness	①	The risk factors can be considered by MECE. (corresponding to purpose 1)	○	①	It was possible to create IoFTA with consent. (corresponding to purpose 1)	○
	②	It is easy to explain to others and to understand the design for successors because the concepts or thoughts of engineers during designing are recorded. (corresponding to purposes 2 and 3)	○	②	• Difference between the skills of veterans and rookies is decreased. • It is good for discussion because others could trace the logic of the design and there is the viewpoint of dividing the upper event. (corresponding to purposes 2 and 3)	○

in two ways. One is the clarification of the description of each Node. Another is familiarity with the description of IoFTA. On the other hand, the usability from the uses is popularity. Overall, an IoFTA actually takes a longer time than FTA to produce, but considering the safety design, total time may be shorter than with the usual (FTA) way. The reason for this is that discussion time could be curtailed because others can understand IoFTAs more easily than FTAs, and it is easy to modify the design because the reasons or viewpoints are clearer.

Finally, effectiveness is discussed. First, the proposals of this study were confirmed. The proposals are (1) support for the safety designer to draw a mutually exclusive and collectively exhaustive (MECE) FTA; (2) making it easier to understand the diagram and meaning of an FTA than by the usual methods; and (3) making it more efficient to hand down the know-how for creating FTAs than before. The effectiveness is discussed based on these three purposes. First, there are the opinions that "the lower events are considered and removed by MECE" and "IoFTA is created with acceptance" as the effectiveness measure for purpose (1). From these opinions, purpose (1) is considered to be achieved. Second, there is the opinion that "it is easy to understand the logic of an IoFTA because there is also a log of thoughts and viewpoints dividing the upper event" as validation of effectiveness for purpose (2). Based on this opinion, it is proposed that an IoFTA could be understood without technical knowledge. Therefore purpose (2) is considered to be achieved.

Finally there is the opinion that "the difference between the skill of a veteran and that of a rookie is decreased." Based on this opinion, discussion is beneficial by raising the level of understanding, and an IoFTA could contribute to handing down know-how. Therefore, purpose (3) is considered to be achieved.

From these three points, it is concluded that the accuracy of FTAs can be improved by using IoFTAs.

6. Conclusion

This study aimed at improving the method to for describing FTAs by adding two Nodes from GSN, which is a method used to describe an assurance case, and one new Node. By modifying the description method, we aim for three goals. These purposes are (1) support for the safety designer in drawing a mutually exclusive and collectively exhaustive (MECE) FTA; (2) making it easier to understand the diagram and meaning of an FTA than by the usual methods; and (3) making it more efficient to hand down the know-how for creating FTAs than it was before. This helps to understand FTAs and to transfer knowledge. Understandability, usability, and effectiveness were evaluated through the example of creating an electric pot FTA. By adding the new Nodes, including the strategy, context, and Reason Nodes, the method of creating FTAs was improved. Thereby, events are listed in accordance with MECE. In addition, engineers are able to record intricate thoughts arising during safety design. Therefore, successors can understand why the senior worker drew the FTA and can comprehend its important points. Furthermore, project members without technical knowledge can understand the logic of an IoFTA. A future step is to confirm the content of Reason Nodes more specifically. Following that, more testing should be done for verification and validation. In addition, adapting the IoFTA approach to actual hazards should be tried; then not only academic, but also practical evaluations should be performed.

Acknowledgements

We would like to thank Dr. Shirasaka and Mr. Kobayashi for advice on making the rules for new Nodes.

References

1. Tanaka, K. "Proposal of Description Rules for Assurance case Based on Systems Engineering-Realization of Visualizing Traceability and Progressive Confirmation of Quality by Utilizing System Hierarchy," Master's thesis, March 2013.
2. Kelly, T., and Weaver, R. "The Goal Structuring Notation - A Safety Argument Notation," DSN Workshop on Assurance Cases, 2004.
3. Yutaka, M. "An Introduction of Assurance Cases," Electronics, Information and Communication Engineers Technical report. KBSE, Intelligence Software Engineering, January 2014.
4. Motofumi Suzuki, Assurance Case Introduction, IPA Lecture, January 2015.
5. Stamatelatos, M. "Fault Tree Handbook with Aerospace Applications," Version 1.1, NASA Office of Safety and Mission Assurance, August 2002.

6. Vesely, W. E. “Fault Tree Handbook,” U.S. Nuclear Regulatory Commission, NUREG-0492, January 1981.
7. JIS Z8115:2000.
8. Yoshimoto, A. “FTA (Fault Tree Analysis)” and Application, Institute of Electrical Engineers Magazine, UDC 621. 004.64, pp. 35, 37, 1975.
9. Yukimachi, T. “Fault Tree Analysis and Human Factors Engineering [III]” importance measure and human error, Ergonomics Vol.13 No. 6, 0549-4974, pp. 261-270, 1977.