Application of new hazard analysis model for embedded systems

KANEMOTO Shigeru[1], and OTOMO Shunsuke[2]

1. School of computer science and engineering, The university of Aizu, Tsuruga, Ikki-machi, Aizuwakamatsu-city, Fukushima, 965-8580, Japan (kanemoto@u-aizu.ac.jp)
2. School of computer science and engineering, The university of Aizu, Tsuruga, Ikki-machi, Aizuwakamatsu-city, Fukushima, 965-8580, Japan (s1200034@u-aizu.ac.jp)

Abstract: Recently, many safety critical embedded systems are going to be involved in our daily life. Although hazards in these systems are small, their economic loss is very large by rumor propagation. So, low-cost and efficient hazard analysis methods are required. A new hazard analysis method called STAMP/STPA(Systems-Theoretic Accident Model and Process / System-Theoretic Process Analysis), which was proposed by Nancy Leveson, would be one of candidates of the above hazard analysis method. The method can analyze the hazards in complicated systems which have many interactions between human and machines. The present paper discusses its usefulness through a case study of simulated chemical plant accident model. The model is virtual one, but, has essential safety features which are equivalent to a general safety critical system including nuclear power plants. In this case study, we found some advantages of STAMP/STPA comparing the conventional hazard analysis method, FTA, which is used in nuclear power plant hazard analysis. Also, we point out the importance of diversity of hazard analysis by different methods and organizations.
Keyword: safety critical embedded systems; hazard analysis; STAMP/STPA; FTA

1 Introduction

Now, embedded systems have widely spread over our life. The embedded systems are used for various products, such as consumer electronics, service robot or highly automated automobile. The one of important features in these systems is that they have various interactions with other systems and many people, and also, are used by people who are not specially trained. So, careful design is necessary to eliminate latent hazards. However, easy and low-cost hazard analysis methodology has not yet established, since a variety of functions and interactions in the embedded system disturbs unified methodology development. Hazards are often caused by not single component failure but interaction flaw among components and human actions. So, it is not easy to analyze the complicated system hazards by a conventional method.

On the other hand, the nuclear power plant safety control system could be also regarded as one of large embedded systems. Here, it was thought that the safety evaluation procedures were established. But, we know these procedures were insufficient after Fukushima 3.11 accident.

According to these backgrounds, Nancy Leveson proposed a new accident analysis model called STAMP(Systems-Theoretic Accident Model and Process) to analyze hazards of complicated systems which have many interactions between human and machines[1]. STAMP consists of two concrete methodologies: One is STPA(System-Theoretic Process Analysis) to identify accident scenarios and to provide guidance to prevent the hazards in the design stage. The other is CAST(Causal Analysis based on STAMP) to fully understand why the accident occurred and how to prevent similar losses in the future. Some practical examples are shown in MIT web site[2].

The present paper tries to evaluate STAMP usefulness for safety assessment of safety critical embedded systems. For this, we utilize a simple chemical plant simulator made by MATLAB/SIMULINK[3]. This simulator controls the tank water at a constant level, and also, has the emergency drain control sub-system to prevent water overflow. We analyze the hazards and their causes of the system by using STAMP/STPA. The results

Received date: June 5, 2015
(Revised date: June 28, 2015)

are compared with the conventional FTA method. Although this model seems too simple, we think the essential safety feature could be discussed by using this model.

Through the discussion of safety evaluation for the virtual safety critical system, we can discuss merits and demerits of the STAMP and conventional methods. Also, the conventional safety evaluation in nuclear power plant industry will be discussed in comparison with STAMP. Although the safety evaluation of nuclear power plants seems to be established, we could expect that new aspects will be revealed by these another approaches. Furthermore, these discussion will be useful for the safety evaluation of various kinds of embedded systems which are going to be involved in our daily life.

2 STAMP/STPA

The STAMP accident model is based on three basic constructs: safety constraints, hierarchical safety control structures, and process models. Safety constraints are the most important concept of STAMP and must be firstly identified and be enforced. By using hierarchical safety control structures, the safety constraints at a higher level can control lower level behaviors. Process models are important for constructing the hierarchical control structures. We need four conditions to control safety process: a goal, action condition, observability condition, and model condition. The goal is the safety constraints. The action condition is implemented in the control channels. The observability condition is embodied in the feedback channels. The model condition is required for controlling process effectively. Figure 1 shows an example of safety constraint and control structure diagram for the power control system[1].

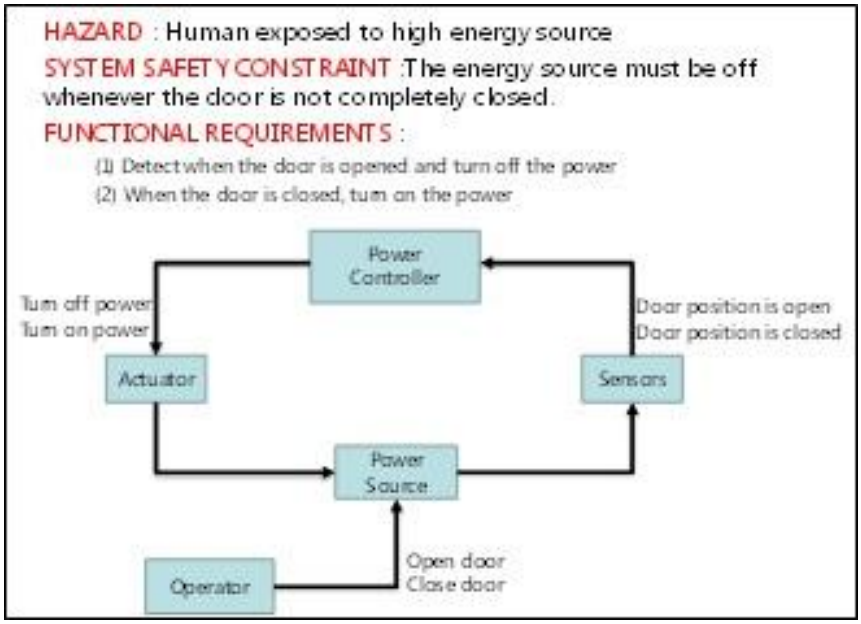

Fig. 1 Safety constraint and control structure diagram for power control system.

STPA is hazard analysis based on the STAMP causality model. Goals for STPA are to identify accident scenarios of the whole process, to provide guidance for assuring safety completeness, and to guide the design process for keeping the safety in the top level design stage. STPA consists of the following four steps: In step-0, we need to identify hazard, system safety constraints, and functional requirements. We also need to identify the hierarchy control structures for the system as a precondition. Step-1 is to assess the safety control structures to determine the potential for leading to a hazard. We find hazards using the following four guidewords of unsafe control actions (UCA) which implies unsafe control actions to investigate the hazards of the system:

1. A control action required for safety is not provided or is not followed.

2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied too long

These four guidewords would be the most important ideas of STPA. In the safety evaluation of nuclear power plants, the trigger event such as earthquake or tsunami is first assumed. And, succeeding events, such as reactor scram or emergency core cooling, are analyzed by ETA (event tree analysis). The each subsystem's fault probability is calculated by FTA (fault tree analysis). Comparing these procedures, STAMP/STPA unsafe control actions seems to be different. Instead, it similar to HAZOP (Hazard and operability study) developed in the chemical industry[4]. Here, the deviation of process signals is first assumed according to guidewords, and, its causes and effects are identified. STAMP/STPA is beneficial than these conventional methods since the top goal of the safety constraint can be satisfied by just thinking the four kinds of UCAs. These UCA guidewords are practical and easily understandable.

In step-2, we identify the causal scenarios of the target system leading to UCAs that violate the component safety constraints by using the following six hazard causal factors (HCF) guidewords:

1. Unsafe inputs,
2. Unsafe control algorithms,
3. Inconsistent, incomplete, or incorrect process model,
4. Inadequate feedback,
5. Flaw of actuators and controlled processes,
6. Out-of-range disturbance, conflict control actions, or environment.

The detailed guidewords mapped to the control structure feedback loop are shown in Fig. 2. In this figure, the causes which lead to UCAs can be list up thoroughly and easily. The relationships among hazards, UCAs and HCFs are summarized by the tree shaped structure shown in Fig. 3.

In final step-3 of STPA, safety constraints for lower level components are made in order to control or eliminate corresponding HCFs. The concrete example will be shown later.

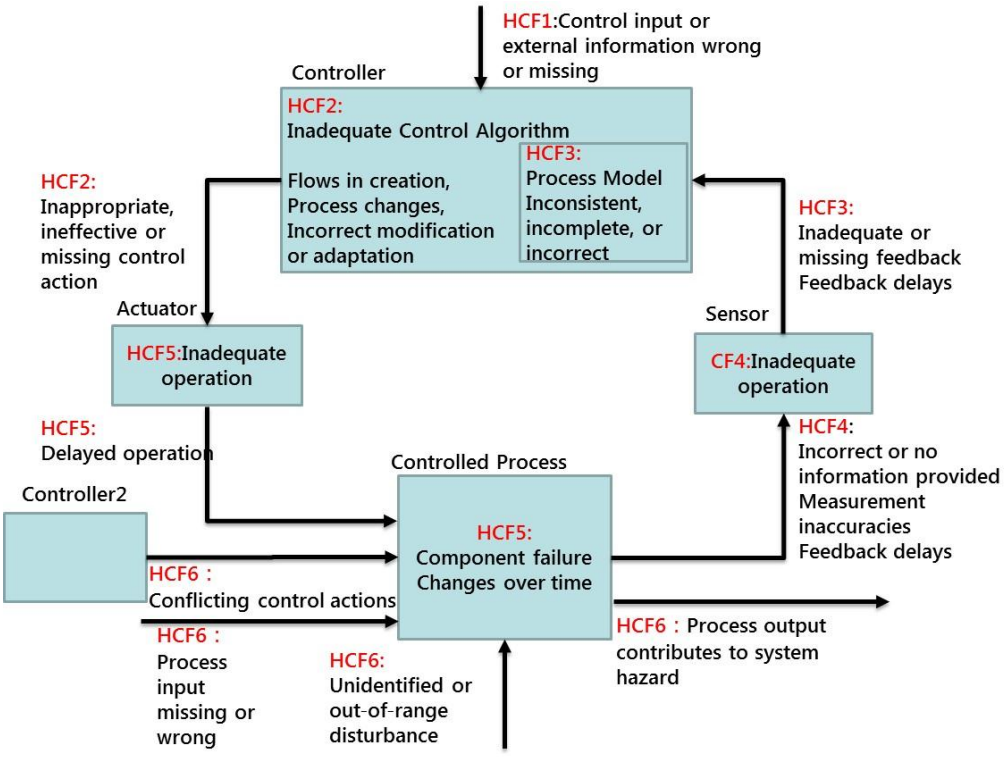

Fig. 2 General hazard causal factor guidewords for considering causal scenarios.

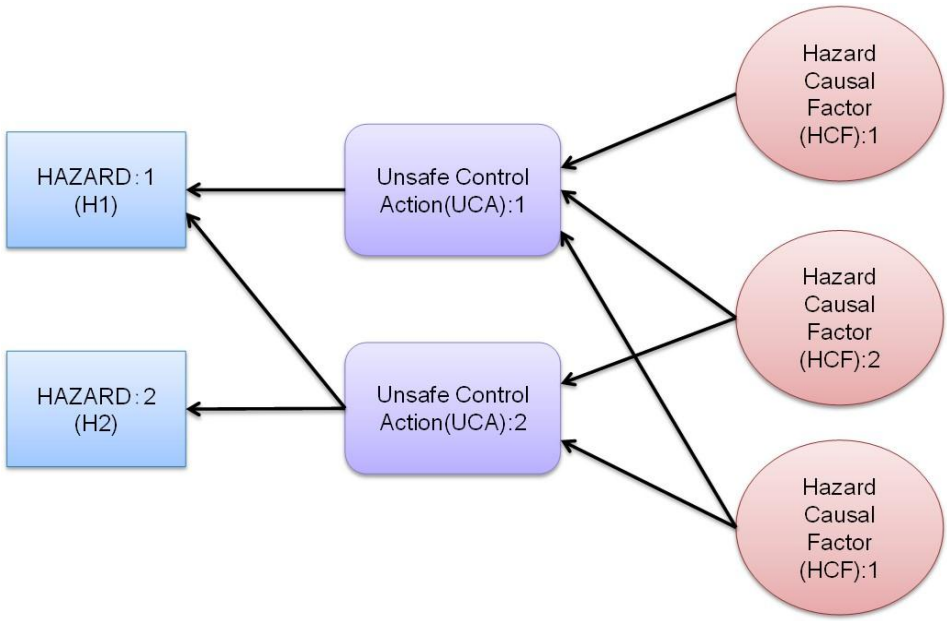

Fig. 3 Tree structure of hazards, unsafe control actions and hazard causal factors.

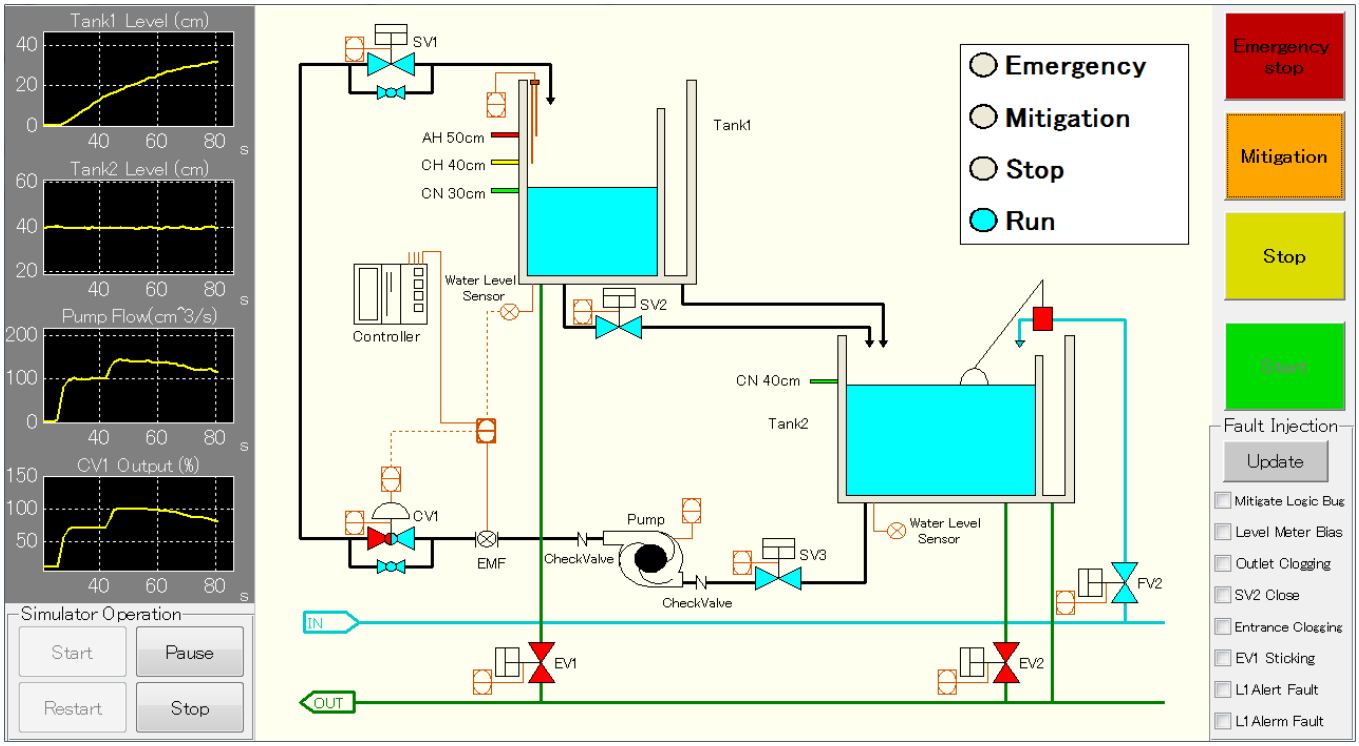

Fig 4. Overview of chemical plant model.

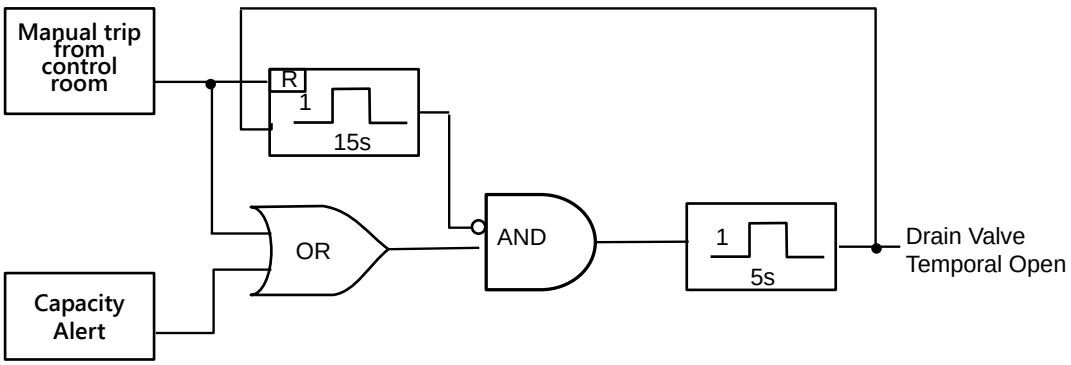

Fig. 5 Mitigation system logic using emergency drain valve.

3 Case Study

3.1 Chemical plant model

In order to verify the usefulness of STAMP/STPA hazard evaluation, we investigate a simple virtual test case using the chemical plant simulator, which was developed by IPA/SEC working group[3]. The simulators are made by MATLAB/SIMULINK to make the control algorithms easily understandable. The chemical plant simulator shown in Fig. 4 has tanks, valves, sensors and a control system including emergency safety control logic. The water of Tank-2 is drawn up by the pump and pour into Tank-1. The water level of Tank-1 is controlled at a constant level by PID controller and control valve, CV1. Here, the main hazard of this system is assumed the overflow from Tank-1. In order to avoid the overflow, the emergency drain valve, EV1, is equipped and automatically opened when the Tank-1 level exceeds an alarm set point. The emergency mitigation control logic is also equipped to suppress the water level before reaching to the alarm level[5]. Here, EV1 is open for just 5 seconds when the Tank-1 level exceeds an alert set point, and, prohibit additional operation for next 10 seconds. This mitigation logic is shown in Fig. 5. In order to simulate the interactions between operator and machine control, the operator can directly open EV1 by pushing the buttons of emergency stop or mitigation which are shown in the top right of the screen of Fig. 4. As shown in Fig. 5, the mitigation operation by the operator is always prioritized to the automated mitigation action.

In the simulator, various kinds of failures are also embedded such as sensor drift, pipe clogging, drain valve stuck or inappropriate control logic, which can be inserted by checking the buttons in lower right screen of Fig. 4.

The main purpose of this simulator is to use it for various V&V procedures examination in the software development. Especially, in the validation procedure, hazard evaluation and its preventive design is one of important issues for safety critical systems. Since the essential feature of the present simulator's safety protection logic is the same as general industry's safety critical systems including nuclear power plants, investigations of hazard evaluation procedures using the present simulator is useful especially for educational or training points of view for safety engineers.

3.2 STAMP/STPA results

In the present simulator, the main hazard is assumed as the overflow from Tank-1. As for a precondition of this hazard, the rise of Tank-1 water level is also considered as hazard. The mitigation subsystem is not considered here, since it is a support system and not directly related to the safety function. Hence, system safety constraints in the STAMP model should be:

- The water in Tank-1 must not be beyond dangerous water level
- The water level in Tank-1 must not become higher than a set point.

According to these safety constraints, the hierarchy control structure for the chemical plant can be made in Fig. 6. Then, UCAs for the overflow can be analyzed according to four guidewords in horizontal cells of Table 1. The vertical cells show a control action, that is, the emergency drain valve opening. Here, three UCAs labelled by A-C are identified. The scenario how UCA breaks the safety constraint should be considered based on the process model. This depends on human domain knowledge. By the same way, six UCAs labelled G-I for the water level rise can be identified in Table 2. Here, two control actions, level increase and decrease, are used.

In the next step, hazard causal factors for the above UCAs are analyzed based on six HCF guidewords shown in Fig. 2. For each UCA, HCFs have to be extracted and written on the safety structure diagram. Obtained all HCFs are unified and shown in Figs. 7 and 8, for the overflow and water level rise, respectively. Here, alphabets indicate the corresponding UCA index, and, numbers indicate HCF guideword index. These symbols which show the guideword index are necessary to avoid inconsistency in multiple examination processes of STPA.

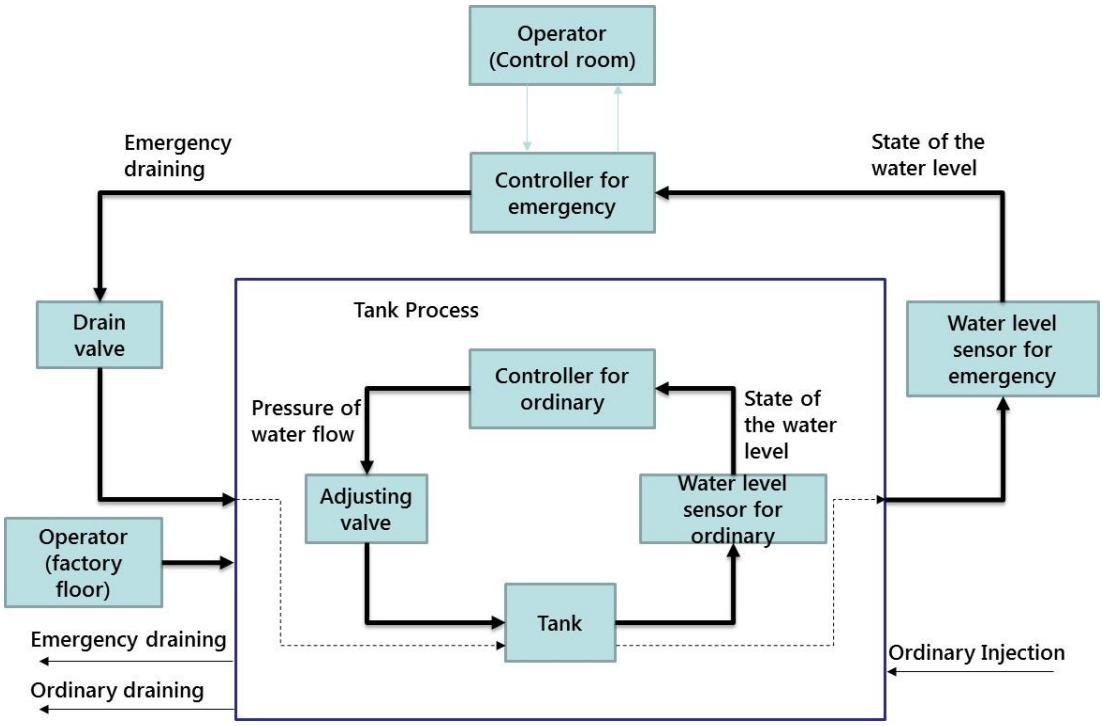

Fig 6. Control structure for chemical plant model.

Table 1 Identifying UCAs of overflow by using four guidewords

Control Action	Not Providing Caused Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
Opening the emergency draining valve	UCA-A Drainage is not done in emergency	Not hazardous (Water level lowers)	UCA-B Even if water level rises, drainage does not begin (delay)	UCA-C Drainage is canceled though water level does not lowers enough

Table 2 Identifying UCAs of water level rise by using four guidewords

Control Action	Not Providing Caused Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
Increasing the water flow	Not hazardous (Water level lowers)	UCA-D Water flow increases when water level is high	UCA-E Water flow increase before water level lowers	UCA-F Water flow remains increasing after water level becomes enough
Decreasing the water flow	UCA-G Water flow does not decrease when water level is high	Not hazardous (Water level lowers)	UCA-H Time after water level becomes high before water flow decrease is long	UCA-I Water flow returns to original pressure though water level does not lowers enough

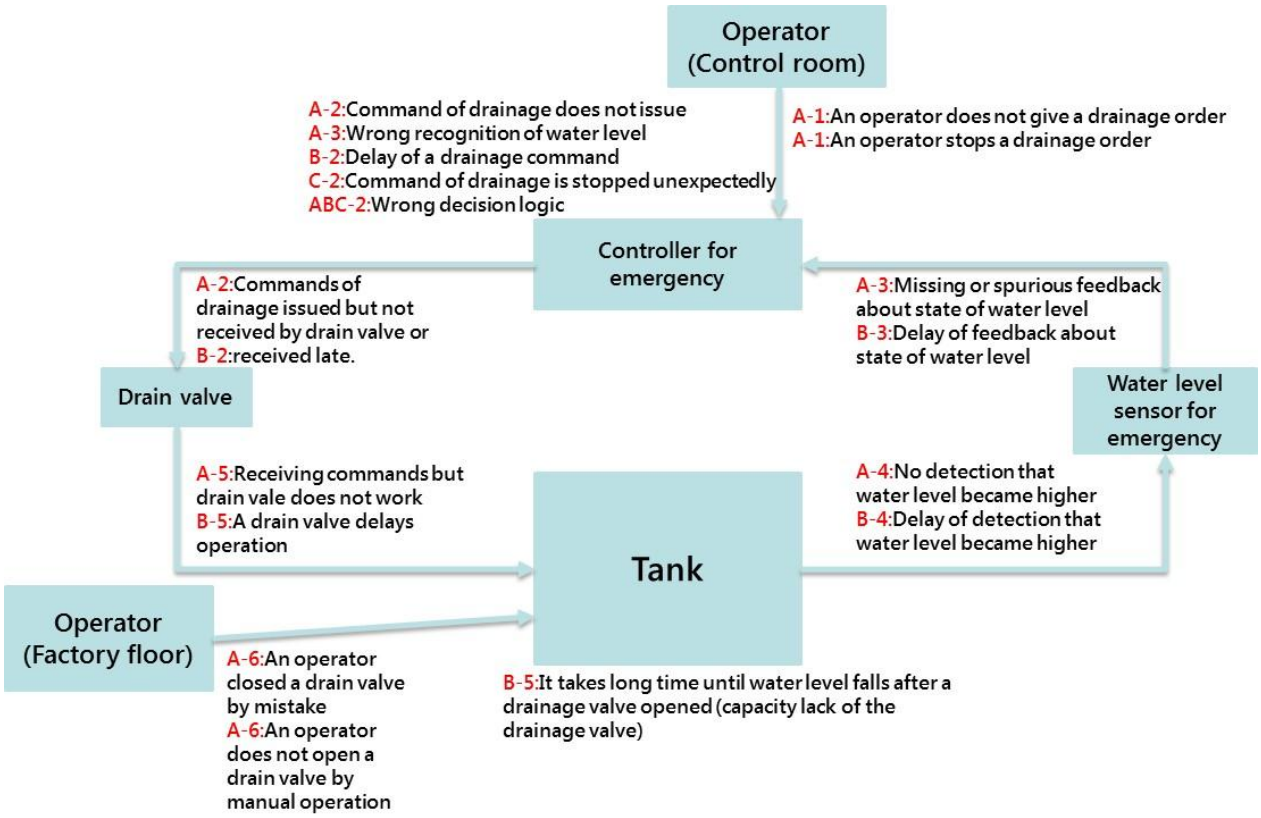

Fig. 7 Hazard causal factor (HCF) for UCAs of overflow from Tank-1.

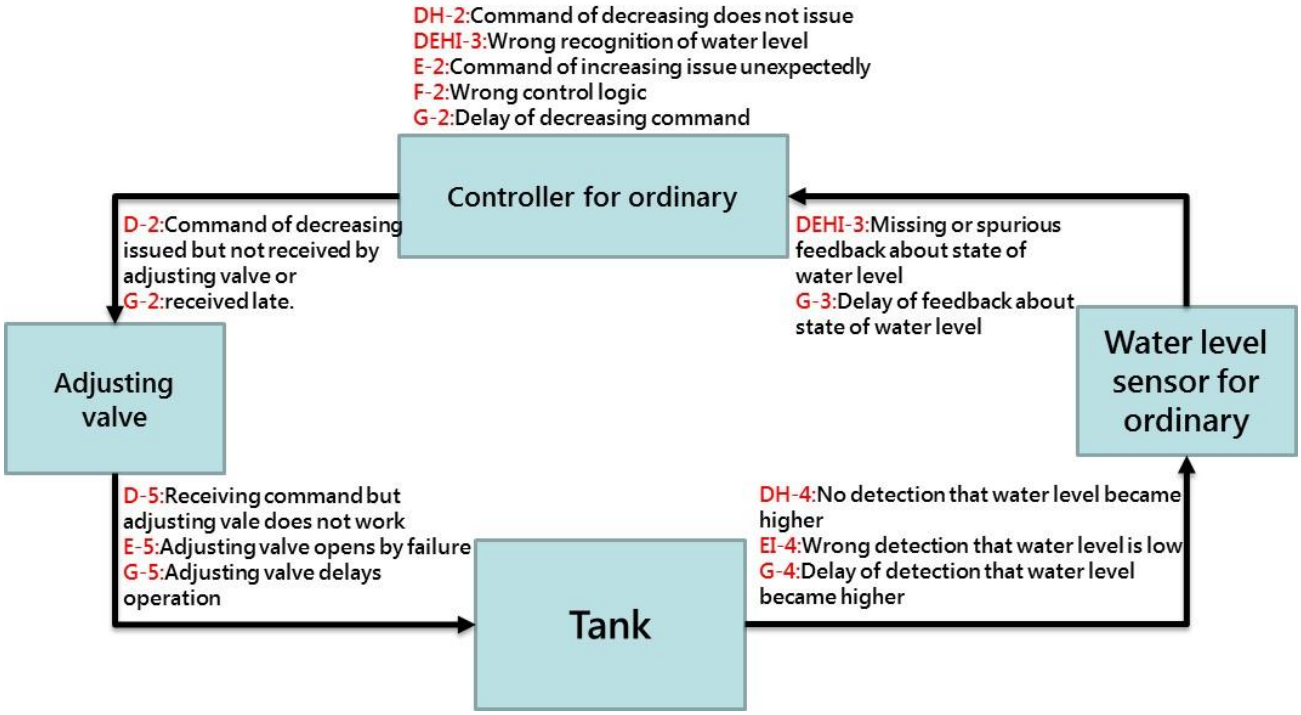

Fig. 8 Hazard causal factor (HCF) for UCAs of water level rise in Tank-1.

In the final step of STPA, safety constraints for lower level components are identified in order to control or eliminate corresponding HCFs. Table 3 and 4 shows the examples of component safety constraints for the overflow and water level rise.

Table 3 Identified HCFs of overflow and corresponding safety constraints for lower level components

CF-No.	Hazard Causal Factor	Component Safety Constraint
A-2	Command of drainage does not issue	Review conditions to give commands and issue them when they are necessary
A-3	Wrong recognition of water level	Don't get wrong detections of water level
A-2	Commands of drainage issued but not received by drain valve	Confirm the communication between the controller and the drain valve
A-5	Receiving commands but drain vale does not work	Maintain the drain valve exactly
A-3	Missing or spurious feedback about state of water level	Check whether feedback comes exactly
A-4	No detection that water level became higher	Maintain the sensor and detect water level surely
B-2	Delay of a drainage command	Do not mistake timing to give commands
B-2	Commands of drainage issued but received late.	Do not delay communication
B-5	A drain valve delays operation	Maintain the drain valve and take the time of operation into consideration
B-3	Delay of feedback about state of water level	Do not delay feedback
B-4	Delay of detection that water level became higher	Review timing to detect
B-5	It takes time until water level falls after a drainage valve opened (capacity lack of the drainage valve)	Review structure or take a delay of the time into consideration
C-2	Command of drainage is stopped unexpectedly	Review algorithm so that it is not stopped
ABC-2	Wrong decision logic	Review design logic
A-1	An operator does not give a drainage order	Give a drainage command in emergency
A-1	An operator stops a drainage order	Prevent emergency drain from being stopped during operation
A-6	An operator closed a drain valve by mistake	Prevent emergency drain valve from being closed during drainage
A-6	An operator does not open a drain valve by manual operation	Open drain valve by manual in emergency

Table 4 Identified HCFs of water level rise and corresponding safety constraints for lower level components

CF-No.	Hazard Causal Factor	Component Safety Constraint
DH-2	Command of decreasing does not issue	Review conditions to give commands and issue them when they are necessary
DEHI-3	Wrong recognition of water level	Don't get wrong detections of water level
D-2	Command of decreasing issued but not received by adjusting valve	Confirm the communication between the controller and the adjusting valve
D-5	Receiving command but Adjusting vale does not work	Maintain the adjusting valve exactly
DEHI-3	Missing or spurious feedback about state of water level	Check whether feedback comes exactly
DH-4	No detection that water level became higher	Maintain the sensor and detect water level surely
E-2	Command of increasing issue unexpectedly	Review conditions to give commands and do not issue them by mistake
E-5	Adjusting valve opens by failure	Maintain the adjusting valve exactly
EH-4	Wrong detection that water level is low	Maintain the sensor and detect water level surely
F-2	Wrong control logic	Verify it in advance properly
G-2	Delay of decreasing command	Do not mistake timing to give commands
G-2	Command of decreasing issued but received late.	Do not delay communication
G-5	Adjusting valve delays operation	Maintain the adjusting valve and take the time of operation into consideration
G-3	Delay of feedback about state of water level	Do not delay feedback
G-4	Delay of detection that water level became higher	Review timing to detect

3.3 Comparison with FTA

The above STPA results can be compared with the conventional typical hazard analysis method, FTA, to verify effectiveness of STAMP/STPA. Figure 9 is the result of FTA. Here, eight hazard causes are extracted by FTA. Table 5 and 6 is the comparison between FTA and HCFs extracted by STAMP/STPA for two hazards, the overflow and water level rise. Here, we can see causal factors of FTA are simple and clear, but, those of STPA are more detailed and STPA can detect other causal factors which are omitted by FTA. In particular, hazard causal factors related to communication functions are remarkably different.

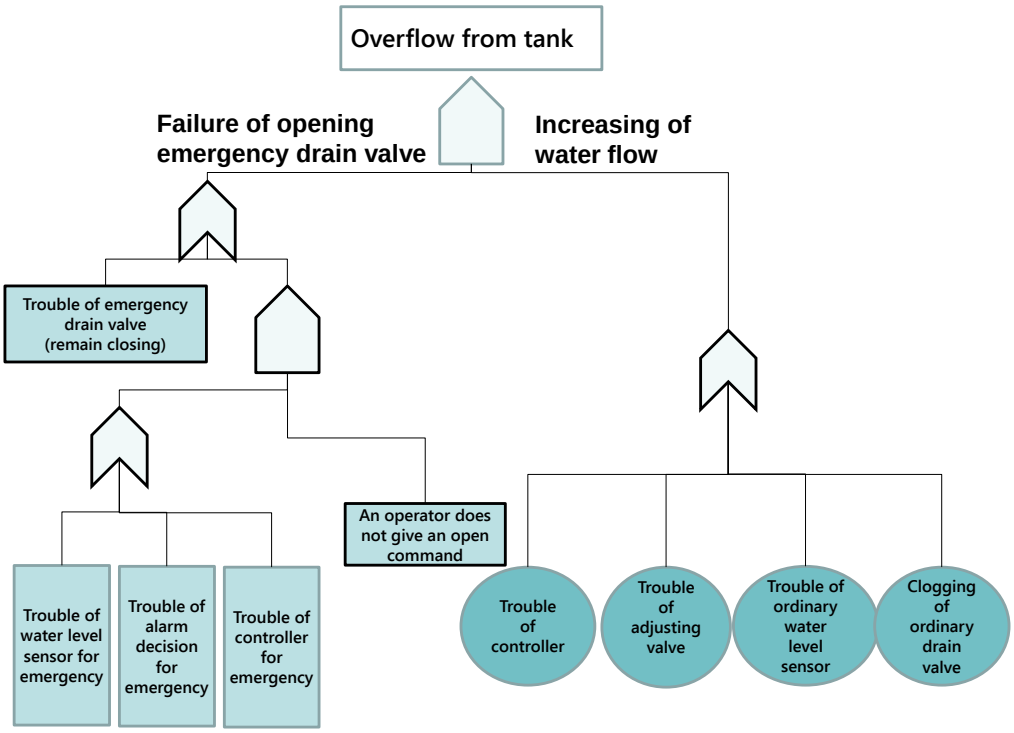

Fig. 9. FTA of overflow from tank-1.

Table 5 Comparison with FTA and STAMP/STPA hazard causal factors of overflow

Causal Factors of FTA	Causal Factors of STPA
Trouble of water level sensor for emergency	A-4:No detection that water level became higher B-4:Delay of detection that water level became higher
Trouble of alarm decision for emergency	ABC-2:Wrong decision logic
Trouble of controller for emergency	A-2:Command of drainage does not issue A-3:Wrong recognition of water level B-2:Delay of a drainage command C-2:Command of drainage is stopped unexpectedly
An operator does not give an open command	A-1:An operator does not give a drainage order A-1:An operator stops a drainage order A-6:An operator closed a drain valve by mistake A-6:An operator does not open a drain valve by manual operation
Trouble of emergency drain valve (remain closing)	A-5:Receiving commands but drain vale does not work B-5:A drain valve delays operation B-5:It takes long time until water level falls after a drainage valve opened (capacity lack of the drainage valve)
The rest (Trouble of communication)	A-2:Commands of drainage issued but not received by drain valve B-2:Command of decreasing issued but received late. A-3:Missing or spurious feedback about state of water level B-3:Delay of feedback about state of water level

Table 6 Comparison with FTA and STAMP/STPA hazard causal factors of water level rise

Causal Factors of FTA	Causal Factors of STPA
Trouble of controller	DH-2:Command of decreasing does not issue DEHI-3:Wrong recognition of water level E-2:Command of increasing issue unexpectedly F-2:Wrong control logic G-2:Delay of decreasing command
Trouble of adjusting valve	D-5:Receiving command but adjusting vale does not work E-5:Adjusting valve opens by failure G-5:Adjusting valve delays operation
Trouble of ordinary water level sensor	DH-4:No detection that water level became higher EH-4:Wrong detection that water level is low G-4:Delay of detection that water level became higher
Clogging of ordinary drain valve	Assumed as precondition failure
The rest (Trouble of communication)	D-2:Command of decreasing issued but not received by adjusting valve G-2:Command of decreasing issued but received late. DEHI-3:Missing or spurious feedback about state of water level G-3:Delay of feedback about state of water level

3.3 Discussions for hazard evaluation

After 3.11 Fukushima nuclear plant accident, it was often said that we should assume unexpected events in accident analysis. But, this is a little bit strange logically, and also, hindsight is often included in the discussion. Rather, we should deepen an argument about who should expect critical events, since we will have a different result depending on the viewpoint of hazard analysis. In other words, we should assume expected events from different viewpoints. Namely, an independent hazard evaluation scheme is important. Here, independent means diversity of both hazard evaluation methods and organizations. Conventionally, the methods such as FTA, ETA, FMEA or HAZOP are used for the hazard evaluation. But, STAMP/STPA could be another candidate of hazard evaluation of nuclear power plants.

This kind discussion is also important for the safety critical embedded systems which are used by general consumers. Even though hazards in these systems would be much smaller than nuclear power plants, their economic loss due to an accident is usually very large by rumor propagation. So, hazard analysis in a design stage is important. Also, accountability after an accident is also important to prevent rumor.

STAMP/STPA could be one of candidates for independent hazard evaluation methods in the above discussion, since it requires less domain knowledge for the target system than conventional methods due to its excellent guidewords. STAMP defines the safety constraints in the top level, and, succeeding analysis procedures are logically clear and easily understood by outsider independent people. Also, it is easy to list up possible hazard causal factors based on the control structure diagram and guidewords. As shown in the above case study, STPA gives us equivalent and more detailed results comparing with FTA. These features suggest the usefulness of STAMP/STPA analysis in independent hazard evaluation and accountability of the system design.

4 Conclusion

For safety critical embedded systems used by general consumers, easy and low-cost hazard evaluation is very important. Also, product liability and accountability are very important. Hence, hazard preventive design based on STAMP/STPA would be very useful for them.

In the present paper, we found that STAMP/STPA has some advantages of hazard analysis via the simple chemical plant model hazard analysis. In particular, it is easy to use than the conventional hazard analysis and can extract more detailed hazard causes. Also, less domain knowledge is required in STAMP/STPA application by utilizing guidewords given by STPA. This feature helps the STAMP/STPA usage in

independent hazard analysis activity. Furthermore, STAMP/STPA can be used to deduce component safety constraints for preventive safety design.

Acknowledgement

A part of the work herein was done in IPA/SEC working group activity (Software Reliability Enhancement Promotion Committee / System Fault Diagnosis WG). The authors thank the useful discussion among WG members.

References

[1] LEVESON, N.G.: Engineering a Safer World, The MIT Press, 2012.

[2] 2014 STAMP Workshop Presentations: http://psas.scripts.mit.edu/home/2014-stamp-workshop-presentations/

[3] http://www.ipa.go.jp/sec/reports/20150331_2.html (in Japanese)

[4] LAWLEY, H.G.: Operability Studies and Hazard Analysis, Chemical Engineering Progress, 70-4, pp. 45-56, 1974.

[5] BJORKMAN, K., *et al.*: Verification of Safety Logic Designs by Model Checking, Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT 2009, Knoxville, Tennessee, April 5-9, 2009.