Application of System-Theoretic Process Analysis to Engineered Safety Features-Component Control System

Dong-Ah Lee[a], Jang-Soo Lee[b], Se-Woo Cheon[c], and Junbeom Yoo[d]
[a,d]Division of Computer Science and Engineering, Konkuk University 1 Hwayang-dong, Gwangjin-gu, Seoul, 143-701, Republic of Korea
[b,c]Korea Atomic Energy Research Institute, 150 Deokjin, Yuseong Daejeon, 305-335, Republic of Korea
[a,d]{ldalove, jbyoo}@konkuk.ac.kr, [b,c]{jslee,swchoen}@kaeri.re.kr

Abstract

Recent developments in safety-critical systems have heightened the need for hazard analysis because results of their accidents have become more and more serious. Traditional hazard analysis techniques, such as fault tree analysis (FTA) or failure mode and effects analysis (FMEA), have been extensively used for decades. However, traditional techniques are not suitable for modern systems which are more complex, software-intensive, socio-technical systems. System-Theoretic Process Analysis (STPA) is a new hazard analysis technique based on System-Theoretic Accident Model and Processes (STAMP) which is a new causality model developed by Nancy G. Leveson. It aims at identifying accident scenarios that encompass the entire accident process. This paper introduces application of the STPA to Engineered Safety Features-Component Control System (ESF-CCS) which prevents radiation leakage from a nuclear reactor. The application performed three functions of the ESF-CCS which has 8 functions. Results of this research show that analysts have a different view about causes of accidents. Furthermore, the view lets the analysts focus on identifying different causal factors from what other hazard analysis techniques identify.

1. Introduction

Recent developments in safety-critical systems, such as nuclear power plants, aerospace systems, and railway transport systems, have heightened the need for hazard analysis because results of their accidents have become more and more serious. For instance, an accident at the Fukushima Daiichi Nuclear Power Plant (NPP) exposed a number of people to radioactivity, leaked radioactive material into the air and the sea, and declared an evacuation zone within a 20 km radius of the plant [1]. Another accident occurred on the Jiaoji Railway in China caused 72 fatalities and 416 injuries because of train collision [2].

Various hazard analysis techniques, such as Fault Tree Analysis (FTA), Failure Modes and Effects analysis (FMEA), Hazards and Operability Analysis (HAZOP), etc., have been proposed and are in use to eliminate or mitigate hazards [3]. Many of the techniques were developed fifty years ago. These traditional techniques are not suitable for modern systems which are more complex, software-intensive, socio-technical systems [4].

System-Theoretic Process Analysis (STPA) is a new hazard analysis technique based on System-Theoretic Accident Model and Processes (STAMP) which is a new causality model developed by Nancy G. Leveson. The STPA's goal is to identify accident scenarios that encompass the entire accident process, not just the electromechanical components. The technique provides systematic guidance to the users in getting good results.

This paper introduces application of the STPA to Engineered Safety Features-Components Control System (ESF-CCS) developed as a part of Korea Nuclear Instrumentation & Control System (KNICS) [5] R&D Center project. The ESF-CCS controls all kinds of safety related components including equipment for engineered safety features. Failures of the ESF-CCS may results serious problems such as leak of radioactive material from a reactor. Although various hazard analysis techniques are applied to the system, the application of the STAP provides analysts with a new angle on the hazard analysis.

This paper is organized as follows. It first gives a brief overview of the STPA and the target system, the ESF-CCS, in Section 2. Section 3 describes how we apply the STPA to the ESF-CCS and what results are. Section 4 shares discussion with experts about the application, and we conclude the paper in Section 5.

2. Background

2.1 STAMP/STPA

System-Theoretic Accident Model and Process (STAMP) is a new accident causality model based on three concepts—safety constraints, a hierarchical safety control structure, and process models—along with basic systems theory concepts. The safety constraint is the most basic concept, which causes events leading to losses where it was not successfully enforced. In STAMP, systems are viewed as hierarchical structures which higher levels control processes at lower levels and the lower levels feedback to the higher levels. <Figure 1> shows a generalized hierarchical safety control structure, which has two basic structure—one for system development and one for system operation—with interaction between them. The controls enforce the safety constraints for which the higher levels are responsible. The process model is conditions to control a process.

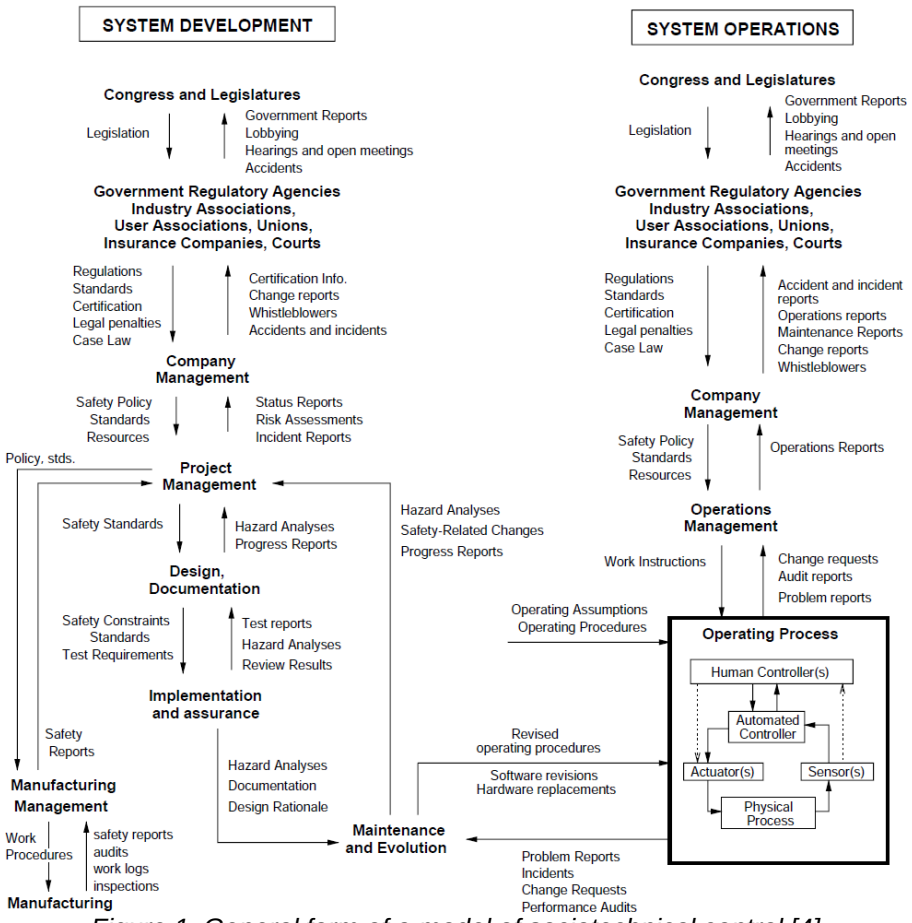


Figure 1. General form of a model of sociotechnical control [4]

System-Theoretic Process and Analysis (STPA) is a new approach to hazard analysis, based on the STAMP causality model. Application of the STPA follows a process below:

1. Identify hazardous states of the system.
2. Develop the control structure of the system.
3. (*STPA Step 1*) Identify the potential for inadequate control of the system that could lead to a hazardous state.
4. (*STPA Step 2*) Determine how each potentially hazardous control action identified in step 1 could occur.

The STPA is not a technique to identify hazards of the system, but causations of the hazards. The hazardous state of the system, therefore, should be identified and the control structure should be developed before the STPA begins. A functional control diagram and the requirements, system hazards and the safety constraints and safety requirements for the system are available for the identification and the development.

The STPA identifies inadequate control actions, using the hazardous states and the control structure, at the first step of the STPA. The inadequate control actions which are leading to a hazard are identified in four ways as follows:

1. *A control action required for safety is not provided or is not followed.*
2. *An unsafe control action is provided that leads to hazard.*
3. *A potential 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 (for a continuous or nondiscrete control action).*

After four kinds of unsafe control actions are identified, the STPA identifies the causal factors leading to the unsafe control actions that violate the safety constraints at STPA Step 2. <Figure 2> shows the general causal factors that there are four types of flaws—(1) a control input or external information wrong or missing; (2) an inadequate control algorithm; (3) a process model and a sensor failure; and (4) a controlled process failure and an actuator failure.

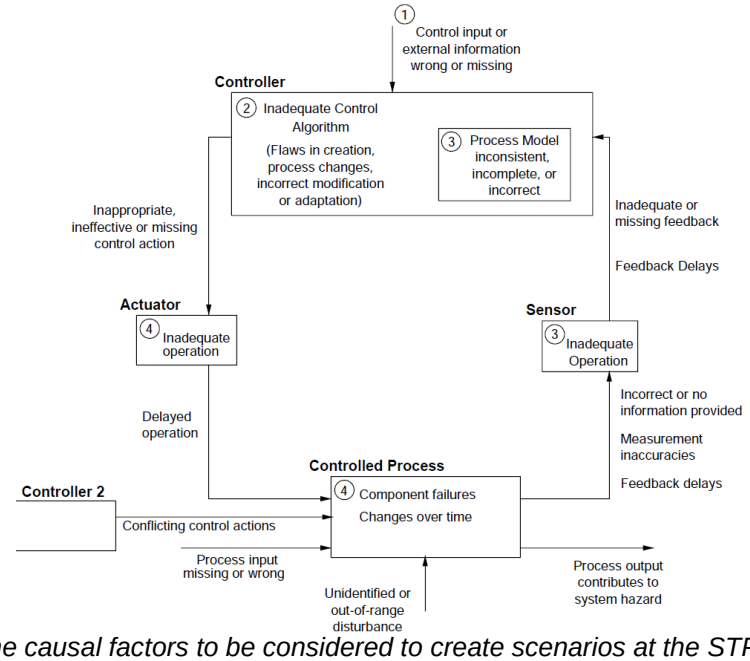


Figure 2. The causal factors to be considered to create scenarios at the STPA Step 2 [4]

2.2 ESF-CCS

Engineered Safety Features-Components Control System (ESF-CCS) controls ESF system by operational signals from a plant protection system (PPS) or a radiation monitoring system (RMS). The ESF system mitigates the consequences of design-basis or loss-of-coolant accident, even though the occurrence of these accidents is very unlikely. The signals are provided when design basis events occur (DBE).

The ESF-CCS has 8 operational functions listed on <Table 1>. Each function controls relevant components in a reactor or a main control room. For example, the SIAS operates a safety injection system which sprays solutions containing boron to cool down a reactor.

Table 1. Operational functions of the ESF-CCS

Function	Description
SIAS	Safety Injection Actuation Signal
CIAS	Containment Isolation Actuation signal
MSIS	Main Stream Isolation Signal
CSAS	Containment Spray Actuation Signal
AFAS	Auxiliary Feed-water Actuation Signal
CREVAS	Control Room Emergency Ventilation Actuation Signal

FHEVAS	Fuel Handling Area Emergency Ventilation Actuation Signal
CPIAS	Containment Purge Isolation Actuation Signal

3. Application

We applied the STPA to the three functions—SIAS, CSAS, and CREVAS. First we defined hazards of the functions. Each function has a different hazard because they have different safety requirement. We also developed control structures for the functions. Although the ESF-CCS controls all of the functions, the control structures are not same because purposes of the functions are different. Next, identifying the unsafe control actions in the control structures are performed, and we identified the causal factors finally.

3.1 Define the Hazard

Application of the STPA starts from defining hazards. When the STPA is applied to an existing design, existing information, such as a control diagram and the functional requirements, system hazards, and the safety constraints and safety requirements for the system, is available when the hazards are defined.

The SIAS provides a reactor emergency coolant containing boron when one of 4 kinds of events:1) the loss of coolant accident (LOCA); 2) the second heat sink loss (2^{nd}HSL); 3) steam- and water-pipe explosion (S/WP-Ex); or 4) the rod ejection accident (REA). The most serious accident of the SIAS is the radioactive leaks. It can lead to huge loss of human life, property damage, environmental pollution, etc. The hazard of the SIAS, therefore, should be below:

Reactor core is damaged because the SIAS does not operate when the 4 events occur.

System safety constraint, moreover, could be defined at this step.

The SIAS must operate when the 4 events occur.

We also identified hazards and safety constraints of the other 2 function. The hazards of the three functions are on <Table 2>.

Table 2. Hazards and safety constraints of the SIAS, CSAS, and CREVAS

Function	Hazard	Safety Constraint
SIAS	Reactor core is damaged because the SIAS does not operate when the 4 events—LOCA, 2^{nd}HSL, S/WP-Ex, or REA—occur.	The SIAS must operate when the 4 events—LOCA, 2^{nd}HSL, S/WP-Ex, or REA—occur.
CSAS	Heat removal and fission clean up fail when the three events—LOCA, S/WP-Ex, or the SIAS—occur.	The CSAS must operate when the three events—LOCA, S/WP-Ex, or the SIAS—occur.
CREVAS	Maintenance of pressure in a main control room fails when the two events—High-level radioactive at air intakes of MCR [1] or the SIAS—occur.	The CREVAS must operate when the two events—High-level radioactive at air intakes of MCR or the SIAS—occur.

[1] Main Control Room

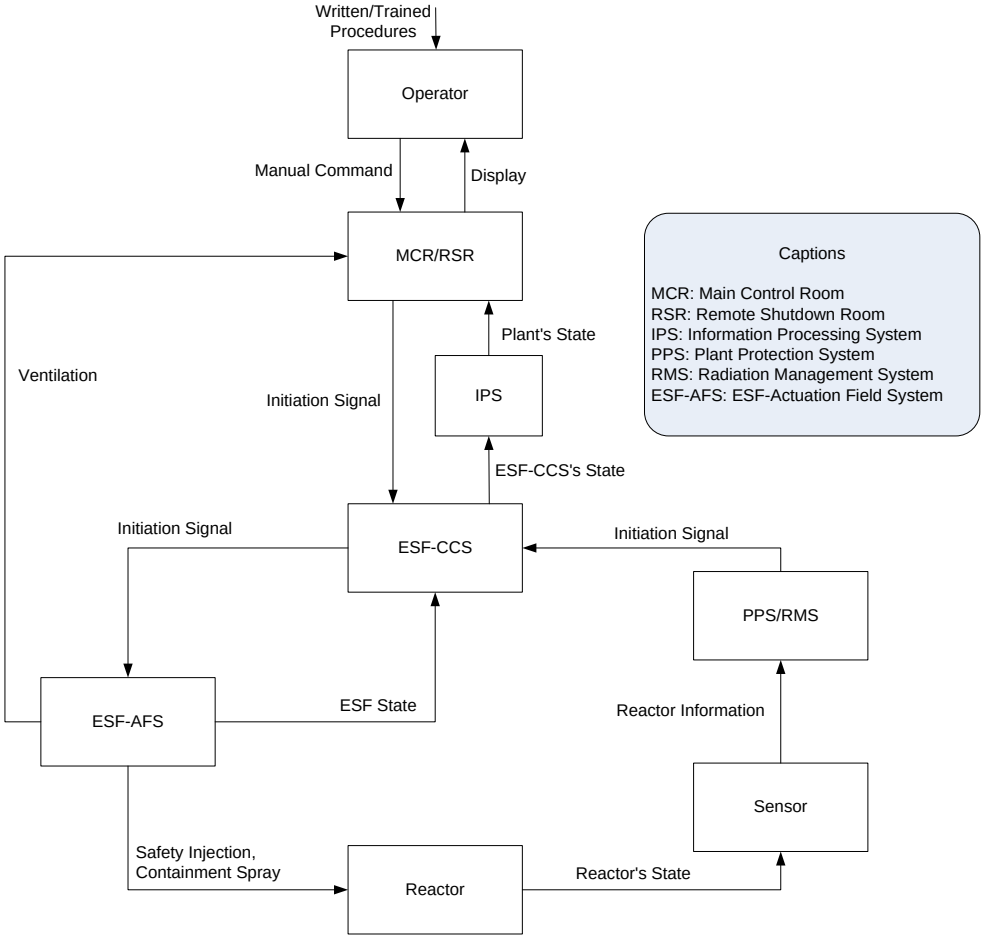
3.2 Develop the Control Structure

<Figure 3> shows the control structure for the ESF-CCS and corresponding components. The main goal for development of a control structure is a clear understanding of relationship between higher- and lower-level components and of each component's responsibility for safety. The control structure is composed of the following components: Operator; MCR/RSR; IPS; ESF-CCS; ESF-AFS; PPS/RMS; Sensors; and Reactor.

The Operator can control the ESF-CCS using devices in the MCR/RSR, and the Operator refers to state of a plant displayed on the MCR/RSR when it decides to initiate the functions. The MCR/RSR sends the Initiation Signal to the ESF-CCS, and receives the Plant's State from the IPS which receives the ESF-CCS's State from the ESF-CCS. The ESF-CCS controls equipment, the ESF-AFS, at the actual spot. The 8 operational functions of the ESF-AFS operate by the Initiation Signals from the ESF-CCS.

The Sensor senses Reactor's State, and sends the information to the PPS/RMS. The PPS/RMS automatically initiates the operational functions at the ESF-CCS, referring to the information. The ESF-CCS receives the initiation, and the remainder of the initiation process is the same process as the manual one.

For the detail analysis of a specific function, we reconstructed the control structure for each function. <Figure 4-5> show the control structure for the SIAS. There are two kinds of initiation for the functions. The first one is a manual one by the Operator, and the second one is automatic by the PPS. The Operator at the top of the control structure in <Figure 3> controls MCR/RSR to initiate the SIAS manually, referring to the information from MCR/RSR. The MCR provides the ESF-CCS a manual initiation signal for operation of the function. The second initiation is by an operational variable from the PPS, which is described in <Figure 4>. If the Sensors detects the 4 events—LOCA, 2^{nd}HSL, S/WP-Ex, or REA—, the PPS referring to the information of the reactor from the Sensors provides initiation of the SIAS to the ESF-CCS by setting the operational variable. The rest of the operation is the same as the manual one. The ESF-CCS handles the two initiations as two inputs of OR operation, which means if one of them initiates the SIAS, the SIAS operates.



"Figure 3. Safety control structure for the ESF-CCS"

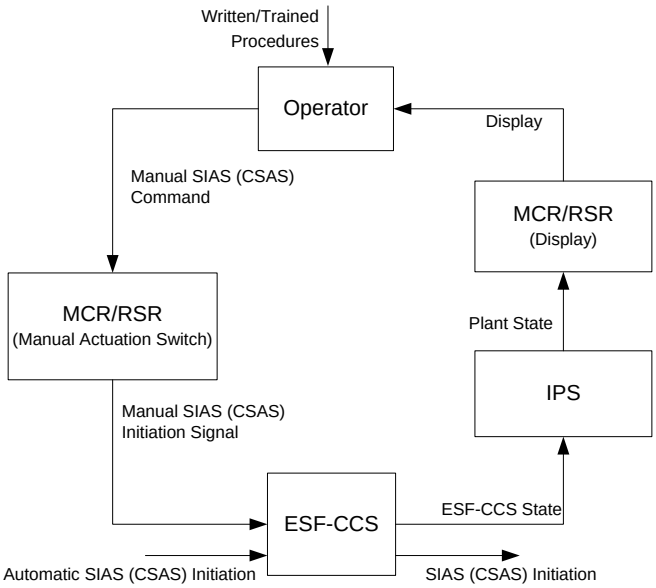


Figure 4. Safety control structure for the SIAS/CSAS by the Operator

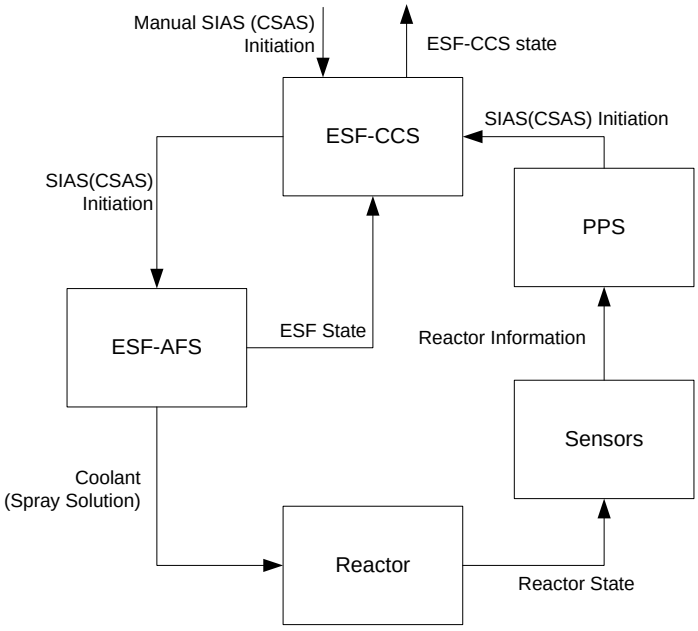


Figure 5. Safety control structure for the SIAS/CSAS by the PPS

The control structure for the CSAS is also described in <Figure 4-5> together with the SIAS. Corresponding components and their relationship are same. Only information in the controls is different. The ESF-AFS sprays solutions on a containment to remove heat and clean up nuclear fission material when the three events—LOCA, S/WP-Ex, or the SIAS—occur.

The control structure for the CREVAS, described in <Figure 6>, is different from the one above. The CREVAS isolates a normal ventilation system and operates an emergent ventilation system when the two events—High-level radioactive at air intakes of the MCR or the SIAS—occur. There also manual initiation by the Operator and automatic initiation by an operational variable from the RMS.

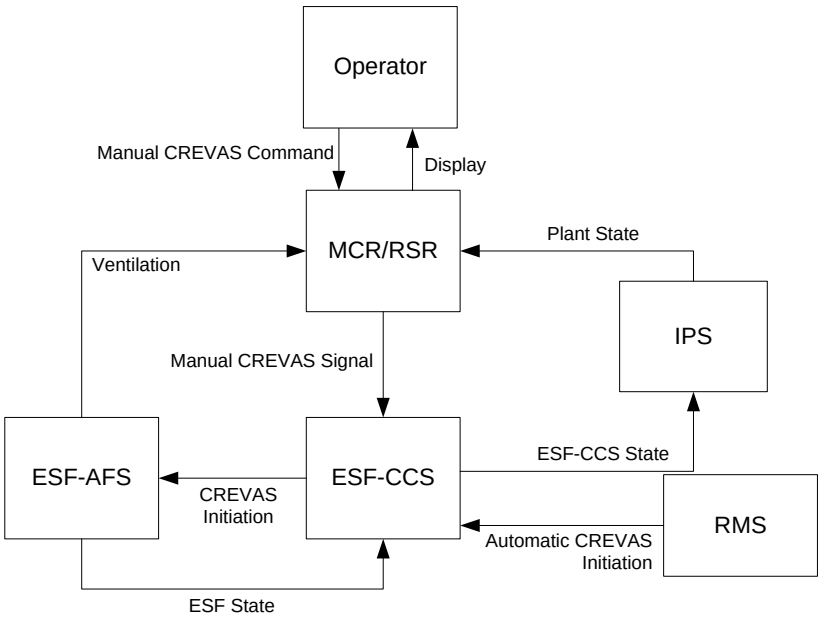


Figure 6. Safety control structure for the CREVAS

3.3 Identify the Unsafe Control Actions (STPA Step 1)

To identify the 4 kinds of unsafe control actions of the ESF-CCS, we used a table. We mention the identification only about the SIAS in the paper because of the space. <Table 3> shows the result of the STPA step 1 for the SIAS by the PPS. The table contains five hazardous types of behaviour:

1. SIAS ON command is not given when one of the five events—LOCA, 2ndHSL, S/WP-Ex, REA, or Manual SIAS ON—occurs,
2. One of the five events—LOCA, 2ndHSL, S/WP-Ex, REA, or Manual SIAS Initiation—occurs and the ESF-CCS waits too long to provide SIAS ON,
3. SIAS ON stops before coolant containing boron is not provided enough;
4. SIAS OFF is provided when one of the five events—LOCA, 2ndHSL, S/WP-Ex, REA, or Manual SIAS Initiation—occurs,
5. SIAS OFF is provided too early (before the temperature decrease enough).

The table does not include incorrect but non-hazardous behaviour. For example, providing a SIAS ON command when the reactor normally operates is not hazardous, although it may cause a great loss of expenses.

Table 3. Identifying hazardous behaviour of the SIAS

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
SIAS ON (From ESF-CCS to ESF-AFS)	*Not providing SIAS ON when LOCA occurs (a1)* *Not providing SIAS ON when 2ndHSL occurs (a2)* *Not providing SIAS ON when S/WP-Ex occurs (a3)* *Not providing SIAS ON when REA occurs (a4)* *Not providing SIAS ON when Manual SIAS Initiation occurs (a5)*	Not hazardous	*When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c1)* *When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c2)* *When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c3)* *When REA occurs, ESF-CCS waits too long to turn SIAS ON (c4)* *When Manual SIAS Initiation occurs, ESF-CCS waits too long to turn SIAS ON (c5)*	*SIAS ON stops before coolant is not provided enough (d1)*
SIAS OFF (From ESF-CCS to ESF-AFS)	Not hazardous	*Providing SIAS OFF when LOCA occurs (b1)* *Providing SIAS OFF when 2ndHSL occurs (b2)* *Providing SIAS OFF S/WP-Ex occurs (b3)* *Providing SIAS OFF REA occurs (b4)* *Providing SIAS OFF when Manual SIAS Initiation occurs (b5)*	*SIAS OFF is provided before the temperature decrease enough (c6)*	Not hazardous
Manual SIAS ON (From Operator to MCR/RSR)	*Not providing SIAS ON when LOCA occurs (a6)* *Not providing SIAS ON when 2ndHSL occurs (a7)* *Not providing SIAS ON when S/WP-Ex occurs (a8)* *Not providing SIAS ON when REA occurs (a9)*	Not hazardous	*When LOCA occurs, ESF-CCS waits too long to turn SIAS ON (c7)* *When 2ndHSL occurs, ESF-CCS waits too long to turn SIAS ON (c8)* *When S/WP-Ex occurs, ESF-CCS waits too long to turn SIAS ON (c9)* *When REA occurs, ESF-CCS waits too long to turn SIAS ON (c10)*	Not hazardous

The identified hazardous behaviours can be translated into safety constraints on the system component behaviour. For the example, the operational function, the SIAS, must enforce five constraints:

1. SIAS ON command must be given when one of the five events—LOCA, 2ndHSL, S/WP-Ex, REA, or Manual SIAS Initiation—occurs;
2. One of the five events—LOCA, 2ndHSL, S/WP-Ex, REA, or Manual SIAS Initiation—occurs and the ESF-CCS must provide SIAS ON in x milliseconds;
3. SIAS ON never stops before coolant containing boron is not provided enough;
4. SIAS OFF must not be provided when one of the five events—LOCA, 2ndHSL, S/WP-Ex, REA, or Manual SIAS Initiation—occurs;
5. SIAS OFF is never provided too early (before the temperature decrease enough).

3.4 Identify the Causal Factors (STPA Step 2)

The STPA Step 2 identifies how each unsafe control action identified in the STPA Step 1 could happen. All of the each unsafe control actions must be considered. <Figure 7> shows the results of the causal analysis in a graphical form.

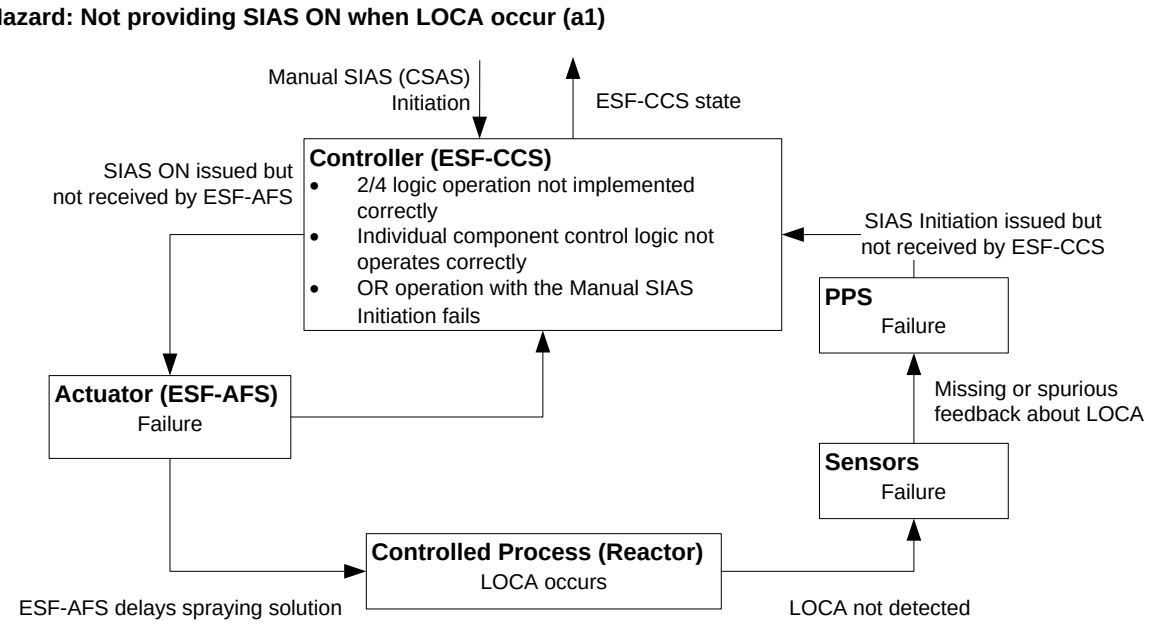


Figure 7. Causal factors about unsafe control action (a1)

The hazard in <Figure 7> is that the LOCA occur but the ESF-CCS does not issue the SIAS ON to the ESF-AFS (a1). The hazard could result if the logic operation in the ESF-CCS is not implemented correctly, individual component control logic does not operate correctly, or OR operation with the Manual SIAS initiation fails at the ESF-CCS itself. Moreover, the causal factors include that the SIAS ON is sent but not received by the ESF-AFS, the ESF-AFS received the SIAS ON but does not implement it (actuator failure), the ESF-AFS delays spraying solution, the LOCA is not detected by the Sensors, the Sensor fails or provides spurious feedback, the PPS received the feedback correctly but does not issue the SIAS Initiation, and the SIAS Initiation is sent but not received by the ESF-CCS. These causal factors are identified using the general causal factors shown in <Figure 2>.

<Table 4> shows causal factors of unsafe control actions (a1-a9). Not only the hazardous behaviour due to '*A control action required for safety is not provided or is not followed*' (a1-a9) but also the others (b1-b5, c1-c7, and d1) are identified, however, the paper presents only the identification about the former.

Table 4. Causal factors of unsafe control actions (a1-a9)

UCAs	A part of the safety control structure	Causal Factors
(a1-a4)	ESF-CCS	2/4 logic operation not implemented correctly
		Individual component control logic not operates correctly
		OR operation with the Manual SIAS Initiation fails
	SIAS On(ESF-CCS to ESF-AFS)	SIAS ON issued but not received by ESF-AFS
	ESF-AFS	ESF-AFS fails to implement its function
	Release Coolant (ESF-AFS to Reactor)	ESF-AFS delays spraying solution
	Sensing (Reactor to Sensor)	The 4 events[2] is not detected by Sensor
	Sensor	Sensor fails
	Reactor's state (Sensor to PPS)	Sensor provides spurious feedback
	PPS	PPS received the feedback correctly but does not issue SIAS Initiation
	SIAS Initiation (PPS to ESF-CCS)	SIAS Initiation issued but not received by ESF-CCS
(a5)	ESF-CCS	OR operation with the SIAS Initiation of PPS fails
	SIAS On(ESF-CCS to ESF-AFS)	SIAS ON issued but not received by ESF-AFS
	ESF-AFS	ESF-AFS fails to implement its function
	Release Coolant (ESF-AFS to Reactor)	ESF-AFS delays spraying solution
(a6-a9)	Operator	Judgement fails about the 4 events
		Misunderstanding about state of Safety Injection operation
	Manual SIAS (Operator to MCR/RSR)	SIAS Initiation issued but not received by MCR/RSR
	MCR/RSR (Manual Actuation Switch)	Manual Actuation Switch fails
	Manual SIAS Initiation Signal (MCR/RSR to ESF-CCS)	Manual SIAS Initiation Signal issued but not received by ESF-CCS
	ESF-CCS State (ESF-CCS to IPS)	ESF-CCS provides spurious information about Safety Injection
		Information about Safety Injection issued but not received by IPS
	MCR/RSR (Display)	MCR/RSR fails to display information
	Display (MCR/RSR to Operator)	Information of the 4 events issued but not received by Operator
		MCR/RSR displays spurious information about the 4 events and Safety Injection

4. Conclusion and Future Work

This paper introduces the application of the STPA to the ESF-CCS. We analysed 3 of 8 functions and identified hazardous behaviours and its causal factors. The paper fully describes the result of the hazardous control behaviour (a1) and partially presents others. We found that the STPA lets analysts have a different view about systems and causes of accidents.

The application of the STAP to the ESF-CCS provided analysts with a different view about causes of accidents. The most conspicuous difference between traditional techniques and the STPA is that the STPA regards the system as a whole. We started the analysis with the ESF-CCS and its accident. The analysis included various components related with the system and identified hazardous behaviours and its causal factors. It is possible to identify the factors not only about the ESF-CCS but also in related components and their relationship. We believe traditional hazard analysis techniques have restrictions to identify such causal factors.

[2] The 4 events in the table include LOCA, 2ndHSL, S/WP-Ex, and REA.

Although the STPA provides analysts with a systematic method to analyse hazards, development of safety control structures and identification of causal factors are very domain-specific. The development and identification might be different, because they depend on understanding of systems by analysts.

We are currently focusing on hazard analysis using STPA and other techniques together. Traditional hazard analysis techniques have made appropriate results for a long time. We expect the collaboration to make more valuable results of the hazard analysis. To apply the STPA to nuclear domain specifically, moreover, we also plan to develop the technique into the development environment for software of nuclear power plant [6][7].

5. Acknowledgement

This research was supported by Basic Science Re-search Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology(2012-0003619) and by the MKE (The Ministry of Knowledge Economy), Korea, under the Development of Performance Improvement Technology for Engineering Tool of Safety PLC (Programmable Logic Controller) program supervised by the KETEP (Korea Institute of Energy Technology Evaluation And Planning)" (KETEP-2010-T1001-01038). It was also supported, in part, by a grant from the Korea Ministry of Strategy, under the development of the integrated framework of I&C conformity assessment, sustainable monitoring, and emergency response for nuclear facilities.

6. References

[1] http://en.wikipedia.org/wiki/Fukushima_Daiichi_nuclear_disaster

[2] http://en.wikipedia.org/wiki/2008_China_Railways_train_T195_accident

[3] Nancy G. Leveson, *SafeWare: system safety and computers*, Addison-Wesley, 1995

[4] Nancy G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, 2012

[5] KNICS, Korea Nuclear Instrumentation & Control System R&D Center, http://www.knics.re.kr/

[6] Junbeom Yoo, Eunkyoung Jee and Sungdeok (Steve) Cha, "Formal Modeling and Verification of Safety-Critical Software," IEEE Software, Vol.26, No.3, pp.42-49, 2009

[7] Jong-Hoon Lee and Junbeom Yoo, "NuDE: Development Environment for Safety-Critical Software of Nuclear Power Plant", Transactions of the Korean Nuclear Society Spring Meeting 2012, pp.1154-1155, 2012