Operational Safety Analysis of HANARO Research Reactor using STAMP/STPA

Sang Hun Lee, Sung-Min Shin, Jinkyun Park*

Risk Assessment and Management Research Team, Korea Atomic Energy Research Institute,
111 Daedeok-daero, 989 beon-gil, Yuseong-gu, Daejeon, Republic of Korea, Email: lees;smshin;kshpjk@kaeri.re.kr

Jeong Sik Hwang

HANARO Management Division, Korea Atomic Energy Research Institute,
111 Daedeok-daero, 989 beon-gil, Yuseong-gu, Daejeon, Republic of Korea, Email: hjs@kaeri.re.kr

The operational policy of nuclear facilities including commercial nuclear power plants and research reactors established and practiced by the utility is required to give safety the utmost priority, overriding the demands of production and project schedules. To date, the probabilistic safety assessment (PSA) has been used as one of the standard tools for the safety evaluation; however, concerns have been raised about its capability to treat the complex interaction between human operators, digital systems, and diverse plant processes. This paper proposes an operational safety analysis procedure based on system theoretic accident model and process/systems-theoretic process analysis (STAMP/STPA). The effectiveness of the proposed procedure is demonstrated with the case study of a cold neutron source system installed in High-Flux Advanced Neutron Application Reactor (HANARO). In result, 127 unsafe control actions (UCAs) were derived for 51 control actions regarding spurious trip scenario. The UCAs were reviewed by the HANARO operators and found new scenarios that requires further investigation for reducing the possibility of a spurious trip. The proposed procedure is expected to provide an integrated viewpoint for operational safety analysis and further used to suggest recommendations for the safety enhancement of nuclear facilities.

Keywords: Operational Safety Analysis, STAMP/STPA, Unsafe Control Action.

1. Introduction

The probabilistic safety assessment (PSA), a systematic method for modelling a plant's response to a set of initiating events, has been used as a standard tool for the safety evaluation of nuclear facilities and provided valuable insights on its safe operation. While the traditional fault-tree analysis (FTA) approach has been used for the PSA of digital I&C systems [1], concerns have been raised about its capability to treat the coupling that may arise due to the dynamic interaction between: 1) the control system and controlled plant process (Type I interaction), and 2) the components of control system (Type II interactions) [2]. If such coupling is not accounted for, potentially significant hazards in nuclear facilities may not be identified.

To overcome the limitations with such cause-effect models, systems approaches to identify hazards introduced from the functional interaction between control units have been proposed [3]. Systemic safety approaches are known to operate as a more holistic approach for safety assessment by accounting for the greater complexity present in the system of systems and considering the role of the operators within the system. Among various models such as Functional Resonance Analysis Method [4], AcciMap [5], and Event Analysis of Systemic Teamwork broken-links approach [6], System-Theoretic Process Analysis (STPA) within the Systems Theoretic Accident Model and Process (STAMP) framework [7] is most widely used for systems approach. STAMP is an accident modelling framework that conceptualizes socio-technical processes as multi-layered control and feedback loops of information between different agents in the system.

The aim of this paper is to propose the operational safety analysis procedure for nuclear facilities characterized by a high level of interactive coupling between human operators and digital control systems. In the procedure, STPA is used to model the operational process of the systems (control structure) and the interaction between subsystems (control action and feedback) in the model is identified based on the available system information such as operation procedures and design specifications. The hazards related to each interaction (unsafe control action) are derived with standardized failure taxonomy.

To evaluate the feasibility of the proposed procedure, it was applied to an example system, namely the cold neutron source (CNS) system of High-Flux Advanced Neutron Application Reactor (HANARO) in Republic of Korea. The case study results were reviewed by the HANARO experts for their validities. Since HANARO experts found important trip scenarios caused by the unsafe interaction between human operators and other systems, further investigation would be meaningful for potential procedure or design improvements.

Proceedings of the 31th European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud and Christophe Berenguer
Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2021-paper

2. Method

The proposed procedure introduces STPA as a part of operational safety analysis to achieve an integrated system view and identify plant hazardous scenarios by taking into account both the technical and human operator aspects as well as the interaction between those agents. The analysis process is divided into four steps: 1) system familiarization, 2) operational document/practice review, 3) STAMP model development, 4) operational safety analysis and review, as shown in Fig. 1.

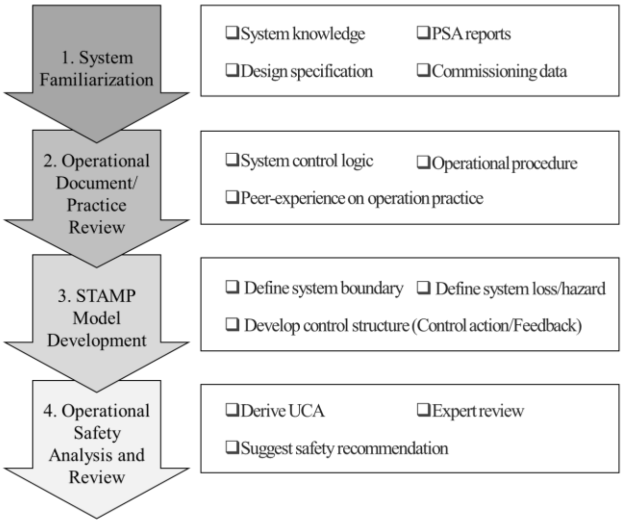
1. System Familiarization
❑System knowledge
❑PSA reports
❑Design specification
❑Commissioning data
2. Operational Document/ Practice Review
❑System control logic
❑Operational procedure
❑Peer-experience on operation practice
3. STAMP Model Development
❑ Define system boundary
❑ Define system loss/hazard
❑ Develop control structure (Control action/Feedback)
4. Operational Safety Analysis and Review
❑Derive UCA
❑Expert review
❑Suggest safety recommendation

Fig. 1. An overview of operational safety analysis procedure

2.1. *System Familiarization*

In nuclear domain, the utilities are obliged with regulatory requirements to prepare documentations on system development and verification lifecycle such as design specifications and safety reports. Such information can be used to understand the subsystems and human operators' activities expected to play a role in plant control which are necessary to capture all possible hazardous scenarios during plant operation.

2.2. *Operational Document/Practice Review*

The general practice adopted in the nuclear industry has been to provide operating procedures for both normal and emergency situations and analyse the plant response in the safety reports. For research reactors in Korea, the operating procedures are managed by the operational procedures preparation, revision and regulation guideline [8]. Such procedures composed of a set of tasks that present step-by-step instructions to select the most appropriate actions for the establishment of safe condition. The instruction can be divided into two major actions: 1) execution and 2) diagnosis, which can be modelled as control action and feedback under STPA framework, respectively. By reviewing the operational documents, the lists of control actions and feedback between process and agents can be developed.

2.3. *STAMP Model Development*

The goal of safety analysis is first defined by identifying the hazard and losses that may occur in the system. Based on a preliminary hazard analysis or expert judgement, the losses specific to system, such as pollution, casualties and property damage, are defined. Then, the hazards are identified which refer to system states or a set of conditions that may lead to the loss, defined within the system boundary [3]. In general, a hazard can lead to one or more losses; therefore, the relationship between loss and hazard can be defined where each hazard is traced to the resulting losses.

A generic control process consists of multiple control levels and the system integrity depends on ensuring the interactions between components do not lead to loss or hazard. In STPA framework, a generic control process can be modelled with a hierarchical control structure, as shown in Fig. 2 [9]. In Fig. 2-(a), the controller A controls both sub-controllers B and C where each controller directly controls the processes X and Y. The control loop between controller C and process Y can be described as Fig. 2-(b) which consists of controller, control action, feedback, and controlled process. The control action implies not only the physical controls by engineered systems such as initiation signals or interlocks but also the managerial or operator controls.

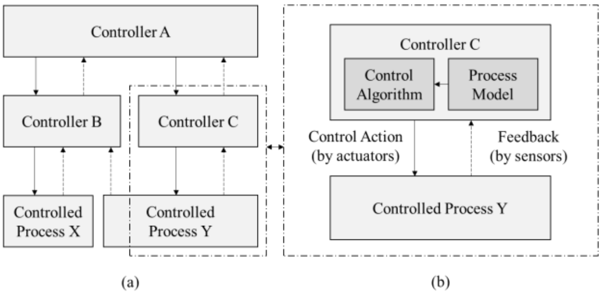

Fig. 2. Example control structure in STAMP model

2.4. *Operational Safety Analysis and Review*

The goal of operational safety analysis is to assess the safety of the facility during its operation and to identify any occurrences that may result in system losses. Major features of STPA include that it identifies non-traditional causal scenarios via unsafe control actions (UCAs) that can lead to system loss arising from dysfunctional component interaction while all components behave in an expected manner.

An UCA is defined as a control action that will lead to a hazard or loss in a particular context or environment [9]. Here, the context is defined as the scenario or condition that assigns safe or unsafe nature to a control action. In this study, six types of UCAs are considered in this study, as follows:

(a) Control action is provided, but not needed and unsafe
(b) Control action is provided, but the intensity is too much or too little
(c) Control action is provided, but executed in incorrect order
(d) Control action is provided, but the duration is too long or too short
(e) Control action is provided, but the starting time is too soon or too late
(f) Control action is not provided, when needed to maintain safety

In the proposed framework, the failure taxonomy within STPA is driven by the use of four standard types of UCAs [3] along with two types of UCAs specific to nuclear applications which are items (b) and (c).

After the UCAs are identified, the associated safety constraints can be derived and its enforcement can help prevent the system from moving into hazardous states. By STPA analysis, the derived UCAs can be used to make functional requirements and design or procedural decision to prevent or mitigate the expected consequences of those UCAs. For example, the specific design features or safety recommendations can be suggested and applied to the existing system allowing effective risk management.

3. Case Study

3.1. *HANARO CNS System*

In Korea, HANARO, a 30-MW multi-purpose research reactor, has been operated since it reached its first criticality at 1995. Especially, experiment facilities such as CNS, shown in Fig. 3, have been playing significant role in various areas including material testing and radioisotope production [11]. However, its operational availability has been reduced as it experiences intermittent unplanned reactor trip and prolonged overhaul to meet enhanced regulatory requirements over years. The operational experience in last decade demonstrated that most of unplanned trips (28%) were caused by the reactor trip due to unstable hydrogen gas pressure in CNS system.

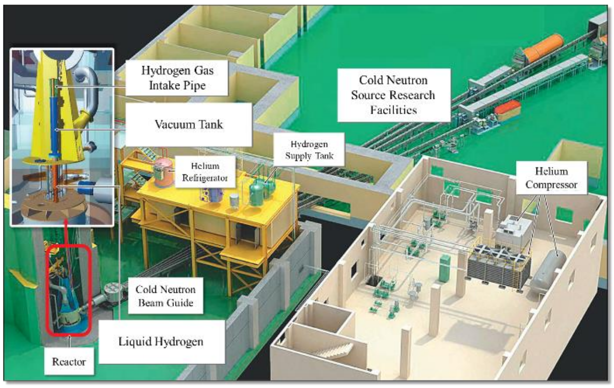

Fig. 3. HANARO CNS system.

The hydrogen pressure in CNS is regulated by the dedicated digital control computer. Since CNS is installed inside the reactor pool, the hydrogen pressure can be affected by the reactor process where manual operation by operator takes place during startup and shutdown. Whenever there is any abnormal situation during the HANARO and CNS operation, the operator can intervene and manually operate the subsystems. The detailed description of the CNS and I&C system where operators conduct manual operation through operator workstation (OWS) can be found in the reference [12].

As a case study, the UCAs which may lead to the spurious trip of HANARO reactor due to the instability of hydrogen pressure in CNS during its operation were derived based on the proposed procedure. In this study, the STAMP model was developed using the RMStudio toolkit [13].

3.2. *Loss/Hazard Definition*

At system level, the CNS system is responsible for maintaining a stable hydrogen pressure in the in-pool assembly (IPA) during its operation. The CNS system consists of components that have been either designed or can be intentionally used as its parts. These includes not only the control systems but also the operators who manually controls the systems via OWS in main control room (MCR) whenever automated systems fail. To derive the UCAs by operator or control system that may cause such spurious trip, the losses and hazard and their logical relationship are defined as shown in Fig. 4.

In the CNS system, the hydrogen pressure in IPA is regulated by various subsystems such as helium refrigeration system (HRS), vacuum system (VS). For example, hydrogen gas in CNS may have high pressure when the vacuum pressure in IPA is not properly maintained due to abnormality of VS which may introduce more heat from the reactor pool. For HRS, the main function is to maintain a stable thermosiphon of hydrogen in IPA. Due to abnormality in HRS, the HRS can cool or heat the hydrogen in IPA excessively than it should be, resulting in high or low pressure in hydrogen system (HS).

3.3. *Control Structure Development*

Fig. 5 shows the control structure of the CNS system. Here, the black solid lines indicate the control action that provides essential signals for the operation of other controllers or controlled processes and the black dotted lines indicate the feedback that provides information to controllers regarding how control actions are carried out.

The digital control systems for CNS include control computer for refrigerator (CCR) and the main control computer (MCC). The CCR regulates the HRS by increasing or decreasing valve opening or the rotation speed of expansion turbine to maintain the cold operation mode of hydrogen (152 kPa, 21 K) in IPA. The MCC controls the components in VS, cooling water system (CWS) and compressed air system (CAS) such as valve opening and pump start or stop to maintain stable operating condition of CNS system.

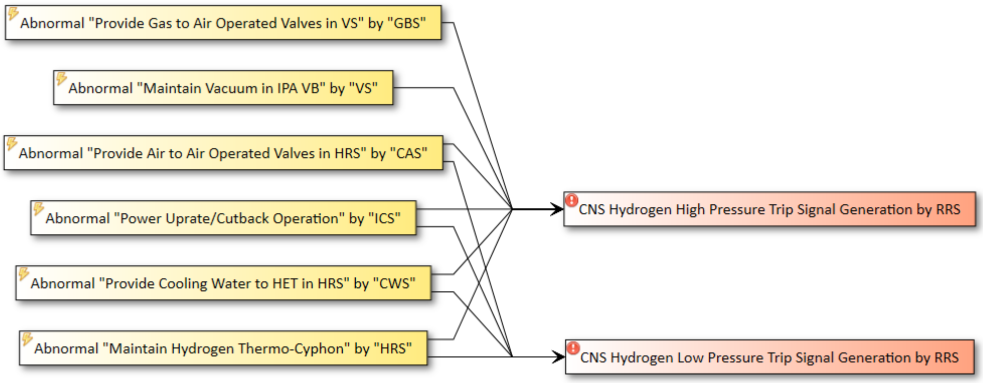
Abnormal "Provide Gas to Air Operated Valves in VS" by "GBS"
Abnormal "Maintain Vacuum in IPA VB" by "VS"
Abnormal "Provide Air to Air Operated Valves in HRS" by "CAS"
Abnormal "Power Uprate/Cutback Operation" by "ICS"
Abnormal "Provide Cooling Water to HET in HRS" by "CWS"
Abnormal "Maintain Hydrogen Thermo-Cyphon" by "HRS"
CNS Hydrogen High Pressure Trip Signal Generation by RRS
CNS Hydrogen Low Pressure Trip Signal Generation by RRS

Fig. 4. Loss-hazard relationship for HANARO CNS system.

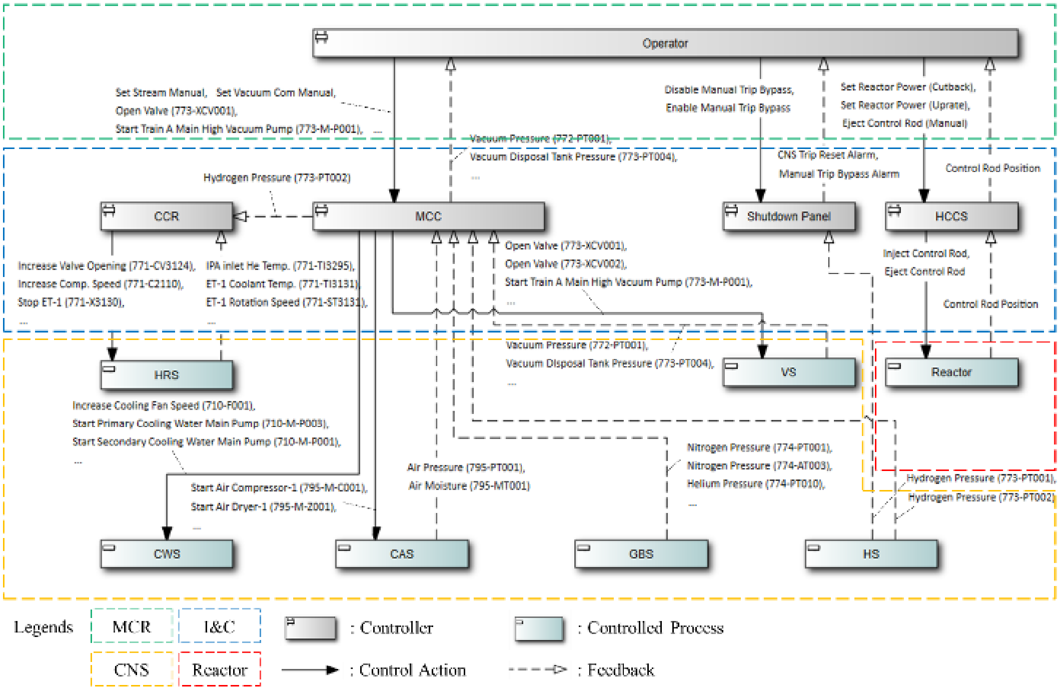
Operator
Set Stream Manual, Set Vacuum Com Manual,
Open Valve (773-XCV001),
Start Train A Main High Vacuum Pump (773-M-P001), ...
Disable Manual Trip Bypass,
Enable Manual Trip Bypass
Set Reactor Power (Cutback),
Set Reactor Power (Uprate),
Eject Control Rod (Manual)
Vacuum Pressure (772-PT001),
Vacuum Disposal Tank Pressure (773-PT004),
...
CNS Trip Reset Alarm,
Manual Trip Bypass Alarm
Control Rod Position
Hydrogen Pressure (773-PT002)
CCR
MCC
Shutdown Panel
HCCS
Increase Valve Opening (771-CV3124),
Increase Comp. Speed (771-C2110),
Stop ET-1 (771-X3130),
...
IPA inlet He Temp. (771-TI3295),
ET-1 Coolant Temp. (771-TI3131),
ET-1 Rotation Speed (771-ST3131),
...
Open Valve (773-XCV001),
Open Valve (773-XCV002),
Start Train A Main High Vacuum Pump (773-M-P001),
...
Inject Control Rod,
Eject Control Rod
Control Rod Position
Vacuum Pressure (772-PT001),
Vacuum Disposal Tank Pressure (773-PT004),
...
HRS
VS
Reactor
Increase Cooling Fan Speed (710-F001),
Start Primary Cooling Water Main Pump (710-M-P003),
Start Secondary Cooling Water Main Pump (710-M-P001),
...
Air Pressure (795-PT001),
Air Moisture (795-MT001)
Nitrogen Pressure (774-PT001),
Nitrogen Pressure (774-AT003),
Helium Pressure (774-PT010),
...
Hydrogen Pressure (773-PT001),
Hydrogen Pressure (773-PT002)
Start Air Compressor-1 (795-M-C001),
Start Air Dryer-1 (795-M-Z001),
...
CWS
CAS
GBS
HS
Legends
MCR
I&C
CNS
Reactor
: Controller
: Controlled Process
: Control Action
: Feedback

Fig. 5. Control structure of HANARO CNS system

The CWS removes the heat from the compressor and cold box in HRS. The cooling tower in CWS consists of three cells where each cell has a cooling fan which is operated in high or low speed mode depending on the cooling water temperature. The CAS consists of redundant air compressor and dryer to provide compressed air to air operated valves in HRS.

The VS maintains the vacuum for insulating cryogenic components such as IPA and cold box in HRS and consists of vacuum pumps and valves which operates depending on the pressure in vacuum box or vacuum disposal tanks. For VS, the operator may switch to manual operation mode and maintain vacuum in IPA. In this case, the operators must follow and conduct a set of tasks to start pump or open valve as specified in the operational procedure. Furthermore, the operators are responsible for manually bypassing the reactor regulation system (RRS) trip signal by manipulating shutdown panel during the startup and shutdown phase.

The gas blanket system (GBS) provides stable gas (helium or nitrogen) to valve boxes in other systems to prevent the hydrogen leak in case of emergency. The HS is filled with hydrogen gas which forms two-phase thermosiphon loop which cools down the neutron from reactor. For both

Proceedings of the 31th European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud and Christophe Berenguer

Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2021-paper

systems, the stable gases are filled in the systems before the CNS operation; therefore, no control action is required during operation, but the gas pressures are continuously monitored by the MCC to detect any abnormalities.

The HANARO control computer system (HCCS) is a part of I&C system which performs the reactor power control by generating step motor operation signals and feedbacks the rod position for operators to monitor the reactor status. In this process, the operator in MCR sets the reactor power level using OWS and HCCS inserts or ejects the control rod as commanded by the operator.

3.4. *UCA Analysis*

To identify UCAs, the context must be specified in which the control action becomes unsafe and leads to system hazards. In this study, the context of UCA is defined using the operational procedure indexes of CNS systems. In the procedure, all actions are described with specific contexts such as the conditions in the controlled process monitored by the controller or the cues to the operator provided by the I&C system. Table 1 shows the examples of context defined in the operating procedure.

In case of OP-103 5.1.7, the valve XCV-001 in VS is controlled by the MCC depending on the value of pressure gauge PT-001. If the XCV-001 valve does not open when PT-001 pressure exceeds the setpoint due to controller, communication, or sensor failures, the vacuum state in IPA will be lost because the piping to IPA remains closed. This will introduce more heat from the reactor pool resulting in trip signal generation by RRS due to high hydrogen pressure in HS. The UCAs for the valve XCV-001 in VS were listed as UCA-60 and 61 in Table 2 and the contexts for those UCAs are defined with the procedure index OP-103 5.1.7 which represents the state of PT-001 pressure.

In case of OP-102 5.2.7, the operator should manipulate the buttons in a specific order to deactivate the trip bypass signal applied during the startup phase. If the operator presses the buttons in an incorrect order or without confirming the process parameters' states, the instability of hydrogen pressure in HS may continue after power uprate operation and results in reactor trip by RRS due to high or low hydrogen pressure. The UCAs for such operator action were listed as UCA-57 and 58 in Table 2.

To develop a full UCA list, each control action defined in Fig. 5 was analysed with the perspective of six UCA types. As a case study, the UCAs for HS, VS and HCCS among CNS systems which involves the control actions by both MCC and operator were identified. As a result, a total of 127 UCAs for 51 control actions related to the target systems were identified which could act as a potential source of system loss. Table 2 shows a part of UCA lists that were considered to be important or were not identified as important factors in the previous safety analysis of CNS system. The full list of UCAs for case study can be found in the reference [14].

Table 1. Context definitions for CNS operational safety analysis

Controller/ Controlled Process	Procedure Index	Description
MCC/ Vacuum System	OP-103 5.1.7	Depending on PT-001 pressure, the valve XCV-001 is continuously operated. - If pressure exceeds 1.33x10^{-6} kPa, open valve. - If pressure is below 1.33x10^{-7} kPa, close valve.
Operator/ Hydrogen System	OP-102 5.2.7	During startup, when reactor power reaches to full power, check the stability of the process parameters: - Helium compressor inlet/outlet pressure - Helium inlet/outlet temperature - Helium expansion turbine inlet valve opening - Hydrogen pressure and 1) press 'CNS Trip Reset' button, 2) press 'Manual HANARO Trip Bypass' button on shutdown panel.

4. Discussion

4.1. *Importance Analysis based on Expert Opinion*

In order to utilize UCAs for formulating recommendations for corrective mitigation measures, the existing protective measures and practices for CNS system were investigated. For this purpose, multiple rounds of expert peer review processes with HANARO operators were conducted where the operators were asked how each UCA is being prevented by which measures; if not, how it is likely to occur based on the operation experiences. In this process, HANARO operators were asked to assess UCAs with the following evaluation scores:

- Possible: UCA requires further investigation to be reflected in the operation procedure or design improvements.
- Impossible: UCA can be mitigated by the existing protective measures or appropriate operator training.

Table 3 shows a part of collected evaluation result. For most UCAs which scored as impossible, the appropriate countermeasures have already been placed based on the past operating experience such as button flow line installation on shutdown panel for UCA-57, the operator training for record checks and OWS manipulation for UCA-58. Two UCAs related to vacuum box valve XCV-001 were considered as potential hazards that require detailed analysis on their failure effect and mitigation measure. Since a single instrumentation channel is used to control the valve, the vacuum in VS will not be maintained if an unsafe control is sent to the valve; therefore, installing redundant sensor channels or generating operator alarms for valve opening and vacuum pressure were suggested as potential improvement plans to mitigate those UCAs.

Table 2. UCA analysis result for HANARO CNS system

Control Action	Source/ Target	UCA Types					
		(a) Provided, but not needed and unsafe	(b) Provided, but the intensity is too much or little	(c) Provided, but executed in incorrect order	(d) Provided, but the duration is too long or short	(e) Provided, but the starting time is too soon or late	(f) Not provided, when needed to maintain safety
Open Valve (773-XCV001)	MCC/ Vacuum System	N/A	N/A	N/A	N/A	**(UCA-60)** Valve 773-XCV001 is opened too late when vacuum box pressure PT-001 is high during OP-103 5.1.7. [H-2]	**(UCA-61)** Valve 773-XCV001 is not opened when vacuum box pressure PT-001 is high during OP-103 5.1.7. [H-2]
Disable Manual Trip Bypass	Operator/ Shutdown Panel	N/A	N/A	**(UCA-57)** Operator manipulated 'Manual HANARO Trip Bypass' button, before 'CNS Trip Reset' button during OP-102 5.2.7 [H-5]	N/A	**(UCA-58)** Operator manipulated trip bypass buttons, before checking the stability of process parameter during OP-102 5.2.7 [H-5]	N/A
Enable Manual Trip Bypass	Operator/ Shutdown Panel	N/A	N/A	N/A	N/A	N/A	**(UCA-112)** Operator does not press 'Manual HANARO Trip Bypass' button before reactor power cutback during OP-01 5.2.1.1 [H-5]

Table 3. Expert review on UCAs of HANARO CNS system

UCA List				Evaluation Score	Expert Elicitation
Controller	Controlled Process	Control Action	UCA		
MCC	Vacuum System	Open Valve (773-XCV001)	**(UCA-60)** Valve 773-XCV001 is opened too late when vacuum box pressure PT-001 is high during OP-103 5.1.7. [H-2]	Possible	The valve and instrumentation is in single train configuration; thus can be potential hazard based on operation experience.
			(UCA-61) Valve 773-XCV001 is not opened when vacuum box pressure PT-001 is high during OP-103 5.1.7. [H-2]	Possible	
Operator	Shutdown Panel	Disable Manual Trip Bypass	**(UCA-57)** Operator manipulated 'Manual HANARO Trip Bypass' button, before 'CNS Trip Reset' button during OP-102 5.2.7 [H-5]	Impossible	As a preventive measure, the operator training was conducted and guide flow lines for trip bypass were inserted in switches of shutdown panel.
			(UCA-58) Operator manipulated trip bypass buttons, before checking the stability of process parameter during OP-102 5.2.7 [H-5]	Impossible	The operators are trained and obliged to write hydrogen pressure in record sheet when the pressure is instable during startup or shutdown phase. The operator will manipulate the button after he/she checks the sheet.
Operator	Shutdown Panel	Enable Manual Trip Bypass	**(UCA-112)** Operator does not press 'Manual HANARO Trip Bypass' button before reactor power cutback during OP-01 5.2.1.1	Impossible	The relevant procedures are practiced regularly by the operators.

Proceedings of the 31th European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud and Christophe Berenguer
Copyright © 2021 by ESREL2021 Organizers. *Published by* Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2021-paper

5. Conclusion

The operational safety analysis of nuclear facilities where human operators and control systems cooperatively operates the system should not only rest on component failures, but also consider hazards resulting from the control actions that are unsafe or involve inadequate interaction between agents. In this paper, the operational safety analysis procedure for nuclear facilities is proposed where the interaction between the subsystems is modelled using STPA framework. The hazards are derived in the form of UCA with six standardized failure types.

The case study on HANARO CNS system showed how the UCA could provide useful insights on operational practice and planning system improvements. As a result of importance analysis, it was demonstrated that the UCAs derived from the proposed procedure can give valuable feedbacks to both designers and operators in the aspect of enhancing the operational safety of target system. For CNS system, new hazards related to spurious trip were found by the proposed procedure and the potential improvements to prevent those hazards were derived during the expert elicitation.

Acknowledgement

This work was supported by the National Research Foundation of South Korea Grant funded by the Korean Government (MSIP) (No.2017M2A8A4015291).

References

[1] OECD/NEA (2009). *Recommendations on assessing digital system reliability in probabilistic risk assessments of nuclear power plants*. OECD/NEA/CSNI, Paris, France, Tech. Rep. NEA/CSNI/R(2009)18.

[2] Aldemir T., D. W. Miller, M. P. Stovsky, J. Kirschenbaum, P. Bucci, A. W. Fentiman, and L. T. Mangan (2006). *Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments.* U.S. NRC, Washington DC, USA, Tech. Rep. NUREG/CR-6901.

[3] Leveson N. G. (2011). *Engineering a safer world: systems thinking applied to safety*. Cambridge, MA, USA: MIT Press.

[4] Hollnagel E. (2012). *FRAM, the functional resonance analysis method: modeling complex socio-technical systems*. Aldershot, UK: Ashgate.

[5] Rasmussen J. (1997). Risk management in a dynamic society: a modelling problem. *Saf. Sci.*, vol. 27, no. 2, pp. 183-213.

[6] Stanton A. and C. Harvey. (2017). Beyond human error taxonomies in assessment of risk in sociotechnical systems: a new paradigm with the EAST 'broken-links' approach. *Ergonom.*, vol. 60, no. 2, pp. 221-233.

[7] Leveson N. G. (2004). A new accident model for engineering safer systems, *Safe. Sci.*, vol. 42, no. 4, pp. 237-270.

[8] Woo J. S. (2008). *HANARO technical administrative procedures manual: manual preparation, revision and management.* KAERI, Daejeon, Republic of Korea, Tech. Rep. HANTAP-05-OD-ROP-TA-08.

[9] Leveson N. G. and J. Thomas (2018). *STPA Handbook*. [Online]. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.

[10] Author, N. (Yeara). *Book Title*. Publisher Name.

[11] Kim Y. K., K. H. Lee, and H. R. Kim (2008). Cold neutron source at KAERI, Korea. *Nucl. Eng. Des.*, vol. 238, no. 7, pp. 1664-1669.

[12] Lee M. W., Y. S. Choi, Y. T. Im, S. G. Doo, K. C. Kim, J. H. Song, C. S. Lee, H. G. Kim, H. S. Jung (2015). *Replacement of the HANARO control computer*. KAERI, Daejeon, Republic of Korea, Tech. Rep. KAERI/TR-6204/2015.

[13] Brown C. and J. Zheng (2017). STPA software module. *In 5th European STAMP/STPA Workshop Conf.*, Reykjavik, Iceland.

[14] Lee S. H., S. M. Shin, and J. Park (2020). *Operational process modelling and analysis for HANARO research reactor based on STAMP/STPA.* KAERI, Daejeon, Republic of Korea, Tech. Rep. KAERI/TR-8100/2020.

Proceedings of the 31th European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud and Christophe Berenguer
Copyright © 2021 by ESREL2021 Organizers. *Published by* Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2021-paper