Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P193-cd

STPA-Based Safety Approach on the Emergency Ventilation System in Nuclear Power Plant

Ankur Shukla

Department of Risk, and Security, Institute for Energy Technology, Norway. E-mail: ankur.shukla@ife.no

Xueli Gao and Yonas Zewdu Ayele

Department of Risk, and Safety, Institute for Energy Technology, Norway. E-mail: xueli.gao@ife.no, yonas.ayele@ife.no

Instrumentation and control (I&C) systems have modernized replacing the hardwired hardware with digital elements. In the past, numerous hazard analysis techniques have been applied to analyze the safety of DI&C systems. However, underlying traditional methods normally do not consider a large extent of the unsafe interactions among system components, human mistakes, and software requirement deficiency. Systems theoretic process analysis (STPA) is a new hazard analysis technique that provides a potential solution to describe how unintended outcomes can occur due to inadequate implementation of constraints on the design, development, and operation of systems. In this paper, we have discussed the STPA-based safety approach to evaluate the safety of the emergency ventilation systems (EVS) in NPPs. We have considered the control structure and process model to identify the unsafe control actions (UCAs), including different controllers (human operator/reactor protection system), types of controls (manual/automatic), and various controlled processes. This approach is implemented on a conceptual EVS inspired by the Halden safety fan (HSF) design. The STPA based safety approach helps to identify safety constraints for the EVS that need to be enforced and ensure that they are adequately enforced in the EVS operation. Moreover, it identifies the process model that the controller needs to provide adequate control and the information required.

Keywords: STPA, Safety, EVS, Human Operator.

1. Introduction

Instrumentation and control (I&C) systems are used in nuclear power plants (NPPs) to monitor, control, and protect plant functions. In this era where electronic and information technology are advancing, most of the industrial systems are transforming to the digital system (Zhang et al. 2020). These digital systems pose a challenge in terms of safety due to complexity and software intensive systems (Thomas and Leveson, 2013, Bao et al. 2019).

In general, NPPs are equipped with number of emergency or safety ventilation systems. These emergency ventilation systems (EVSs) are composed of different elements or sub-systems such as cooling systems, filtration systems, and pressure differential systems. In NPPs, EVSs are mainly used to remove heat in case of an incident that could result in a temperature increase in the containment, to reduce the amount of radioactive materials in exhaust paths by diverting them through special filters instead of directly venting them to the environment, to keep the pressure differential outside of the containment higher that reduces the likelihood of leaks from the containment into the reactor and auxiliary buildings, and to keep emergency equipment cool when it is in operation. As a result of the Fukushima nuclear disaster, one of the most important lessons learned is that a reliable EVS is crucial to ensure the effective incident management during severe accidents especially for smaller volume containments (IAEA, 2017, Son et al. 2012). After the Three Mile Island accident in 1979, many NPPs put effort to improve the capability to prevent and mitigate core damage accidents, as a result filtered containment venting systems, and hardened containment venting systems were installed; for example, Mark I containment designs at BWR plants (IAEA, 2017). Therefore, it is important to ensure the safety of EVSs.

For the safety of DI&C systems of the NPPs, several safety analysis methods have been used for safety assurance and risk management including PHA (Preliminary Hazard Analysis), HAZOP (Hazard and Operability), and FTA (Fault Tree Analysis) and FMEA (Failure Mode and Effect Analysis). However, these methods have certain limitations when analyzing the modern complex systems such as they do not consider the interaction between system components. This problem was addressed by creating a new accident causality model called

STAMP (System-Theoretic Accident Model and Processes) which reframed the safety problem as a control problem (Thomas and Leveson, 2013, Bao et al. 2019, Leveson, 2012). The method considers several factors as potential causes of an accident, such as component failures, external disturbances, and unsafe interactions between system components. Based on STAMP, a new powerful hazard analysis method, STPA (System Theoretic Process Analysis), was created (Leveson and Thomas, 2018) to identify the safety constraints and required process model.

In the past, STPA has been applied for some case studies to ensure the safety of different critical systems of NPPs (Bao et al., 2019, Kim et al., 2017, Shin et al., 2021, Rowland et al., 2021, Shin et al., 2021, Zhang et al., 2022). Thomas and Leveson (2013) introduced the STPA methods for DI&C systems and discusses its advantages over the STAMP method. Their study evaluates the applicability, feasibility, and relative efficacy of STPA using a generalized version EPR (Evolutionary Power Reactor), a type of PWR. Kim et al. (2017) developed a formal-method-based software development, verification, and safety analysis environment, i.e., Nuclear Development Environment 2.0 (NuDE 2.0) for safety-critical digital I&Cs systems. In this environment, they have used STPA for the safety analysis. They performed case studies considering different phase of KNICS APR-1400 RPS BP (KAERI, 2005). Bao et al. (2019) and Zhang et al. (2022) developed a risk assessment process for DI&C upgrades by integrating hazard analysis, reliability analysis and consequence analysis. They used STPA method in the hazard analysis to identify the potential software failures. However, very little attention has been paid to the safety assurance for EVS in NPPs.

In this paper, we have discussed the STPA-based safety approach and implemented to the EVS, which is inspired from the Halden safety fan (HSF) design (Gran et al., 2022). HSF consists of a normal ventilation system for operation and an EVS for unwanted situations such as e.g., containment leaks and radioactive spills. This safety method has been implemented systematically in four steps: defining purpose of analysis, control structure modelling, identifying the unsafe control structure, and the loss scenario. The control structure and process are modelled considering different controllers (human operator and reactor protection system), types of controls (manual and automatic) and controlled processes and used to identify the unsafe control actions (UCAs). This approach is found very useful to identify safety constraints for the EVS that need to be enforced.

The rest of the paper is organized as follows: the basic information and design of EVS is discussed in Section 2. In Section 3, we have discussed the STPA approach, implementation details on EVS, results and discussion. In Section 4, we presented the conclusion.

2. Emergency Ventilation System in NPPs

In NPPs, ventilation plays a crucial role in incident management during severe accidents to ensure the plant safety. A nuclear ventilation system removes or reduces the release of radioactivity into the environment that helps to and maintains a clean and safe environment. It also controls the containment pressure. In the event of an accident, ventilation system helps to remove heat from the containment and scrub radioactivity from the air (Lee et al., 1998). There are two components of a ventilation system in the research reactor building: inlet ventilation and outlet ventilation. The main elements of the emergency ventilation system include fan, cooling system, filter system, pressure differential system, ducts, and control systems (Geue, 1973). Among the elements of a ventilation system, the fan is the primary mover, therefore considers as a heart of the ventilation system. A fan routes air to the ventilation system and maintain pressure of the facility (Cadwallader, 199). The cooling system helps to remove the heat from the containment if an incident would cause the temperature to reach dangerous levels. The cooling system also helps to cool the operational emergency equipment.

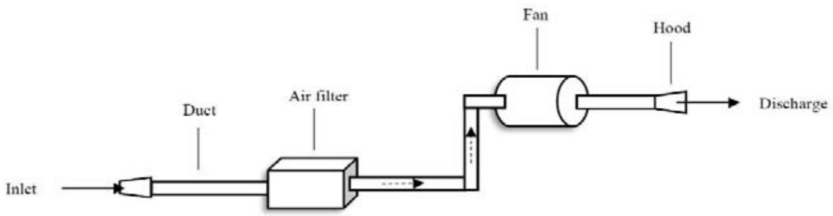

Figure 1. Example of a basic ventilation system

A pressure difference system maintains high pressure differentials outside the containment in order to prevent leakage from the containment to the reactor or auxiliary building. Emergency ventilation system equipped with other components such as heating system, valves, sensors and so on. An example of a basic ventilation system is presented in Figure 1.

In NPPs, the general ventilation system works in the normal situation. In case of emergency, the EVS works since it has greater capacity than the normal ventilation system. The EVS mainly has three states, on, stand-by, and off. In situation of an accident, the reactor protection system (RPS) sends signals to the EVS through an automatic action to activate it. The EVS system can also be activated manually by human operator through human machine interface (HMI). In the accident situation, when RPS fails to active the EVS, it must be activated manually by the human operator.

3. STPA based Safety Assessment Approach

There are several accident causation models in risk management that have been developed over the years. STPA is a relatively new technique developed by Dr. Nancy Leveson (2002) based on a new model of accident causation for hazard analysis that considers unsafe interaction of system components in addition to the component failures. Unsafe interaction between the system components can result into the system failure even if none of the components are failed. The STPA method is based on STAMP, which incorporates three basic elements: constraints, hierarchical control levels, and process loops. This model studies the dynamic control problem that help to enforce the system safety constraints.

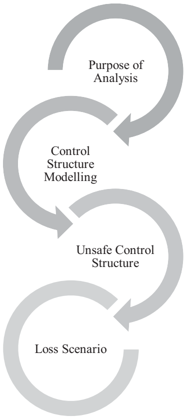

Figure 2. STPA process

In this section we have discussed each step of STPA process and implemented it to the EVS. In this case study, we have considered the situation where the RPS fails to generate the automatic signal and manual action from the human operator is needed to start EVS.

3.1. *STPA process*

The STPA has mainly four basic steps (Figure 2) as follows:

3.1.1. *Purpose of analysis*

According to the STPA handbook (Leveson and Thomas, 2018), the first step of STPA is defining the purpose of analysis, that is divided into four parts: identifying losses, system-levels hazards, system-levels constraints, and one optional part, refining hazards.

The purpose of this analysis is to analyze the situation where RPS fails to generate the automatic signal and manual signal from the human operator is needed. This case study is limited to the manual control action to the EVS and the harm to the environment, i.e., radioactive release to the environment. The detailed discussion of each step of the purpose of analysis is given as follows:

a. Losses:

The main purpose of performing STPA is to study how to prevent the losses. In NPPs, losses related to the emergency ventilation system may include environmental pollution due to radioactive leak or spill to the environment, the loss of human life or human injury due to leaks from the containment to the reactor and auxiliary buildings, loss of property such as safety equipment damages due to high temperature and humidity safety equipment, loss of reputation and loss of mission. However, this case study is limited to the environmental loss and loss of human life or injury. Therefore, we have considered the following losses:

[L-1] Environmental loss due to release of radioactive material to the atmosphere.

[L-2] Loss of human life and/or human injury

b. System-level Hazards

According to the STPA handbook (Leveson, 2018), a hazard is a set of conditions or system states that, when combined with a particular set of worst-case environmental conditions, will cause a loss. In case of an accident, normal ventilation system may fail to filter air properly which may release the radioactive material to the nearby atmosphere, that can lead the environmental harm and loss of life. Therefore, EVS should function properly in case of an accident to avoid the losses. The system states or conditions that lead to the above defined loss can be

[H-1] RPS fails to generate the automatic signal to EVS

[H-2] Failure of manual trip signal to EVS

c. System-level Constraints

The system-level constraint describes the conditions and behaviours to be satisfied to prevent hazards (Leveson and Thomas, 2018). A constraint can also specify how losses must be minimized in the event of hazards. The system level constraints correspond to the above system level hazards are as follows:

[H-1] RPS fails to generate the automatic signal to EVS

SC-1: If RPS fails to generate the automatic signal to EVS, then manual signal must be sent to active it.

[H-2] Failure of manual signal to EVS

SC-2: In case of failure of manual signal to EVS, plant must be shut down immediately.

3.1.2. *Control Structure Modelling*

In this step, control structure of the EVS is modelled. A control structure mainly contains controllers, control actions, feedback, and controlled processes. In case of EVS, RPS and human operators are the main controllers that control EVS (controlled process) by generating automatic or manual trip (control actions) to activate EVS. RPS receives the feedback from the containment regarding the current state and generate automatic signal to the EVS. RPS also receives the current state of the EVS and send the relevant alarm to the human operator. Based on the situation, human operator sends manual signal to EVS through the HMI. The basic control structure of the EVS is given in Figure 3. In this case study we have not considered the redundancy in the design, however, in the real case, it is essential to have redundancy in safety systems so they can achieve high reliability.

3.1.3. *Identify Unsafe Control Actions*

After modelling the control structure, the next step is to identify UCAs that can lead to the system hazards. The following are four ways in which a control action can be unsafe:

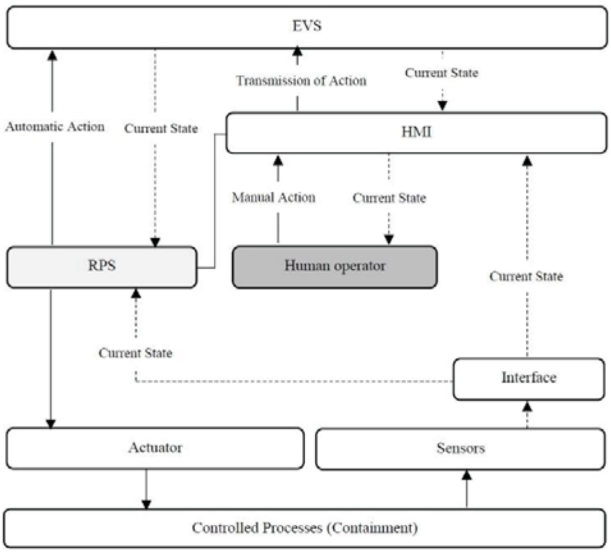

Figure 3. The control structure of the basic EVS.

Table 1. Combination of the potential events including EVS state and action required.

Events	RPS Alarm	Safety Measurement	EVS State (Before action)	Manual Action Required	EVS State
Event 1	No	Normal	Stand-by	No	Stand-by
Event 2	No	Abnormal	Stand-by	Yes	ON
Event 3	Alarm	Normal	ON	Yes	Stand-by
Event 4	Alarm	Normal	Stand-by	No	Stand-by
Event 5	Alarm	Abnormal	ON	No	ON
Event 6	Alarm	Abnormal	Stand-by	Yes	ON

1. A hazard occurs if the control action is **not provided**.
2. A hazard occurs if the control action is **provided.**
3. A hazard occurs if the control action is **provided too early, too late, or in the wrong order**.
4. A hazard occurs if the control action **lasts too long or is stopped too soon**. It applies to continuous control actions rather than discrete ones.

The case study focuses on three types of UCAs (action provided, action not provided, and action provided too late) because they pose major safety concerns. A UCA generally includes five parts: source, type, control action, context, and link to hazards. In the case of EVS, the source is human operator, types of the actions are discussed above, and control actions are the automatic signal by RPS and manual signal by the human operator. The context can be defined based on status of RPS alarm, safety measurement values, and EVS current state as given in the Table 1.

As, we can see in the above table, there can be different events with the combination of RPS alarm, safety measurement, EVS states, and manual signal requirements. However, all of them are not hazardous, for example, event 1 is the normal scenario where RPS is working properly and manual trip is not required; in case of events 3, RPS generating false alarm and activating the EVS, however, in event 4 RPS only generating false alarm and not activating the EVS. These events are not associated with any accidents, so they will not pose the defined loss. However, events 2, 5 and 6 are related to the hazards H-1 and H-2. Therefore, UCA will be linked to the event 2, 5 and 6, as follows:

UCA-1: RPS **does not generate** automatic trip to turn EVS from stand-by to on mode when events 2 occurs [L-1, L-2].

UCA-2: RPS **does not generate** automatic trip to turn EVS from stand-by to on mode when events 6 occurs [L-1, L-2].

UCA-3: Human operator **does not generate signal manually** to turn EVS from Stand-by to ON mode when event 2 occurs [L-1, L-2].

UCA-4: Human operator **does not generate signal manually** to turn EVS from Stand-by to ON mode when event 6 occurs [L-1, L-2].

UCA-5: Human operator **generate** manual trip **too late** to turn EVS from Stand-by to ON mode when events 2 occurs [L-1, L-2].

UCA-6: Human operator **generate** manual trip **too late** to turn EVS from Stand-by to ON mode when events 6 occurs [L-1, L-2].

UCA-7: Human operator **generates** signal manually to turn EVS from ON to Stand-by mode when event 5 occurs [L1, L2].

3.1.4. *Identifying the loss scenario*

This is the last step of the basic STPA process. There are two ways to identify the loss scenarios: first is to find the reason of UCAs and the reason behind the control actions that are improperly executed or not executed.

The problem or failure of the control systems, RPS, HMI and PLC can prevent the automatic signal to the EVS and may give wrong information to the human operator. The potential problem can be identified by reviewing the control structure. The problem in one or combination of the components may prevent signal to reach to the EVS. For example, in case of UCA 1 and 2, there can be problem with the interface sending wrong reading to the RPS or problem with the RPS itself due to that RPS is not sending automatic signal to activate EVS. On the other hand, in UCA 6 there can be possibility that RPS is received the right signal, sent alarm and also generated the automatic signal but could not reach to the EVS due to problem in one component of combination of components in between RPS and EVS, for example PLC. Inadequate control algorithm can also be one of the reasons that leads to these UCAs. In case of UCA 3, RPS received wrong information from the interfaces and activated the signal, however in case of UCA 4, it is not activating the signal. The reason behind these two events can also be the combination of the reasons for UCA 1, 2 and 6.

In case of UCA 3, and 4 human operators does not generate the manual signal to active the EVS during the events 2 and 6. The human operator can make mistake due to variety of factors, improper training, poor communication, fatigue, stress, and distractions. The human operator may not have necessary skills and training to perform the complex operation in case of an emergency. It is also due to the overconfidence of the operator who overlooks routine tasks and essential measurements. It can be the same reason when human operator generating late manual signal as discussed in UCA 5 and 6. There may be another reason that due to the faulty equipment the manual signal is delayed. On the other hand, UCA 7 is the different case where human operator turn EVS from ON to Stand-by mode in the case of emergency. This action can be deliberate or unintentional. Human operator can make mistakes due to several reasons as discussed above. However, the deliberate action does not constitute human error and proper investigation should be made and appropriate disciplinary measures should be taken.

Therefore, to avoid the risk identified from the STPA process, necessary actions should be taken based on the above scenarios and UCAs to avoid losses, for instance, identifying mitigations, additional requirements, reviewing the design, defining new test cases, managing operator stress and work, providing education and training, reviewing profiles, etc._In the event where RPS fails to generate automatic signals (UCA-1 & 2), inadequate design processes, unrealistic assumptions during development, inadequate control algorithms, or unreliable software/hardware can be some of the most common reasons for this failure. Therefore, it is necessary to review the control structure, identify the problem and take necessary action. In the events, where human operator does not generate the manual signal when it is needed (UCA-3 & 4) or generated it too late (UCA-5 & 6), and in the event human operator switched the EVS from ON to Stand-by mode (UCA-7). Therefore, it is needed to have human operator with necessary skills and provide proper training in various environment and conditions, also the identified the reason behind the stress, fatigue and distraction with proper investigation and take necessary actions.

4. Conclusion

There are many techniques for analyzing the hazards of DI&C systems in NPPs. However, these traditional techniques have limited considerations for the unsafe interactions among system components, human error, software requirement error. STPA that is relatively a new hazard analysis technique, overcomes these limitations and provides a solution to describe how unintended outcomes can occur due to inadequate implementation of constraints on the design, development, and operation of systems. In this paper, we have implemented the STPA on EVS that is inspired by the HSF to analyze the safety of the EVS in NPPs. We have modelled the control structure considering the different controllers, types of controls and controlled processes. In this case study, we have considered the situation where the RPS fails to generate the automatic signal to activate EVS and manual signal from the human operator is needed. This case study is limited to the environmental loss and loss of human life or injury. The results from the STPA, provide the valuable inputs to the safety assurance of the HSF that was missing from the current system specification, since it considers all potential casual factors such as software and human operator, unsafe interactions among system components, human error, software requirement error considering software unlike the traditional methods. The next step of the project is to conduct a detailed STPA on HSF by considering different components, multiple controllers, controlled processes, and control actions and results and based on the results the assumptions and specification documents of HSF will be reviewed and necessary changes will be made.

Reference

Bao, H., Zhang, H., & Thomas, K. (2019). An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants (No. INL/EXT-19-55219-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).

Bjørn Axel Gran, André A. Hauge, John Eidar Simensen, Sizarta Sarshar, Fabien Sechi, Xueli Gao, Miki Sirola Halden Safety Fan – Context Description and System Specification.

Cadwallader, L. C. (1999). Ventilation Systems Operating Experience Review for Fusion Applications (No. INEEL/EXT-99-01318). Idaho National Lab (INL), Idaho Falls, ID (United States).

Geue, P. J. (1973). Ventilation systems and components in nuclear power plants and radioactive laboratories (No. AAEC-LIB/BIB--402). Australian Atomic Energy Commission Research Establishment.

Gran B.A., Hauge A.A., Simensen J.E., Sarshar S., Sechi F., Gao X., and Sirola M. (2020). Halden Safety Fan – Context Description and System Specification. Halden Work Report, HWR-1289, OECD Halden Reactor Project, Norway, 2020.

IAEA., International Atomic Energy Agency, Severe Accident Mitigation Through Improvements in Filtered Containment Vent Systems and Containment Cooling Strategies for Water Cooled Reactors: Proceedings of a Technical Meeting on Severe Accident Mitigation Through Improvements in Filtered Containment Venting for Water Cooled Reactors Held, IAEA TECDOC Series No. 1812 Issue 1812 of IAEA TECDOC Series, ISSN 1011-428, International Atomic Energy Agency, 2017.

Kim, E. S., Lee, D. A., Jung, S., Yoo, J., Choi, J. G., & Lee, J. S. (2017). NuDE 2.0: A formal method-based software development, verification, and safety analysis environment for digital I&Cs in NPPs. Journal of Computing Science and Engineering, 11(1), 9-23. (14)

Korea Atomic Energy Research Institute, "SRS for reactor protection system (KNICS-RPS-SRS221)," 2005.

Lee, K. M., Kang, I. S., Bae, S. M., Kim, T. K., & Kim, K. J. (1998). Design of the ventilation system of the nuclear facility (I). General requirements (No. KAERI/TR--983/98). Korea Atomic Energy Research Institute.

Leveson N., Engineering a Safer World, MIT Press, 2012.

Leveson, N. G., & Thomas, J. P. (2018). STPA handbook. Cambridge, MA, USA.

Rowland, M. T., & Clark, A. J. (2021). Application of the Information Harm Triangle to inform defensive strategies for the protection of NPP I&C systems (No. SAND2021-4659C). Sandia National Lab. (SNL-NM), Albuquerque, NM (United States).

Shin, J., Choi, J. G., Lee, J. W., Lee, C. K., Song, J. G., & Son, J. Y. (2021). Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system testbed. Nuclear Engineering and Technology, 53(10), 3319-3326.

Shin, S. M., Lee, S. H., Shin, S. K., Jang, I., & Park, J. (2021). STPA-Based Hazard and Importance Analysis on NPP Safety I&C Systems Focusing on Human–System Interactions. Reliability Engineering & System Safety, 213, 107698.

Song, Y. M., Jeong, H. S., Park, S. Y., Kim, D. H., & Song, J. H. (2013). Overview of containment filtered vent under severe accident conditions at Wolsong NPP unit 1. Nuclear Engineering and Technology, 45(5), 597-604.

Thomas, J., & Leveson, N. (2013). A New Approach to Risk Management and Safety Assurance of Digital Instrumentation and Control Systems. Transactions, 109(1), 1948. (7)

Zhang, F., Hines, J. W., & Coble, J. B. (2020). A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities. Nuclear Technology, 206(7), 939-950.

Zhang, H., Bao, H., Shorthill, T., & Quinn, E. (2022). An Integrated Risk Assessment Process of Safety-Related Digital I&C Systems in Nuclear Power Plants. Nuclear Technology, 1-13.

Bao, H., Zhang, H., & Thomas, K. (2019). An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants (No. INL/EXT-19-55219-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).

Bjørn Axel Gran, André A. Hauge, John Eidar Simensen, Sizarta Sarshar, Fabien Sechi, Xueli Gao, Miki Sirola Halden Safety Fan – Context Description and System Specification.

Cadwallader, L. C. (1999). Ventilation Systems Operating Experience Review for Fusion Applications (No. INEEL/EXT-99-01318). Idaho National Lab (INL), Idaho Falls, ID (United States).

Geue, P. J. (1973). Ventilation systems and components in nuclear power plants and radioactive laboratories (No. AAEC-LIB/BIB--402). Australian Atomic Energy Commission Research Establishment.

IAEA., International Atomic Energy Agency, Severe Accident Mitigation Through Improvements in Filtered Containment Vent Systems and Containment Cooling Strategies for Water Cooled Reactors: Proceedings of a Technical Meeting on Severe Accident Mitigation Through Improvements in Filtered Containment Venting for Water Cooled Reactors Held, IAEA TECDOC Series No. 1812 Issue 1812 of IAEA TECDOC Series, ISSN 1011-428, International Atomic Energy Agency, 2017.

Kim, E. S., Lee, D. A., Jung, S., Yoo, J., Choi, J. G., & Lee, J. S. (2017). NuDE 2.0: A formal method-based software development, verification, and safety analysis environment for digital I&Cs in NPPs. Journal of Computing Science and Engineering, 11(1), 9-23. (14)

Korea Atomic Energy Research Institute, "SRS for reactor protection system (KNICS-RPS-SRS221)," 2005.

Lee, K. M., Kang, I. S., Bae, S. M., Kim, T. K., & Kim, K. J. (1998). Design of the ventilation system of the nuclear facility (I). General requirements (No. KAERI/TR--983/98). Korea Atomic Energy Research Institute.

Leveson N., Engineering a Safer World, MIT Press, 2012.

Leveson, N. G., & Thomas, J. P. (2018). STPA handbook. Cambridge, MA, USA.

Rowland, M. T., & Clark, A. J. (2021). Application of the Information Harm Triangle to inform defensive strategies for the protection of NPP I&C systems (No. SAND2021-4659C). Sandia National Lab. (SNL-NM), Albuquerque, NM (United States).

Shin, J., Choi, J. G., Lee, J. W., Lee, C. K., Song, J. G., & Son, J. Y. (2021). Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system testbed. Nuclear Engineering and Technology, 53(10), 3319-3326.

Shin, S. M., Lee, S. H., Shin, S. K., Jang, I., & Park, J. (2021). STPA-Based Hazard and Importance Analysis on NPP Safety I&C Systems Focusing on Human–System Interactions. Reliability Engineering & System Safety, 213, 107698.

Song, Y. M., Jeong, H. S., Park, S. Y., Kim, D. H., & Song, J. H. (2013). Overview of containment filtered vent under severe accident conditions at Wolsong NPP unit 1. Nuclear Engineering and Technology, 45(5), 597-604.

Thomas, J., & Leveson, N. (2013). A New Approach to Risk Management and Safety Assurance of Digital Instrumentation and Control Systems. Transactions, 109(1), 1948. (7)

Zhang, F., Hines, J. W., & Coble, J. B. (2020). A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities. Nuclear Technology, 206(7), 939-950.

Zhang, H., Bao, H., Shorthill, T., & Quinn, E. (2022). An Integrated Risk Assessment Process of Safety-Related Digital I&C Systems in Nuclear Power Plants. Nuclear Technology, 1-13.