Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
©2025 ESREL SRA-E 2025 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P9554-cd

Application of STPA in Probabilistic Risk Assessment of the Loviisa Nuclear Power Plant

Petri Koivisto
Jensen Hughes, Helsinki, Finland. E-mail: petri.koivisto@jensenhughes.com

Probabilistic risk assessment (PRA) of nuclear power plants requires the use of hazard analysis methods. System-theoretic process analysis (STPA) is a relatively new hazard analysis method based on systems-theoretic accident model and processes (STAMP) causality model. This paper studies the use of STPA in the context of probabilistic risk assessment. This is achieved by conducting a case study of the refueling pool backup cooling system of the Loviisa Nuclear Power Plant in Finland. Results of the case study are compared with an existing risk model of the system. The results of the study indicate that STPA is a promising method for hazard analysis. It can identify all hazard scenarios that were previously identified using multiple techniques, such as failure mode and effect analysis (FMEA) and human reliability analysis (HRA). In addition, the method has been found to be useful in communicating results within a multidisciplinary team of subject-matter experts. However, the incorporation of a new method into the well-established PRA methodology requires further research.

Keywords: system-theoretic process analysis, probabilistic risk assessment, hazard analysis, spent fuel pool, nuclear safety.

1. Introduction

The production of nuclear power is increasingly important to modern societies as the decarbonization and electrification of energy systems progresses. However, in nuclear power production, the risk of nuclear accident and radiological release always exists. Thus, the risk of an accident must be minimized. Traditionally, this is achieved through deterministic accident analysis and plant design principles. Another tool for improving nuclear safety is probabilistic risk assessment (PRA), which is a well-established method for identifying and quantifying the risk of core damage and release of radioactive material.

Radiation and Nuclear Safety Authority (STUK) requires that a PRA is made for all nuclear power reactors in Finland. Background analyses for PRA require, for example, conducting a failure mode and effects analysis (FMEA) and human reliability analysis (HRA). However, there are also numerous other hazard analysis techniques available (Ericson, 2016). One relatively new technique is system-theoretic process analysis (STPA), which has gained popularity in recent years in safety-critical fields, such as aviation, space, and automobile industries (Zhang et al., 2022). In the nuclear power production industry, the applications of STPA have been relatively scarce so far, but there is increasing interest in the field (Thomas, 2021).

Where FMEA identifies hazards by dividing a system into individual components and attempts to find failure modes for the components, STPA is a top-down approach based on system theory (Leveson, 2012). The method assumes that accidents can occur due to unsafe interactions between components or the system and its environment, also including situations in which no components have failed.

This paper studies whether and how STPA can be used in a PRA context either as an individual hazard analysis method or in conjunction with other methods such as FMEA. This is achieved with a case study by performing STPA of the spent fuel pool backup cooling system of the Loviisa Nuclear Power Plant (NPP). The findings of this case study are then analyzed and compared to the existing PRA model of the same system.

The rest of the paper is organized as follows. In

Section 2, a brief introduction to STPA method is given. Section 3 presents an STPA of the fuel pool cooling system. In Section 4, the results of the case study are compared with the existing probabilistic risk assessment and the findings are discussed. Section 5 concludes.

2. Background

A *hazard* has numerous definitions depending on the source and the context. For example, in the PRA context, hazard usually refers to a concrete threat that can cause an initiating event, such as a fire, flood, or tornado. However, in this paper, the term hazard refers to a general cause or precursor of an accident or mishap.

To estimate the probability of an accident, the hazards that can lead to it must be identified. The systematic identification of hazards is called hazard analysis, and there are numerous hazard analysis methods developed (see e.g. Ericson, 2016).

System-theoretic process analysis is a relatively new hazard analysis method. It is based on the systems-theoretic accident model and processes causality model presented by Leveson (2012). The underlying principle behind the method is that, instead of traditional divide-and-conquer methods where the system is broken into parts that are examined separately, the safety and potential safety hazards of a system are considered to arise from the interactions between elements of the system or the system and its environment. The latest version of the method is presented in the STPA Handbook (Leveson and Thomas, 2018). The version presented in the STPA Handbook is slightly updated, making the method easier for practitioners to use.

The STPA method has gained increasing popularity during the last decade (Zhang et al., 2022). Especially in numerous safety-critical fields, such as aviation, space, and automotive industries, the method has had some applications, even leading to standards. However, applications in the nuclear industry have been relatively scarce. The STPA method has been reviewed by the U.S. Nuclear Regulatory Committee (NRC), where it has gained interest (Thomas, 2021). The U.S. NRC sees STPA to be most valuable in addressing the ”unknown unknown”, that is, the identification of risks that have not been recognized previously. They also see potential in hazard analysis of digital instrumentation and control (I&C) systems. Bao et al. (2023) apply STPA in analysis of digital I&C systems of NPPs. They use a redundancy guided variant of STPA to analyze common cause failures for multiple redundant systems.

In the Finnish nuclear industry, there have also been some studies related to STPA. At Fortum, Puustinen (2020) used STPA to analyze the operation of the emergency response organization of the Loviisa NPP. Puustinen (2020) also developed tools to ease the use of the method. Recently, as part of SAFER2028 project, Berger et al. (2024) applied STPA to analyze the feed water system of Olkiluoto NPP plant units 1 and 2. Berger et al. (2024) also include a risk priority number in the STPA process to guide resource allocation in the STPA process.

The STPA method is a four-step analysis process that results in a list of system-level losses, hazards, unsafe control actions, and loss scenarios that are interlinked for backward traceability (Leveson and Thomas, 2018). STPA uses a top-down approach, in which control and feedback relations of the analyzed system are modeled, and potential hazards are identified. Thus, the STPA method can identify hazards from technical component failures as well as human and software errors. The steps are covered in more detail in the next section, where an STPA analysis of the spent fuel backup cooling system of the Loviisa NPP is explained.

3. Case Study: Application of STPA in Cooling System Hazard Analysis

3.1. *Spent fuel pool backup cooling system*

Since spent nuclear fuel produces decay heat even after the nuclear fission reaction has ended, fuel assemblies must be cooled to prevent them from melting. Thus, spent nuclear fuel is submerged in water, which is used as coolant and also absorbs radiation emitted by the highly radioactive nuclear fuel protecting staff from radiation. Spent nuclear

fuel is stored in spent fuel pool (SFP) for at least a year after the fuel is removed from the reactor. SFP is also used during the refueling outage while fresh nuclear fuel is changed to the reactor. The SFPs of the Loviisa NPP are located inside the steel containments of the reactor buildings. Figure 1 shows the layout of the reactor building of Loviisa plant unit 1 during refueling.

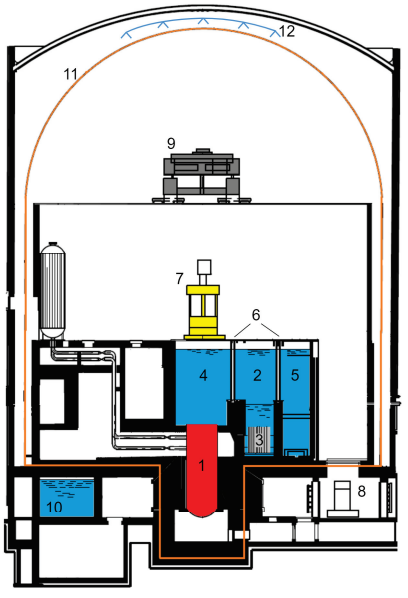

Fig. 1. Layout of reactor building of Loviisa 1 plant unit. (1) Reactor pressure vessel, (2) Spent fuel pool, (3) Fuel assemblies, (4) Reactor pool, (5) Well 1, (6) Removable water-tight gates, (7) Fuel loading machine, (8) Fuel transfer cask (9) Polar crane, (10) Emergency water tank, (11) Steel containment, (12) Containment shell cooling sprinklers.

The temperature of the water in the SFP under normal conditions is kept below 70 °C using spent fuel pool cooling system. If the primary cooling systems for the spent fuel pool are inoperable, the temperature of the coolant water rises, and eventually the water starts to boil. The spent fuel pool backup cooling (SFPBC) system can be used to maintain the cooling water level of the SFP by pumping water to compensate for evaporation of the water.

The SFPBC system allows multiple options for the injection of water into the spent fuel pool. A simplified piping and instrumentation diagram of the system is presented in Figure 2. The water source for the system water pump can be selected from an emergency water tank of the plant unit or, if the tank is empty, from recirculation sump. In addition, if the SFPBC system water pump is not operable, water can also be pumped from an external source using, for example, fire engine pumps.

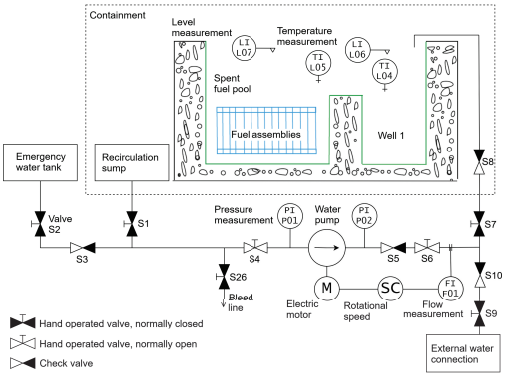

Fig. 2. Piping and instrumentation diagram of the SFPBC system.

The SFPBC system has no automated control: all valves in the system are hand-operated or medium-controlled, and the water pump is turned on manually. However, some measurements are provided to the operators: inlet and outlet pressures of the water pump, water flow measurement that controls the rotational speed of the 3-phase electric motor of the pump, and water temperature and level measurements in the spent fuel pool.

3.2. *STPA of the system*

In this paper, not all considerations and results from the analysis are presented, but selected examples that give the reader a sufficiently broad picture of the analysis and the STPA method.

3.2.1. *Step 1: Defining the purpose of the analysis*

Step 1 of the STPA process requires first identifying *losses*. A loss in STPA context refers to

an accident or mishap that is unacceptable to the stakeholder, and thus is something that is to be eliminated with the analysis. A loss may be, for example, injury or loss of human life, loss of production, damage to equipment, or pollution of the environment. A list of losses can be defined freely to focus the analysis on a specific loss, or if multiple losses are considered, some kind of importance ranking can be used.

Several losses could be identified for the fuel pool cooling system. However, in the scope of Level 1 PRA, only scenarios that can lead to melting of nuclear fuel are analyzed. Thus, the loss is defined as

L-1: Melting of nuclear fuel in the SFP.

After the losses have been defined, *system-level hazards* have to be identified. A hazard in the STPA method is defined as a state of the system that can lead to a loss if certain conditions are met. In this way, the hazard can be interpreted as a state or condition of the system that occurs just before an accident.

There are two main ways that can lead to the loss: either the water level of the SFP drops too low, revealing the fuel assemblies, or the cooling channels of the assemblies are somehow clogged, preventing effective cooling. Thus, two hazards can be defined:

H-1: Water level in SFP boils down to the level of the top of the fuel assemblies. [L-1]

H-2: The cooling channel of a fuel assembly is clogged. [L-1]

The hazards are linked to the loss that they can cause by marking it in square brackets.

The hazards are analyzed for the SFPBC system, so no other means of cooling the spent fuel pool are considered in the analysis. However, operators using the SFPBC system are considered as parts of the system in the analysis.

3.2.2. *Step 2: Modeling the control structure*

Step 2 of the STPA method involves modeling the system with a *control structure*. The control structure is a hierarchical model of the system consisting of feedback control loops. The control structure is presented as a *control diagram* where *control actions* (CA) are presented with downward facing arrows, and the upward facing arrows represent feedbacks. Horizontal arrows describe other inputs and connections between system components. The hierarchy between system components is shown by drawing controllers with higher authority higher on the diagram.

The control structure for the analyzed system was modeled on the basis of available documentation and expert judgment. Since the system has many human controllers, numerous operating procedure documents were analyzed to combine the information into a single control diagram presented in Figure 3.

3.2.3. *Step 3: Identifying unsafe control actions*

After creating the control diagram, step 3 involves identifying *unsafe control actions*. Unsafe control action (UCA) is a control action that can lead to a hazard. A control action is unsafe, if one or more of the following statements are true:

(i) Not providing CA can lead to hazard.

(ii) Providing CA can lead to hazard.

(iii) Providing CA too early, too late, or in an incorrect order can lead to hazard.

(iv) Stopping it too soon or applying it too long can lead to hazard.

Step 3 of the STPA method is to analyze for each CA in the control diagram whether any of these four situations can lead to previously identified hazards. As an example, the analysis is presented for the control action ”Prepare process connection” from field operator to hand-operated valves.

Not providing causes hazard:

UCA-1: Field operator does not connect water source when SFPBC system is taken into use [H-1]

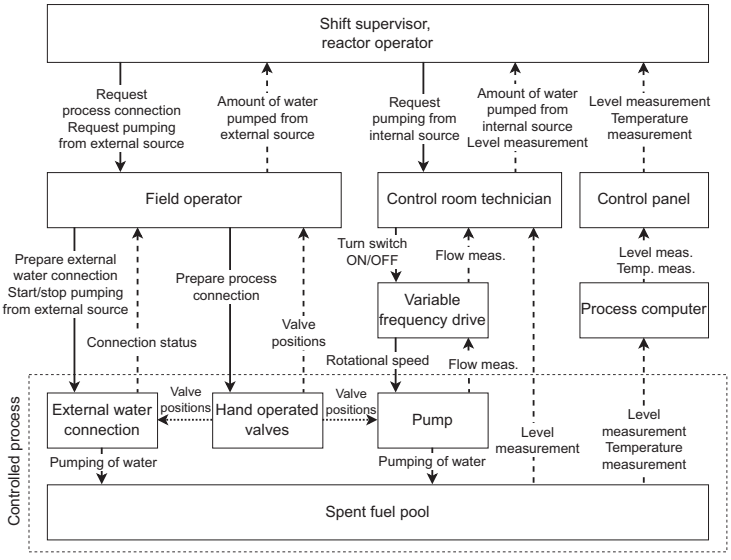

Fig. 3. Control diagram for the spent fuel pool backup cooling system.

Providing causes hazard:

Not applicable, as connecting the right water source does not cause any hazard.

Providing to soon, too late or in wrong order causes hazard:

UCA-2: Field operator connects wrong water source when SFPBC system is taken into use [H-1]

Stopping too soon or applying too long causes hazard:

UCA-3: Field operator does fully open the valves when SFPBC system is taken into use [H-1]

As can be seen in the example, all the unsafe control actions identified are related to hazard H-1. There are no conditions for this example CA that directly could cause hazard H-2.

3.2.4. *Step 4: Identifying loss scenarios*

In step 4 of the STPA method, *loss scenarios* are identified. Loss scenarios describe the causes that can lead to UCAs and hazards. There are two types of loss scenarios that are considered: these answer the questions (Leveson and Thomas, 2018)

(a) Why would UCAs occur?

(b) Why would CAs be improperly executed or not executed, leading to hazards?

Scenarios were identified by first analyzing scenarios leading to UCAs, that is, type (a) scenarios. Below are some example scenarios that can cause unsafe control actions listed in the previous section.

Scenario 1 for UCA-1: The field operator cannot open the hand-operated valve S7 because it is stuck closed [UCA-1]. As a result, the SFPBC system cannot be taken to use. [H-1]

Scenario 2 for UCA-1: The field operator cannot physically go to open the valves due to conditions (internal flooding, radiation, etc.) [UCA-1]. As a result, the SFPBC system can not be taken to use. [H-1]

Scenario 1 for UCA-2: The field operator connects the feed to the pump from internal source, even though the emergency water tank is empty [UCA-2]. This can result from incorrect instructions, following wrong operating procedures, or a wrong situation picture. If the wrong connection is not noticed, there is no water flow to the SFP [H-1].

STPA provides numerous scenarios for a single UCA. Each of these scenarios is equally important in the STPA sense, as there is no in-build priorisation of scenarios or UCAs in the method. It is also noticeable that these scenarios can be formulated in such a way that single devices that can cause a hazard can be determined. This leads to another observation: the total number of loss scenarios identified in the analysis is greatly affected by how much the analyst is willing to combine similar causes to a single scenario.

Type (b) loss scenarios involve scenarios where the right control actions are made but they do not have the desired effect. These are not directly related to the UCAs listed in Step 3 of this case study. Below is an example of type (b) loss scenario identified in the case study.

Scenario 1: The field operator makes the process connection, but there is air in the feed water line. The pump bleeding valve cannot be accessed during a severe accident, so the pump starts to cavitate breaking the pump. If an external connection cannot be used, the feed to the SFP fails. [H-1]

These scenarios are selected to represent the possible scenarios that can be found with the STPA method. The next section compares the scenarios found to those that have been recognized earlier in the Loviisa NPP PRA study.

4. Results and Discussion

4.1. *Comparison of current PRA model and STPA results*

The scenarios created in the case study were compared with the existing PRA model of the SFPBC system. The failure of the system is modeled with a fault tree. On top of the fault tree is a top event "SFPBC system fails". The leaves of the tree are basic events, which describe a failure of, for example, a technical device. Basic events lead to the top event through logical gates, and if basic events have been assigned with probabilities, the probability of the top event can be calculated from the basic event probabilities using Boolean algebra.

The basic events of the fault tree are identified through different methods. For component failures, failure mode and effects analysis is used. The FMEA of the SFPBC system includes 27 components with a total of 40 failure modes. All of these could be identified with STPA as well. Human reliability analysis is used to identify operator errors. PRA model of the SFPBC system has four identified operator errors (see Figure 2 for component codes):

- Operator fails to recognize the need to use SFPBC system or fails to operate it
- Manual valve S4 or S6 erroneously closed and recovery fails
- Operator fails to connect external water source
- Operator fails to connect external water source due to initiating event

These are are similar to the scenarios detected in the case study. However, the scenarios produced by STPA are more descriptive. Most notably, the operator error "Operator fails to recognize the need to use SFPBC system or fails to operate it" is modeled with only one probability.

4.2. *Discussion*

Based on the case study, the STPA method can identify all scenarios that are included in the current PRA model. In the analysis of the SFPBC system, STPA could find more accurate scenarios for human errors than those identified with PRA methods. This indicates that STPA is a noteworthy method for hazard analysis for PRA purposes. However, based on the case study, the STPA method seems to offer little benefit compared to the added analysis time.

The PRA methodology is carefully designed to produce mathematically robust and quantitative results. Fitting STPA into the methodology would require more research to find the best practices to use STPA so that the results can be inputted to the PRA model. However, there is definitely potential in the method.

In discussions with experts in the nuclear industry, the most beneficial part of the STPA method was

found to be the control diagram. The control diagram is an effective tool to combine information from numerous documents into one easily interpreted figure. The control diagram provides a platform for discussions with experts from different disciplines. It also models the hierarchy of control of the system. Many times, possible hazardous interactions can be identified directly from the control diagram.

Modeling of the control diagram also enables the analyst to think about hazards other than component failures. However, in the identification of the loss scenarios (Step 4) of the method, the scenarios can be written so that single component failures are also found. The STPA handbook (Leveson and Thomas, 2018) actually warns about this, as focusing on single-component failures reduces the method to FMEA. However, in PRA context single-component failures are also important to analyze in order to obtain importance measures for components, and the straightforward FMEA method is probably more effective and suited for the task.

The STPA method produces a large number of UCAs and scenarios even for a relatively simple system like the refueling pool backup cooling system. The normal STPA method lacks a way to prioritize these scenarios in order of importance. This is a problem when analyzing systems that are already built and not in the design phase, since all possible loss scenarios probably cannot be mitigated. A crude prioritization of scenarios could be incorporated through Risk Priority Numbers (RPN) for STPA (Berger et al., 2024).

Although the STPA method is relatively straightforward, during the case study, it was observed that some kind of software tool is beneficial for analysis. Keeping track of all links between STPA elements is difficult if, for example, the initial control structure is changed in the latter part of the analysis. During the analysis, it was found that a normal spreadsheet program is a cumbersome platform for the task. An STPA-specific software tools could be tested or developed. In addition, STPA process could perhaps be automated to generate applicable questions to guide the analyst at each step of the process.

The refueling pool backup cooling system analyzed in the case study is a relatively simple system. Most STPA studies have been performed on large complex systems. Thus, the potential advantages of the method compared to other hazard analysis methods could possibly have been better demonstrated by performing the analysis on a more complex system.

Human errors have been identified as a major contributor to the uncertainty of the Loviisa PRA results. Traditionally, if determining failure probability of a basic event is difficult, the probability is estimated conservatively. In order to achieve more accurate PRA results, a best estimate approach should be preferred for probability estimation. STPA could possibly be used to analyze the possibilities for human error in system operation, on the basis of which the HRA probabilities could be estimated more accurately. However, while a more accurate modeling of human errors could reduce the estimated risk, the HRA modeling has been consciously kept relatively simple for easier maintenance.

The STPA method produces qualitative results. On the other hand, in PRA the emphasis is on quantifying the risk associated with a system. PRA methodology is sometimes criticized for focusing too much on the probability of risk (see, e.g. Leveson, 2024). However, often the actual frequency of an accident is not that interesting, but the importance measures and other results that are obtained from the analysis. These can be used to target the usually limited budget to reduce the risk of a system in the most cost-effective manner. This is especially useful in improving the safety of old nuclear power plants that follow design principles from the 1960s.

5. Conclusion

This paper studied the use of system-theoretic process analysis in background analyses for probabilistic risk assessment by conducting a case study of the spent fuel pool backup cooling system of

the Loviisa Nuclear Power Plant. The results of the case study were compared with a previous PRA model of the same system.

The results indicate that STPA is a promising method for hazard identification. It identifies all failure scenarios that are included in the current PRA model of the system. However, for the identification of hazards of single component failures, FMEA is probably still a more effective method. STPA is not the silver bullet that could be used to replace all existing hazard analysis techniques but another tool to the analyst's toolbox.

As human errors are a major contributor to not only risk but also uncertainty in the PRA of the Loviisa NPP, the greatest benefit of the STPA method could probably be achieved with more accurate identification and modeling of operator errors. However, this finding is highly affected by the system that was analyzed, as it has little automated control.

The probabilistic risk assessment of the Loviisa Nuclear Power Plant has been constantly updated and improved since the 1980s. The PRA methodology is a well-established procedure that has numerous standards and guidelines for implementation. PRA of nuclear power plants is also required and regulated by supervisory authorities. Thus, when implementing a new hazard analysis method in the PRA context, great consideration must be given to the benefits and costs of the new method. Based on the case study presented in this paper, the benefits of the STPA method for PRA are not enough to justify its use. However, this does not mean that the method would not be useful in the future as the I&C systems of nuclear power plants are going to be more software intensive. Some best practices for STPA implementation to PRA should be researched and developed prior to wide usage of the method.

PRA is a tool that can be used to achieve higher safety through a better understanding of the risks involved in the production of nuclear power. Similarly, STPA can also be a useful tool outside the PRA context to improve the safety of nuclear power production, for example, through general risk management and the development of operating procedures. A risk-informed use of STPA to improve the safety of old nuclear power plants would present an interesting topic for research.

Acknowledgement

This paper is based on the author's master's thesis, which was approved at Aalto University in 2024. The author thanks Professor Ahti Salo for supervising the thesis, Tommi Purho at Loviisa Nuclear Power Plant for his advice during the writing of the thesis, and Fortum Power and Heat Oy for providing the topic and funding of the thesis.

References

Bao, H., H. Zhang, T. Shorthill, E. Chen, and S. Lawrence (2023). Quantitative evaluation of common cause failures in high safety-significant safety-related digital instrumentation and control systems in nuclear power plants. *Reliability Engineering & System Safety 230*, 108973.

Berger, J., R. Tiusanen, H. Kothalawala, and A. Pakonen (2024). Applying Priority-Informed STPA to a Nuclear I&C System. In *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*.

Ericson, C. A. (2016). *Hazard Analysis Techniques for System Safety* (Second ed.). John Wiley & Sons.

Leveson, N. G. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press.

Leveson, N. G. (2024). Discussion of Some FAQ Submitted by Workshop Attendees. [Online]. Available at: `https://psas.scripts.mit.edu/home/wp-content/uploads/2024/2024-06-05-1540__FAQ_Nancy.pdf`, accessed 7.1.2025.

Leveson, N. G. and J. P. Thomas (2018). *STPA Handbook*. Massachusetts Institute of Technology.

Puustinen, O. (2020). Systeemiteoreettisen prosessianalyysin hyödyntäminen valmiustoiminnan suunnittelussa. Master's thesis, LUT University.

Radiation and Nuclear Safety Authority (STUK) (2019). Probabilistic risk assessment and risk management of a nuclear power plant (YVL A.7).

Thomas, J. (2021). Investigation of the use of System-Theoretic Process Analysis at the NRC. Technical report, U.S. NRC.

Zhang, Y., C. Dong, W. Guo, J. Dai, and Z. Zhao (2022). Systems theoretic accident model and process (STAMP): A literature review. *Safety Science 152*, 105596.