Integrating STPA to NPP Systems Engineering Processes

Josepha Berger, Akira King, Antti Pakonen

This is the submitted version. Please cite the final published version:

Berger, J., King, A., Pakonen, A. Integrating STPA to NPP Systems Engineering Processes. 14th Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2025), June 15-18, 2025, Chicago, IL, USA, pp. 1762-1771.

DOI: 10.13182/NPICHMIT25-46634

Integrating STPA to NPP Systems Engineering Processes

Josepha Berger[1,*], **Akira King**[2], **Antti Pakonen**[3]

[1]VTT Technical Research Centre of Finland Ltd., Tampere, Finland
[2]Aalto University, Espoo, Finland
[3]VTT Technical Research Centre of Finland Ltd., Espoo, Finland

ABSTRACT

STPA has demonstrated its usefulness in identifying hazards in NPP I&C systems. Its strengths lie in visualizing system-level control structures, uncovering interactions among technical components and human operators, and offering insights into complex feedback loops. We believe these strengths can be further leveraged by expanding the STPA method from its current focus on isolated I&C use cases to becoming a tool for broader Systems Engineering (SE) processes. By doing so, STPA could offer valuable insights to support decision-making and planning across all SE phases.

This paper proposes enhancements to the STPA process that enable smoother integration into NPP SE, particularly within the V-model. A key contribution is the introduction of a fifth step in the STPA process, which translates loss scenarios into system requirements, connecting them to mitigation strategies and assigning responsible persons for follow-up. Additionally, we propose establishing links to internal documentation and relevant regulatory frameworks. This should provide direct insight into for example important technical specifications of system elements and support the definition of system requirements. Further improvement suggestions include risk-based prioritization of loss scenarios, color-coded categorizations of interaction types, and grouping of common underlying risk factors in loss scenarios. These enhancements allow for more efficient analyses, targeted expert involvement, and foremost support the integration of STPA to all phases of NPP SE.

Keywords: STPA, Systems Engineering, Nuclear Power Plant

1. INTRODUCTION

The Systems-Theoretic Process Analysis (STPA) has proven valuable for identifying safety risks in nuclear power plant (NPP) instrumentation and control (I&C) systems. Experiences from our earlier studies [1,2] confirm its effectiveness, particularly in visualizing system-level control activities, feedback loops, and interactions between technical components and human operators. STPA's control structure offers a complementary perspective to traditional methods, especially regarding human-technology interactions and control modes.

However, in its current form, as applied in Finnish nuclear industry, STPA is largely used as a stand-alone analysis method. It is primarily used for identifying potential hazards of isolated I&C systems rather than supporting system development or modification throughout the system lifecycle. This is due to a set of limitations:

*josepha.berger@vtt.fi

1. The 2018 STPA version [3] ends in a list of loss scenarios (Step 4: “Identify Loss Scenarios”), describing how certain circumstances can give rise to accidents and other undesired scenarios. This is not an ideal outcome for smooth integration into nuclear systems engineering (SE) as no mitigation measures or follow-ups are defined.

2. Depending on the use case, STPA Step 4 often produces a lengthy list of loss scenarios. While assigning a Risk Priority Number (RPN) [4] has proven useful for prioritizing these scenarios [1], it can be time-consuming. Additionally, the RPN criteria, particularly the severity rating scale, should be tailored to the nuclear industry.

3. In Step 3 (“Identify Unsafe Control Actions”), Control Actions (CAs) are analyzed to identify Unsafe Control Actions (UCAs). It can be challenging to match UCAs with the right system expert for validation, as certain experts are best suited to review UCAs related to specific system elements. When UCAs are presented as a plain list, it becomes difficult to see which UCAs are tied to which parts of the system, making it harder to involve the appropriate experts.

4. Effective use of STPA requires a software tool that integrates all analysis phases and connects to both the input and generated output information. Although STPA’s traceability is often highlighted [3], the method will only be truly effective within NPP SE if its traceability feature extends beyond STPA itself. This level of integration and data management is not achievable with word processors or pen and paper. Only a dedicated software tool can ensure that information remains reusable, transparent, and accessible across SE activities, enabling STPA results to support continuous system development and collaboration among experts.

In this paper, we address these limitations, and find ways for smoother integration of STPA into nuclear SE. We introduce the basic concepts of STPA and SE in chapters 2 and 3. We then explore how STPA can contribute to various phases of a NPP’s life cycle in chapter 4. Chapter 5 lists our suggested enhancements to the STPA process. Finally, we present our conclusions in chapter 6.

2. SYSTEMS-THEORETIC PROCESS ANALYSIS

In 2012, Leveson [5] introduced STPA to address the dynamic nature of systems, where interactions between system elements can lead to unforeseen and undesired outcomes. The methodology focuses on identifying Unsafe Control Actions (UCAs) and analyzing their underlying causes.

The steps of the latest STPA process are illustrated in Fig. 1. A key feature of the method is its use of a hierarchical visualization, known as the control structure, which maps the flow of Control Actions (CAs) and feedback between system components. This structure, exemplified in Fig. 2, depicts all system elements and indicates whether they send or receive CAs or feedback. While STPA does not directly propose specific countermeasures, it is a powerful tool for pinpointing critical loss scenarios and guiding efforts towards proactive risk prevention [1].

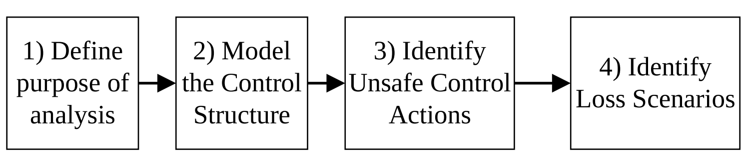

Figure 1: Four steps of STPA method [3]

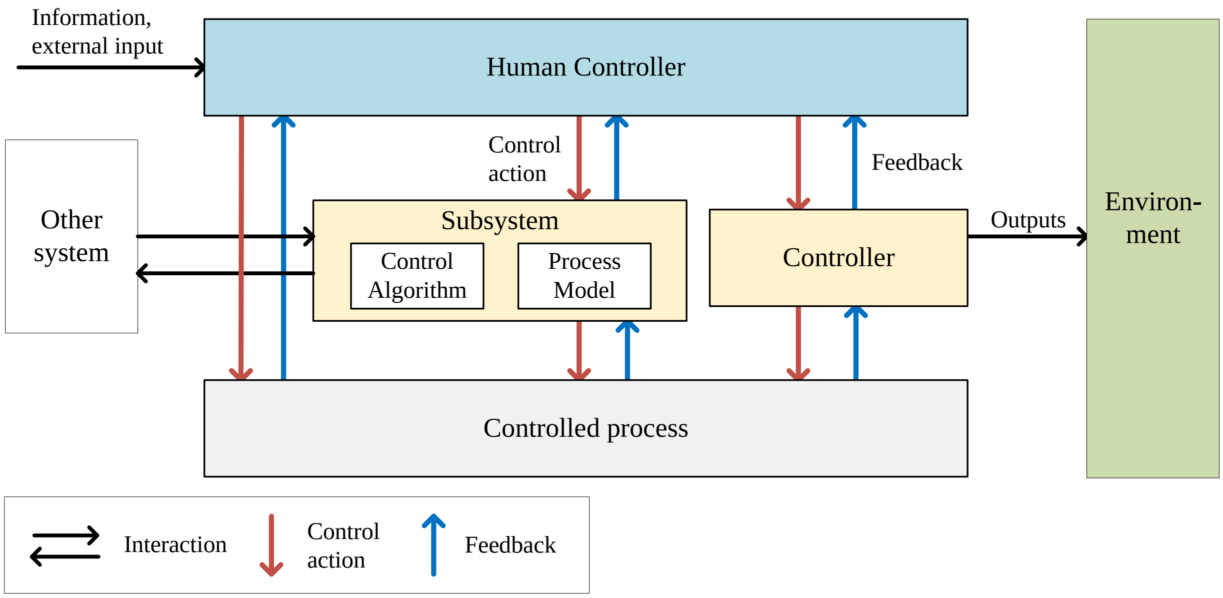

Figure 2: Generic STPA control structure (modified from [6])

3. SYSTEMS ENGINEERING

SE is an interdisciplinary approach that organizes and guides the design, development, and lifecycle management of complex systems [3]. SE provides structure to various engineering process and disciplines, aiming to improve project outcomes, and ensures that systems meet stakeholder needs, budgets, and timelines. Central to SE is "systems thinking," which considers each part as connected within a larger whole, requiring collaboration across disciplines and iteratively refining information and decisions step-by-step until all requirements are met [7,8].

The V-model, or "Vee-model," is a framework used in SE to illustrate the sequence of key project phases. Shaped like a "V," it visually represents the progression of a project from left to right over time. The model begins on the upper left with high-level system planning, focusing on requirements analysis, system design, and defining specifications, while moving to more detailed levels. As the project reaches the bottom of the "V," the components and subsystems are fully designed. The right side of the V then emphasizes integration, testing, and evaluation, to verify that initial requirements defined on the left side are met. This ensures, that the final system functions as intended when manufactured and deployed. Throughout the process, iterations are conducted to ensure that risk management assessments are completed and implemented, and to confirm that any proposed changes remain acceptable to stakeholders [8].

SE plays a vital role in NPPs due to the complexity of coordinating diverse stakeholders and technical disciplines. Stakeholders can include owners, designers, suppliers, builders, operators, regulators, societal representatives, grid managers, and unions. On the technical side, expertise is needed across fields such as I&C, safety, security, probabilistic analysis, process design, electrical systems, operations, maintenance, construction, and hazard analysis. Adding to this complexity, NPP projects often span decades, meaning the individuals involved at the start may not see the project through to its completion, operation, or decommissioning. To remain competitive with alternative energy sources, NPPs must be faster, cheaper, and more efficient to construct and operate. SE helps achieve these goals by enabling safe, secure, and cost-effective implementation of innovations and operational improvements. Additionally, NPPs are subject to licensing requirements. The structured application of SE provides clarity, completeness, and transparency, facilitating effective communication and understanding between licensing authorities and applicants. Its systematic processes for managing information and knowledge ensure continuity and coherence across all phases of a nuclear facility's lifecycle [7].

4. THE ROLE OF STPA IN NPP SE

As highlighted in the STPA Handbook [3], STPA can be integrated into any phase of the standard V-model. Fig. 3 demonstrates how the ideas in [3] could apply to SE activities for NPPs. The arrow at the top reflects the technical SE processes an NPP should follow throughout its lifecycle as recommended by IAEA [7].

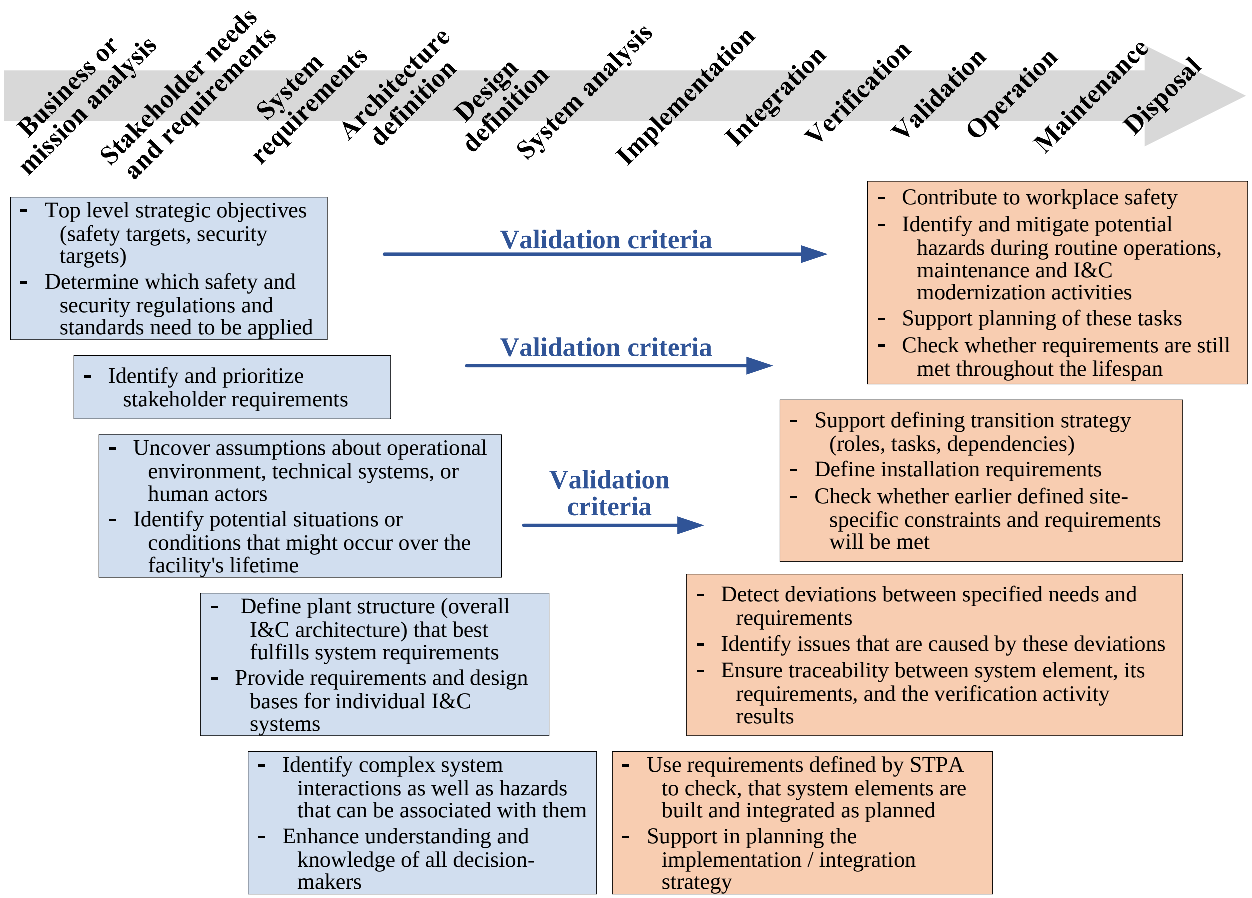

Figure 3: Potential ways STPA could contribute to nuclear I&C system life-cycle stages (restructured from [3] and [7])

In the business or mission analysis process, STPA can help define high-level strategic goals related to safety and, with the STPA cybersecurity extension [9], security as well. It can assist in selecting relevant regulations and standards to follow from the start. Applying STPA at this early stage supports the identification of key stakeholders and essential services needed for training, operation, maintenance, outages, and renovation. Additionally, it can clarify initial assumptions about environmental conditions and requirements, and highlight logistical needs that must be addressed.

In the process of defining stakeholder needs and requirements, STPA can facilitate stakeholder discussions, helping to identify and possibly even prioritize their needs. This applies to a broad range of nuclear facility stakeholders (including facility owners, operators, electrical grid managers, regulators, local authorities, vendors, facility personnel, and the wider community) as well as I&C stakeholders (process engineers, systems engineers, operators, maintenance staff, plant architects, layout designers, power supply engineers, and I&C suppliers).

In the next phase, stakeholder requirements are translated into practical, verifiable system requirements, which need to be of the highest quality as they form the basis for numerous technical processes. STPA can help uncover assumptions made by various stakeholders regarding the operational environment, technical systems, or human actors, as well as identify potential situations or conditions that might occur over the facility's lifetime so they can be addressed in the system requirements. Therefore STPA could help ensure that system requirements are unambiguous and complete.

While [7] separates the architecture definition and design definition phases, Fig. 3 combines these steps to illustrate how both benefit from iteratively conducted STPAs. The architecture definition process identifies plant systems and their interactions, setting the stage for the design definition process, which refines these outcomes into detailed data and specifications for each I&C system. The architectural solutions must fulfill the objectives set in the business or mission analysis and the previously defined system requirements. This overall architecture then sets requirements and design foundations for individual I&C systems, addressing redundancy, diversity and separation for fault tolerance, data communications, platform and component selection, sizing, and cyber security [7]. Specifically, Step 2 of STPA ("Model the control structure") [3] is valuable for defining the overall architecture by visualizing system interactions and identifying critical functions and key human actions. Similarly, STPA can guide the architecture definition process for each I&C system, ensuring alignment with essential safety and operational criteria.

The main focus of the system analysis phase is to ensure seamless integration by coordinating information and system requirements between connected systems and subsystems. The goal is to identify key integration information that decision-makers must be aware of. For example, the reactor protection system (RPS) [7], in addition to its own measurements, also interfaces with other I&C systems to monitor parameters such as neutron flux, and also transmits its own signals to other systems. The RPS, upon need, then initiates actuation of the required functions. STPA could be particularly valuable here for identifying, modeling, and analyzing such complex interactions, command flows, feedback loops, and potential hazards within integrated systems. Additionally, since STPA relies on close collaboration with system experts, it naturally provides an ideal framework for enhancing the knowledge and understanding of all decision-makers involved.

The implementation and integration phases, which the IAEA [7] recommends treating as separate, are combined here (and in Fig. 3) because STPA can take similar roles in both. In the implementation phase, individual system elements are developed as planned during the design definition phase, while in the integration phase, these elements and components are assembled and made to work together as outlined in the architecture and design phase. A key part is verifying that all requirements and specifications are met. For both phases, integrators could use STPA's earlier identified system requirements to verify whether components have been assembled as instructed and integrated as planned. Additionally, STPA can proactively aid in defining the implementation and integration strategy by identifying critical dependencies, and potential risks that require attention.

The purpose of the verification process is to provide objective proof that the system or its elements adhere to specified requirements. This is achieved through e.g., formal verification [10], code inspections, structural and functional tests, unit tests, system tests, and workstation-based simulations [7]. The process goes beyond detecting deviations, by identifying problems, that can be caused by these deviations and offering information for corrective action. STPA can play a valuable role in the verification phase by providing a reference to earlier defined specifications to detect deviations from the original requirements. Further, the tool can help identify deficiencies that arise from these deviations and offer insights on how to correct them. Also, STPA's traceability feature could enhance the process's overview, by linking each system element to its requirements and the results of verification activities.

In the transition process, STPA can play a multifaceted role. This phase marks the shift from developing the NPP facility to preparing it for real-world use ensuring that all necessary resources, including personnel and systems, are in place for ongoing operation. It requires collaboration among various stakeholders, including facility designers, plant systems specialists, suppliers, operators, and regulators, and across different disciplines such as site preparation, logistics, construction, system integration (e.g., power grid), training, and commissioning [7]. STPA can assist in defining the transition strategy by identifying the key participants, specifying their roles, tasks, inputs, interactions, dependencies, and deliverables, and setting the overall schedule. It also helps determine the training requirements for personnel to ensure smooth operation and support. Furthermore, STPA can define installation requirements and verify that earlier identified site-specific constraints and requirements are met.

The objective of the validation phase is to confirm, that while in its intended environment the system meets it's goals and stakeholder requirements [7]. STPA can be used as a reference to confirm outputs from business or mission analysis process and from stakeholder needs and requirements definition process, respectively. Since the validation process is typically implemented alongside other processes, Fig. 3 does not explicitly separate STPA's role in this phase.

Key contributions of STPA during the operation, maintenance and disposal phase include identifying and mitigating potential hazards during routine operations, maintenance and I&C modernization activities as well as the planning of these tasks. It can also be used to analyze near-misses, monitor for operational constraints, and check whether requirements are still met even under changing conditions throughout the lifespan. For disposal planning, STPA can pinpoint required I&C functions and equipment, such as fuel pool cooling systems, monitoring systems, and power supplies, that must remain operational during disposal [7].

5. IMPROVEMENT SUGGESTIONS TO STPA

This chapter provides a series of recommendations for modifying STPA to enhance its usability and facilitate its integration into the previously described phases of the NPP systems engineering efforts.

Modification suggestion 1: We propose an additional step to STPA, STPA Step 5: "Transforming loss scenarios into verifiable system requirements". This step aims to ensure, that upon formulating, or cross-checking the loss scenario with a system expert a first approach for a solution is drafted. We consider this useful because the person cross-checking the loss scenario will likely already have some initial ideas about potential solutions. While we do not expect a fully developed solution to be delivered during this session, we recommend leveraging the system expert's momentum by providing a platform for them to document their initial thoughts and ideas or bring this to the attention of a suitable responsible person. This ensures that if there are hundreds of loss scenarios, valuable time is saved by avoiding the need to search for and identify specific scenarios later. If STPA is integrated into a larger SE software, this step can also serve to link documents, regulations and legislation that hold parts to the answer, facilitating easy access.

Modification suggestion 2: When STPA experts hand over lengthy lists of loss scenarios, especially to decision-makers who were not involved in the process, it can leave them unsure where to start. The task of turning these loss scenarios into meaningful system requirements may appear harder than it is. Therefore, we propose introducing a filtering method for underlying factors in loss scenarios. In practice, this means that already when formulating loss scenarios, one can highlight or link the key system element(s) affected by or contributing to the scenario. When tasked with revising the loss scenarios one can then take advantage of filtering the loss scenarios and group them to common underlying factors for more efficient follow-up. Such a feature not only enables more focused analysis but could also visually highlight weak or loss-prone system elements, which may require extra attention. Applying this feature to a case study [2] filtered 73 loss scenarios for the system element "recirculation control valve", 106 loss scenarios for the automated controller "Low-power controller", and 178 loss scenarios for the human controller "operator".

Modification suggestion 3: In addition to the previously mentioned filtering function, we propose an risk-based prioritization of loss scenarios. Specifically, we suggest that, during the formulation of loss scenarios, their severity is roughly estimated and represented by, for example, using a simple color code (e.g., yellow, orange, red). This three-level risk ranking provides a quick estimation of the severity of the worst-case consequences associated with each scenario. This prioritization method is significantly faster than the RPN approach [4], because it focuses solely on the estimation criterion of severity, reducing the complexity of the assessment. Another key advantage is that it avoids the risk of overlooking potential scenarios that might otherwise be filtered out prematurely during the application of the RPN method in Step 3 [1]. Further, such a lighter version of risk estimation might be especially useful when using STPA for managerial decisions such as those made during business or mission analysis, stakeholder needs and requirements, but also when formulating the implementation and integration strategy. While we have tested this approach in a confidential case study within the mobile work machine industry, the concept for how such an interface could appear can be adapted from Fig. 4.

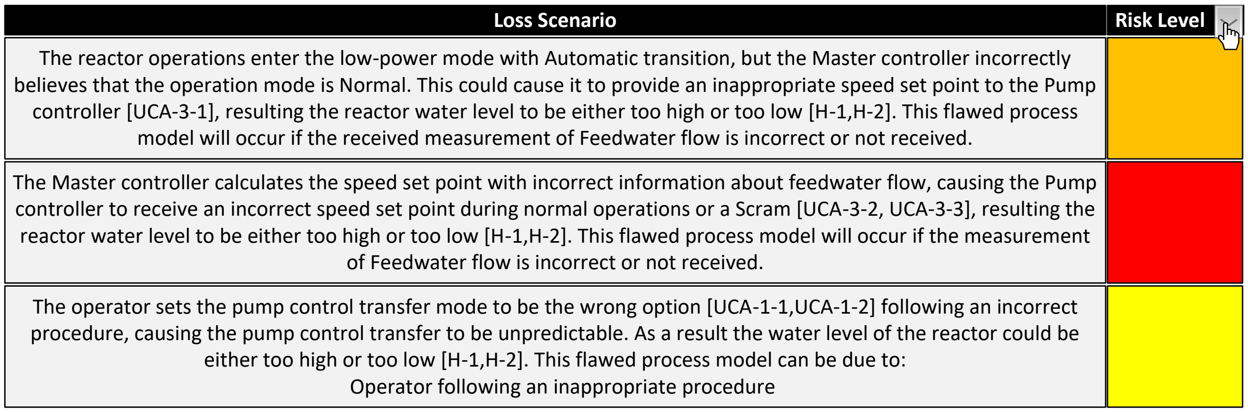

Figure 4: Risk-based prioritization.

Modification suggestion 4: For Step 3 and Step 4, we recommend that the textual descriptions of UCAs and loss scenarios, respectively, include links to their associated system elements. Hovering over these elements could display additional information, such as technical specifications (valve types, system(s) and functions(s) which monitor or control the valve, pressures, can it be manually controlled, and if, then from where (control room / field)), or list relevant sections in the operator manual to provide quick and convenient context. Fig. 5 illustrates how such a feature could appear when integrated into a software tool.

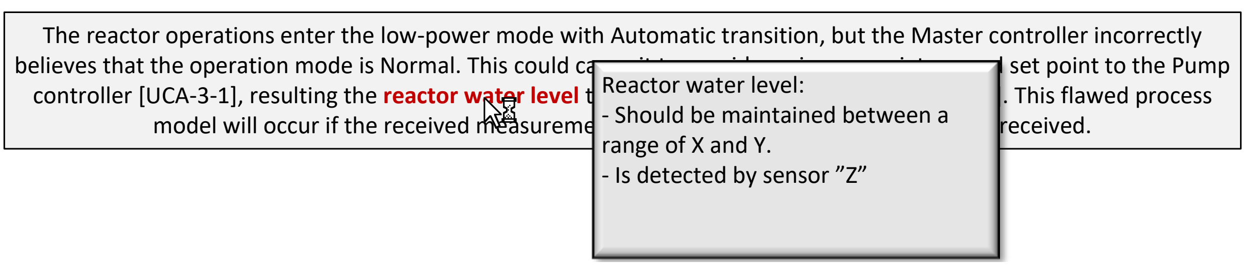

Figure 5: Software feature to leverage STPA's traceability

Modification suggestion 5: For large systems, where multiple system experts are involved, easy identification of areas where each expert can contribute is crucial. To support this, we propose a feature in the control structure that uses color coding to differentiate types of interactions, such as human-human, human-technical system, and technical system-technical system. This functionality is particularly useful when refining interactions, for example, to distinguish which operator interacts with specific parts of the system in cases where multiple individuals have similar roles. Additionally, we propose that when a specific UCA or loss scenario is being worked on or reviewed, its associated CA, feedback loop, or system element are visually highlighted within the control structure. This ensures users can easily locate and reference the relevant part of the system, streamlining navigation and enhancing context during the analysis.

From experiences made in our previous STPA work in the nuclear [1,2], mining [11], and mobile work machine industries [12], we conclude that tools like MS Word, MS Excel, MS Visio, or even their combined use cannot fully harness the capabilities of STPA. To truly benefit from STPA, a dedicated software tool is essential. Such a tool should be designed to support different types of users, as STPA involves more than just experts specializing in the method. System experts or component specialists should be able to contribute directly to parts of the analysis after being introduced to its basics by an STPA expert. At the very least, the tool should enable STPA experts to efficiently present the analysis outcomes to system and component experts for cross-checking. Additionally, decision-makers play a key role in defining system safety requirements. During collaborative sessions, the tool must enable intuitive and smooth back-and-forth navigation, allowing users to revisit the control structure, jump between loss scenarios, focus on specific CAs, UCAs, or system elements, and seamlessly verify results and formulate requirements. Fig. 6 shows a simplified UML Use Case diagram for a potential STPA software design, illustrating which user groups are primarily interested in specific aspects of the STPA process.

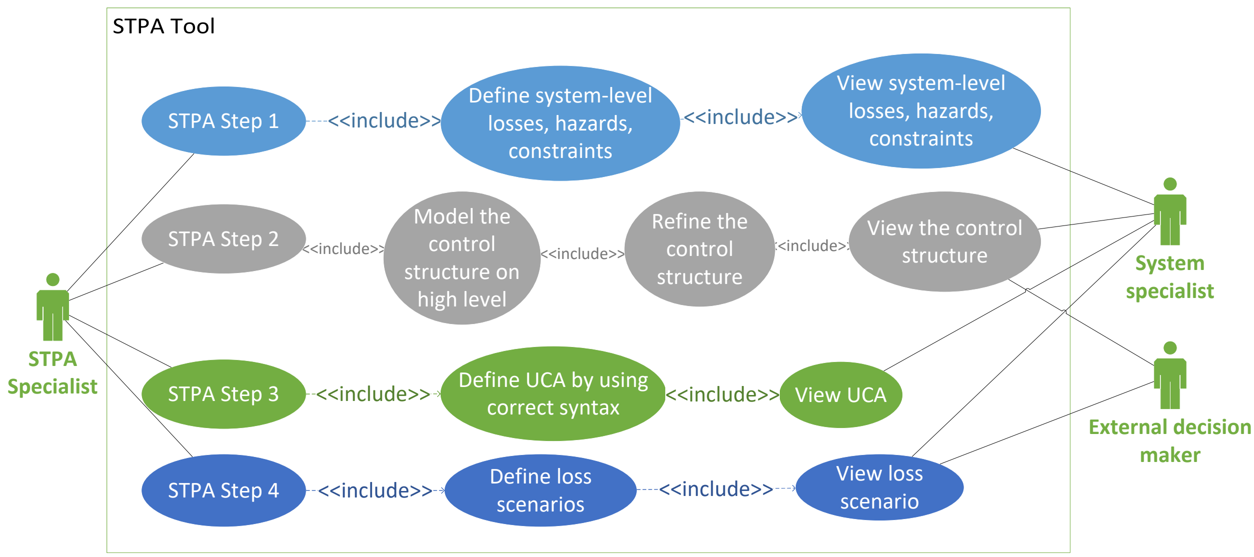

Figure 6: Simplified UML Use Case diagram for potential STPA software.

6. CONCLUSIONS

STPA has demonstrated its utility in identifying risks in NPP I&C systems. Its strengths lie in visualizing system-level control structures, uncovering interactions among technical components and human operators, and offering insights into complex feedback loops. We believe these strengths can be further leveraged by expanding the STPA method from its current focus on isolated I&C use cases to becoming a tool for broader SE processes. By doing so, STPA could give insights that support management decisions and planning throughout all SE phases.

Currently, STPA is mainly used during the conceptual design phase of SE [13], regardless of the domain. We recognize the need for more research into its application during later SE phases, such as organizational design, developmental testing [14], verification and testing [15], and validation.

Furthermore, we understand that due to strict NPP security requirements, only carefully vetted commercial software tools can be utilized. This drives the development of in-house software solutions hosted on secure servers, a challenge that aligns with the contribution of this work. Our improvement suggestions primarily focus on modifications to the STPA method itself in order to increase usability throughout the whole SE life cycle.

A comprehensive list of software requirements derived through requirements engineering process can be found in [16], which not only identifies over 30 software requirements for a potential STPA tool, but also compares existing software solutions against these requirements. While various STPA software tools exist with differing degrees of usability [17], we emphasize the pressing need for tools specifically tailored to the stringent security and lifecycle integration needs of the NPP domain.

ACKNOWLEDGEMENTS

This work was supported by the Finnish National Nuclear Safety and Waste Management Research Programme 2023-2028 (SAFER2028).

REFERENCES

[1] J. Berger, R. Tiusanen, H. Kothalawala and A. Pakonen, "Applying priority-informed STPA to a nuclear I&C system," *29th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2024)*, Padova, Italy, Sept. 10-13 (2024).

[2] H. Kothalawala, *Application of System-Theoretic Process Analysis (STPA) in Nuclear Instrumentation and Control Systems*, Master's thesis, Aalto University (2023).

[3] N. Leveson and J. Thomas, *STPA Handbook* (2018).

[4] H. Kim, M. A. Lundteigen, A. Hafver and F. B. Pedersen, "Utilization of risk priority number to systems-theoretic process analysis: A practical solution to manage a large number of unsafe control actions and loss scenarios," *Journal of Risk and Reliability*, **235** (1), pp. 92-107 (2021).

[5] N. Leveson, *Engineering a safer world: Systems thinking applied to safety*, MIT Press, Cambridge, MA (2012).

[6] J. Berger, "STPA Guide", VTT Research Report, no. VTT-R-00848-23, VTT Technical Research Centre of Finland, (2024).

[7] IAEA, "Introduction to Systems Engineering for the Instrumentation and Control of Nuclear Facilities", IAEA Nuclear Energy Series No. NR-T-2.14 (2022).

[8] INCOSE, *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 4th edition, John Wiley & Sons (2015).

[9] T. Malm, J. Berger, R. Tiusanen, A. Ranta, J. Seppälä, B. Silverajan and H. Zhao, "Comparison of cybersecurity and functional safety risk assessments", VTT Research Report, no. VTT-R-00499-24, VTT Technical Research Centre of Finland (2024).

[10] Pakonen, A., Tuominen, L., Viitasalo, M. and Nuutinen, P. "Formal Safety Assessment Methods in Olkiluoto 1&2 NPP I&C Renewal Project DIMA," submitted to: *14th Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2025),* Chicago, IL, June 15–18 (2025).

[11] J. Berger, R. Tiusanen and T. Malm, "Assessing an automated mining operation with STPA," *Safety of Industrial Automated Systems (SIAS 2024)*, Tampere, Finland, June 12-16 (2024).

[12] J. Berger, "STPA Guide", VTT Research Report VTT-R-00848-23 (2024).

[13] C. H. Fleming and N. Leveson, "Integrating systems safety into systems engineering during concept development," *INCOSE International Symposium*, **25** (1), pp. 989-1003 (2015).

[14] D. C. Horney, *Systems-theoretic process analysis and safety-guided design of military systems*, Master's Thesis, MIT, (2017).

[15] A. Abdulkhaleq, S. Wagner and N. Leveson, "A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA", *Procedia Engineering*, **128**, pp. 2-11 (2015).

[16] A. King, *Assessing the Suitability of Software Tools for the System-Theoretic Process Analysis of Nuclear Instrumentation and Control Systems*, Master's thesis, Aalto University (2024).

[17] "MIT Partnership for Systems Approaches to Safety and Security (PSASS) – STAMP Tools," https://psas.scripts.mit.edu/home/stamp-tools/, (2022).