Applying priority-informed STPA to a nuclear I&C system

Josepha Berger, Risto Tiusanen, Hiruni Kothalawala, Antti Pakonen

Citation:

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

DOI: 10.1109/ETFA61755.2024.10710653

Applying priority-informed STPA to a nuclear I&C system

Josepha Berger, Risto Tiusanen
VTT Technical Research Centre of Finland Ltd.
Tampere, Finland
josepha.berger@vtt.fi;
risto.tiusanen@vtt.fi

Hiruni Kothalawala
Design Engineer, Filter Automation Metso Finland Oy
Espoo, Finland
hiruni.kothalawala@metso.com

Antti Pakonen
VTT Technical Research Centre of Finland Ltd.
Espoo, Finland
antti.pakonen@vtt.fi

***Abstract*— The transition from analog to digital instrumentation and control systems in nuclear power plants introduces increased complexity, and functionality and consequently new types of risks. Systems Theoretic Process Analysis (STPA) aims to uncover losses caused by inadequate control measures between system elements and could therefore help identify control flaws also in Instrumentation and control (I&C) systems. Our objective is to assess the method's effectiveness in the context of a nuclear power plant's digital feedwater control system use case. We highlight the completeness of the hierarchical control structure of the use case, as a substantial part of the analysis relies on its content. The perspective of STPA viewing safety as a control problem offers valuable insights into the instrumentation and control use case. Altogether more than 140 unsafe control actions and 400 loss scenarios were identified originating from 18 control actions. STPA generates numerous unsafe control actions and loss scenarios but lacks inherent prioritization. The absence of a distinction between important and minor hazards treats all findings equally in terms of criticality for safety requirements and system design considerations. As a result, we tested the risk priority number approach and recognized its utility in screening and prioritizing these findings. This proves beneficial when allocating resources for safety considerations in digital instrumentation and control systems within the nuclear domain.**

Keywords—STPA, Risk Priority Number, I&C systems, Nuclear power plant

I. INTRODUCTION

Instrumentation and control (I&C) systems can be seen as the central nervous system of a nuclear power plant (NPP)[1]. This is because I&C systems affect every aspect of a plant's normal, abnormal, and emergency operation. I&C systems for example perform control, service and monitoring functions related to the operation of an NPP and consequently consist of sensors, actuators such as valves and motors, communication, surveillance, and diagnostic as well as control, regulation, and safety systems. As analog, electromechanical I&C systems approach obsolescence, their modernization and replacement by digital systems are inevitable [2]. Nevertheless, these new digital I&C systems, due to their size, complexity, and increased functionality, introduce new challenges including unintended software behaviors and component interactions [1], [3]. It is no longer sufficient to examine system components separately and in isolation, as done by many traditional hazard analysis methods (fault tree analysis (FTA) [4], failure modes and effects criticality analysis (FMECA)[5], event tree analysis (ETA)[6], and hazard and operability analysis (HAZOP)[7]). In complex systems, such as the I&C systems of NPPs, losses may not necessarily occur due to component failures but rather as a result of unpredictable and undesired interactions among system elements [8], [9]. Systems Theoretic Process Analysis (STPA), grounded in system theory, aims to address this complex, non-linear way of how losses can arise. As a result, the method could be well-suited for identifying control flaws also in I&C systems [3]. Our objective is to verify if the latest version of STPA can identify new types of risks effectively in a process control system setting. Through our work, we aim to support the Finnish Nuclear industry in their evaluation of integrating STPA to their safety practices.

The Electric Power Research Institute's (EPRI) 2013 report [3] highlighted STPA as one of the five relevant hazard analysis method for digital I&C systems. However, a newer version of STPA was since published in 2018 by Leveson [8]. In our study, we applied the newest version of STPA to gain practical experience, evaluate its applicability for a digital I&C system use case, and develop improvement ideas for the STPA methodology. The system under investigation includes human as well as automated controllers. We did not consider existing safety measures such as redundancy, as we align with Leveson's intention for STPA to function as a worst-case analysis method. STPA is designed to help prevent hazards regardless of the presence of these safety features. Moreover, safety features themselves may cause unpredictable behavior [8].

In this paper we investigated the level of information necessary to design a hierarchical control structure for the given use case. We concentrated our efforts on performance of the STPA, including data collection and the analysis technique. While we extensively cross-checked some findings with the use case provider, resource constraints limited a thorough examination of all results. Additionally, we applied the Risk Priority Number (RPN) approach on a subset of STPA results to evaluate whether their screening and ranking could guide resource allocation in the STPA process and aid in developing system safety requirements. Further, we wanted to investigate and understand whether STPA could be a valuable tool to identify system requirements and safety goals for I&C systems in NPP environments.

II. PRELIMINARIES

A. STPA

According to [8], STPA is implemented in four stages (Fig. 1 a): defining the analysis' purpose, modeling the control structure, identifying the *unsafe control actions* (UCA), and finally describing *loss scenarios*. The initial step, the definition of the analysis' purpose, is guided by the sub steps of defining losses, system-level hazards and system-level constraints. If the analysis benefits a more detailed perspective, the hazards and constraints may be refined optionally. Losses act as a steering mechanism for the analysis, as they determine which hazards the STPA practitioner should focus on and investigate. In STPA, hazards are the states a system can be in just before the loss might manifest. Step 2, the modelling of the control structure, sets the stage for the actual hazard analysis. The control structure, an example of it can be viewed in Fig. 4, is a hierarchical representation of all system elements, including components like controllers, sensors, and actuators. Downwards arrows represent commands, so called *control actions* (CA). CAs are transmitted from elements with more hierarchical power to the ones with less. Feedback streams, upwards arrows, represent information that is collected and passed forward to support the decision-making of controllers. Inputs from outside the system under investigation must be included if their neglect otherwise leads to an incomplete representation. The objective of STPA Step 3 is to pinpoint the contexts in which the earlier identified CA may become unsafe. This step results in a list of UCAs describing the combination of conditions that could lead to their realization. STPA steers the analysis for UCAs by declaring four different types in which a CA might become unsafe. The types being, the UCA is "Provided", "Not provided", "Provided, but at the wrong time" (too early, too late, or in the wrong order), and "Provided for an inappropriate duration" (for too long or for too short). STPA gives special attention to CAs by dedicating Step 3 to the identification how assumingly suitable and safe CA can become unsafe. But also, physical components, feedback, other inputs, and controllers themselves can trigger UCAs, and ultimately give rise to losses. Step 4 addresses this gap by examining all system elements for their potential to induce UCAs and cause loss. The outcome of this analysis is a set of textual descriptions known as "loss scenarios." These loss scenarios show causal relationships between the contributing factors that give rise to a loss, essentially explaining how system elements can result in the realization of one or more losses that were identified in step 1.

B. Risk Priority Number (RPN)

Many traditional hazard analysis methods, such as HAZOP, FMECA, and PHA (Process Hazard Analysis), incorporate the RPN approach to assess and prioritize hazards. In contrast to traditional methods, STPA, while resulting in a substantial number of UCAs and loss scenarios—often ranging in the hundreds or thousands based on the level of detail in the control structure—lacks an inherent procedure for prioritizing its findings. The absence of a distinction between important and minor hazards means that all UCAs and loss scenarios are treated equally in terms of criticality. Researchers from the Norwegian Centre for Research-based Innovation on Subsea Production and Processing (SUBPRO) recognized this limitation and proposed additional steps to the STPA method, introducing criteria adapted from the RPN approach in traditional risk assessment methods [10]. In our study, we applied a trial run to test SUBPRO's proposed methodology (Fig. 1 b) for screening and evaluating UCAs and loss scenarios.

Taking advantage of STPA's top-down approach, as opposed to the bottom-up approach of traditional methods, this methodology minimizes the workload by identifying and eliminating unnecessary scenarios early in the analysis. By incorporating RPN-based prioritization, less relevant UCAs can be screened out already in the middle of the analysis, which minimizes the originally required efforts in STPA Step 4 as less loss scenarios must be identified. Consequently, resources can be focused on the creation and prioritization of the remaining loss scenarios. UCAs are evaluated by multiplying an estimation of (1) severity, (2) available time to respond, and (3) strength of knowledge on UCA (Fig. 1 b 3-2). Loss scenarios are evaluated by multiplying the corresponding UCA RPN with an estimation of (4) likelihood and (5) strength of knowledge on loss scenario (Fig. 1 b 4-2). Each evaluation criterion's estimation ranges from 1 to 5, whereas a lower number resembles less severe damage (1), a slow transition time between an UCA results in a loss (2), strong overall knowledge of the analyst on UCA (3), respectively on loss scenario (5) and the event to happen rarely (4). The criterion of strength of knowledge reflects the level of confidence or certainty in predicting the occurrence and outcome of an event. This adaptation is in line with Flage & Aven's recommendation to consider uncertainty as a prerequisite for successful quantitative risk assessment [11].

While SUBPRO's RPN approach effectively prioritizes UCAs and associated loss scenarios, it lacks a mechanism for ranking loss scenarios from sources like system elements or feedback. Our study, with nearly 100 such scenarios, brings out the need to extend the RPN approach for these cases. Adapting the STPA methodology with SUBPRO's approach for these scenarios requires adjustments, as they lack a specific UCA RPN factor. Our methodology addresses this gap by multiplying an estimation of likelihood with an estimation of the strength of knowledge to establish an RPN for scenarios from feedback or system elements. However, direct comparison with RPNs from the standard method is not feasible due to the different calculation formula.

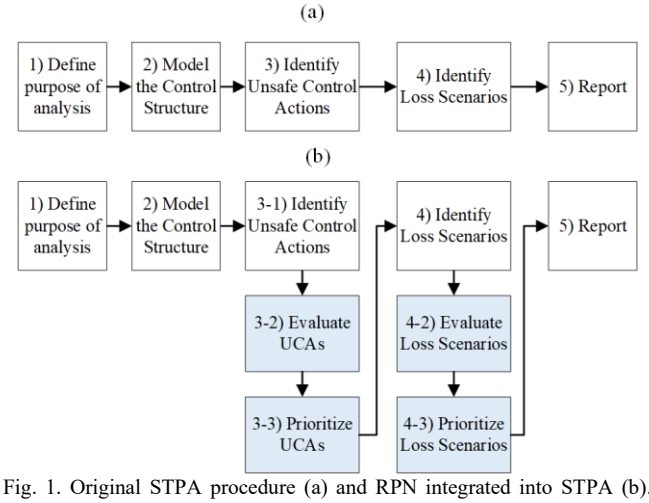


Fig. 1. Original STPA procedure (a) and RPN integrated into STPA (b). (modified from [10])

III. Related Research

STPA was initially introduced to the nuclear domain by the method's creator [12], [13]. The study applied STPA to a generalized Pressurized Water Reactor, successfully identifying design flaws. Moreover, the study highlighted STPA's ability to uncover the necessary mental model guiding a human operator's decision-making process. Since then, STPA has been utilized to assess various other digital I&C systems in NPPs [14], [15], [16], [17], [18], [19].

Similarly, in a context parallel to our use case, a study carried out in Switzerland employed STPA in examining the feed water level control I&C system of a nuclear power plant's steam generators [17]. However, their methodology is grounded in Leveson's 2011 version of STPA [9]. This particular case study exclusively addressed automated controllers and omitted analyzation of human controllers. Additionally, their study did not consider the different power states a NPP can undergo and focuses rather on the methodology than the completeness of the case study.

The EPRI report determined that no single method adequately met all the objectives for a comprehensive safety and security analysis of digital I&C systems. In response to this finding, further research was initiated, through a collaboration between Sandia National Laboratories and EPRI. Researchers have identified potential in combining STPA with Failure Modes and Effects Analysis (FMEA), as well as STPA with FTA and to encompass the identification of cybersecurity risks in critical infrastructure [20]. The resulting methodology combines STPA and FTA into a unified and systematic framework known as Hazard and Consequence Analysis for Digital Systems (HAZCADS) [21].

Recognizing that STPA, as a worst-case analysis method, does not inherently address the complexity of redundant design, which is crucial in digital safety systems, researchers around Bao & Zhang developed a risk assessment process termed Redundancy-guided System-Theoretic Hazard Analysis (RESHA) [22], [23], [24], [25], [26]. RESHA combines a redundancy-guided modification of STPA, HAZCAD and other methods from hazard analysis, reliability analysis and consequence analysis into this new risk assessment process for digital I&C upgrades. The STPA is a fundamental component of RESHA and focuses on the identification of software common cause failures.

Researchers have recognized the need to prioritize the many results obtained from STPA [19], [27], [28]. Some proposed different methods for prioritization [10], [29], [30], [31]. For example, [30] tried to turn the qualitative STPA results into a measurable optimal control problem, while [31] suggested using statistical model-checking to analyze risk for hazardous scenarios identified through STPA. This process includes a systematic translation from the STPA results to formal models suitable for a statistical model-checking tool. However, for our specific case and data, we found the RPN approach to be the most practical, as this approach gives us a straightforward way to prioritize STPA results that fits well with our study's needs and context [10].

IV. Case Study

A. Feedwater Control System

The I&C feedwater control system of the Boiling Water Reactors (BWR) Olkiluoto 1 and 2 NPP served as use case to our study. It regulates the flow of feedwater into, and consequently the water level in the reactor vessel. There, the heat generated by fuel rods transforms the feedwater into steam. This steam powers turbines, which, in turn, drive generators that produce electricity. Following this, the steam is condensed back into water in a condenser and returned to the reactor vessel via feedwater pumps. The total feedwater flow is the water that leaves the condenser and is available to flow through control valves into the reactor. A portion of this flow goes back to the condenser, allowing for precise control of the feedwater flow into the reactor vessel (Fig. 2).

The feedwater control system receives input signals from various components, including transducers installed in the feedwater circuit, monitors, and the safety systems of the plant. Key input measurements reported to the feedwater control system include reactor water level, total steam flow, feedwater flow, feedwater pump speed, and control valve positions. Actuators such as feedwater pumps, control valves, and shutoff valves are activated by the system's corresponding output signals.

Depending on the different operational states of the NPP, the feedwater control system can switch between three automated control modes: (1) Normal operation, (2) Low power operation, and (3) Reactor Scram (emergency shutdown). These modes are executed by different controllers of which the Master controller and Low power controller have the highest level of control. The Master controller is in charge during normal power operation and during Scram (Fig. 3 a), whereas the Low power controller controls the feedwater pumps during low power operation and the valves constantly, independent from the operational states (Fig. 3 b). Master and Low power controller execute their specific control strategies through Slave controllers. However, manual human operator control is required when feedwater flow falls below 3 kg/s, which is primarily during reactor start-up and shutdown procedures.

B. Application of STPA on Feedwater Control System

1) STPA Step 1

The first step of STPA necessitates gaining a comprehensive understanding of the system under investigation. Therefore, expertise in both the specific use case and the STPA process is required. In our case, technical documentation and system expertise was provided by Teollisuuden Voima Oyj (TVO).

The purpose of our analysis, summarized in Table I, is to identify situations that cause the reactor water level to deviate from the specified level, either exceeding or falling below it. Such an undesired system state is deemed a system-level hazard and must be prevented as it may result in the specified losses. As defined by the list of losses, the analysis focuses on safety related scenarios, and does not encompass situations that effect e.g., the power production. Visualized with square brackets ([ ]), each system-level constraint is designed to

handle the respective hazard and specifies on a higher level how to prevent these undesirable system states.

TABLE I. PURPOSE OF THE ANALYSIS

System-level Losses	System-level Hazards	System-level Constraints
L-1 Injuries to humans L-2 Exposure to radiation L-3 Damages to the plant equipment and components	H-1 Reactor Water level falls below the minimum required level [L-1],[L-2],[L-3] H-2 Reactor Water level exceeding the maximum allowed level [L-1],[L-2],[L-3]	SC-1 Reactor Water level should be maintained above the minimum required level [H-1] SC-2 Reactor water level should be maintained below the maximum allowed level [H-2]

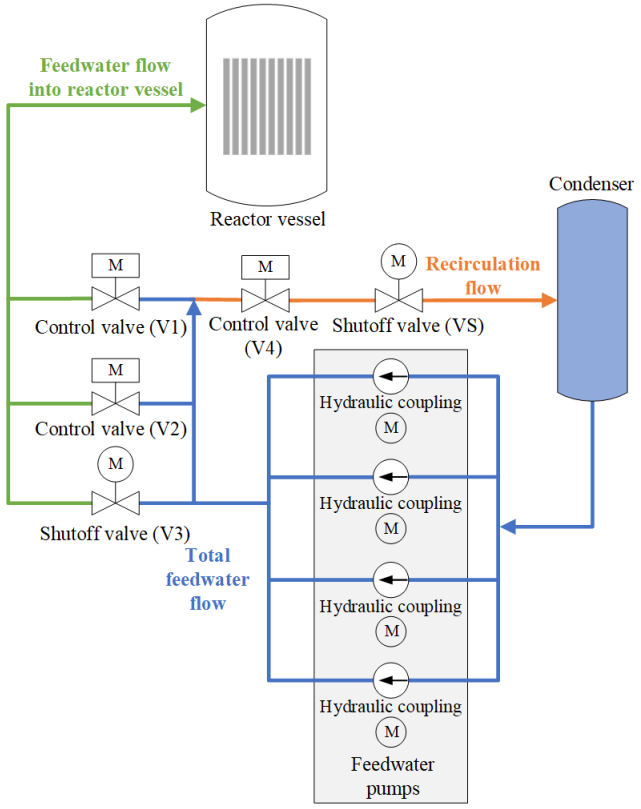
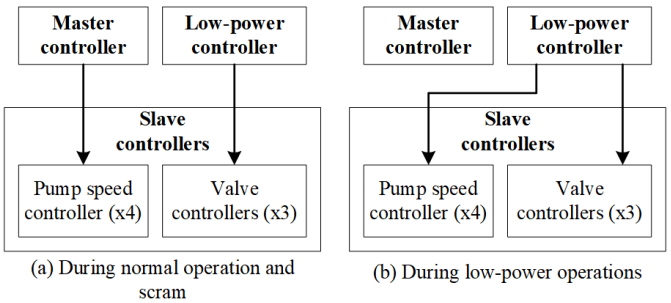


Fig. 2. Feedwater System.



(a) During normal operation and scram

(b) During low-power operations

Fig. 3. Controller behavior during different operation modes.

2) STPA Step 2

The final control structure has been modelled through several rounds of refinement with MS Visio. Color coding highlights different system elements. Main source of information were textual descriptions of the system's operation during different power states. Discussions with system experts ensured the use case is hierarchically correctly represented having enough detail and yet not being overly complex. Fig. 4 shows an extract of the control structure. The full control structure is available in [32].

3) STPA Step 3

In this step, each CA depicted in the control structure was analyzed for under which conditions it might turn into UCAs. Key considerations when defining the context were the different operating modes the NPP can enter (Normal operation, Low power operation, and Reactor Scram) and the consequent switch of controllers in charge, as well as the possibility for manual operation.

Table II is an example of how one control action e.g. CA-3 can result in multiple UCAs. CA-3 labels the command from Master Controller to Pump Controller to adjust the pump speed to a certain set point. This command should be given when the Master controller is in charge, which is during normal power operation and scram modes. However, in some UCAs the command is given during an inappropriate control mode, too late, or not at all. Altogether more than 140 UCAs were identified originating from 18 CAs.

TABLE II. UCAS THAT ORIGINATE FROM CA-3

Provided	Not provided
UCA-3-1: The master controller provides the pump speed set point to the Pump controller during the Low power operation. [H-1, H-2] UCA-3-2: The Master controller provides an incorrect pump speed set point to the Pump controller during Normal operation. [H-1, H-2] UCA-3-3: The Master controller provides an incorrect pump speed set point to the Pump controller during a Scram event. [H-2]	UCA-3-4: Master controller does not provide the pump speed set point to the Pump controller point during Normal operation. [H-1, H-2] UCA-3-5: Master controller does not provide the pump speed set point to the Pump controller point during a Scram event. [H-2]
Provided at wrong time	**Provided for an incorrect duration**
UCA-3-6: The Master controller provides the pump speed set point to the Pump controller too late after a Scram event is initialized. [H-2]	N/A

4) STPA Step 4

We retrieved the list of loss scenarios by brainstorming the combination of various worst-case factors. In our case, we identified more than 400 such scenarios, some of which are straightforward and related were grouped together for clarity. Notably, loss scenarios tied to physical system elements, such as sensors and actuators, proved particularly suitable for grouping, due to their directness, and conciseness. This is exemplified by loss scenario-400 in Table III. Loss scenario-34 exemplifies one of the ten identified loss scenarios associated to UCA-3.1. Each loss scenario refers to the

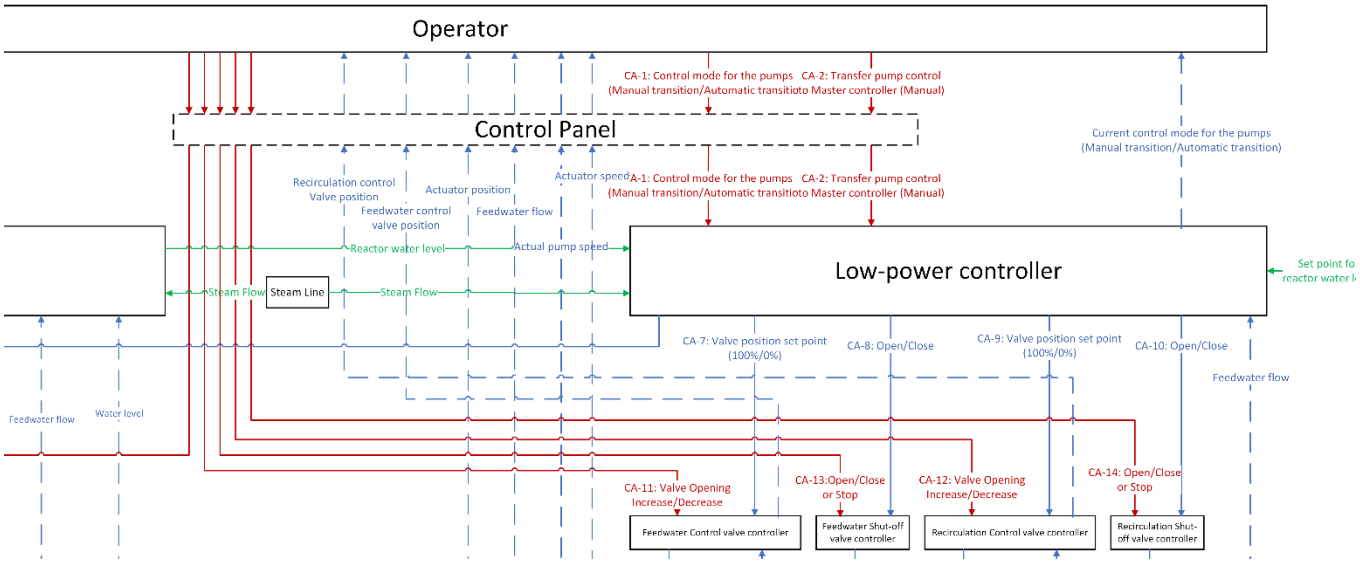


Fig. 4. Extract of the hierarchical control structure.

corresponding system element and hazard. The complete list of loss scenarios can be viewed as appendix in [32].

TABLE III. LOSS SCENARIOS

Loss Scenario-34	The reactor operations enter the low-power mode with Automatic transition, but the Master controller incorrectly believes that the operation mode is Normal. This could cause the Master controller to provide an inappropriate speed set point to the Pump controller [UCA-3-1], resulting the reactor water level to be either too high or too low [H-1, H-2]. This flawed process model will occur if the received measurement of Feedwater flow is incorrect or not received.
Loss Scenario-400 (Pump Actuators)	Mechanical failures in the pump actuators. [H-1, H-2] Errors made during maintenance and repair. [H-1, H-2] Failure of power supply to the pump actuator. [H-1, H-2]

C. *Application of RPN approach on STPA results*

The official STPA analysis concludes with the creation of loss scenarios. However, not all loss scenarios are equally relevant for general system design considerations and for upgrading the old I&C systems to digital I&C systems in NPPs. Therefore, prioritizing the STPA results supports the allocation of resources to relevant UCAs and Loss scenarios.

Instead of integrating the RPN approach directly into the STPA, we opted for a trial run where RPN was applied afterward to a selected set of UCAs and their resulting loss scenarios. In a workshop setting, system experts, representing TVO, provided their estimations for each evaluation criterion.

This study focused specifically on investigating the UCA RPNs for all UCAs originating from CA-1 and CA-3. This approach allowed us to efficiently screen out minor UCAs and proceed with estimations for the remaining loss scenarios. CA-1 and CA-3 were chosen because they represent CAs given by a human operator and an autonomous operator, respectively. CA-1 represents the human controller's decision to either operate manually or to enable the low-power controller for automatic operation. (Fig. 4).

Drawing from our experience in defining UCA RPNs, we determined it was safe to disregard all loss scenarios originating from a UCA RPN smaller than 12. A UCA RPN of 12, in the range of 1 to 125, appears to be low, but nevertheless indicated the potential for a severe loss, emphasizing the need for careful considerations in system and I&C design. This observation highlights the nuclear industry's heightened sensitivity to risk. However, it also suggests that the RPN approach in the nuclear sector could benefit from a finer resolution of estimation. In our workshop, system experts felt, that SUBPRO's estimation of severity is relatively coarse for the nuclear industry, and this could be an area of improvement.

Moreover, the deduction of UCA RPNs associated with UCA-1 proved to be considerably more time-consuming compared to estimating RPNs for UCA-3. This discrepancy arises from the nature of UCA-1, which involves a human operator. Given the wide range of possible actions by a human operator, even though the UCAs were thoroughly described, the estimation of evaluation criteria was not as straightforward as with the CA given by the master controller.

Furthermore, when determining the RPN for loss scenarios linked to system elements and feedbacks, we obtained results that could be ranked, marking our adjustment to the RPN approach as a success. Our trial was conducted for a water level sensor—a physical system element—and the actuator position, which serves as feedback for the position sensor.

V. Discussion

As noted by [17], establishing a comprehensive system boundary proves challenging in Step 1 alone. However, the design of the control structure in Step 2 has proven instrumental in refining the analysis' scope. The iterative nature of STPA facilitated seamless adjustment of the control structure without negative impacts. In fact, the traceability feature greatly eased the modification of the control structure. An important observation is that as we add more details to the control structure, the analysis requires more resources. We acknowledge information that serves the construction of the control structure as crucial when considering type and amount of data needed for STPA. The control structure is integral, as a substantial part of the analysis relies on its content [19]. Decisions to omit specific CAs need careful consideration, as neglecting them may result in overlooked UCAs and subsequent loss scenarios. We rely on our system experts' estimation when claiming that our hierarchical control structure accurately represents the use case.

The perspective of STPA viewing safety as a control problem offers valuable insights into the I&C feedwater control system. Throughout the analysis, system experts reflected on the system design. Given that the system under investigation is used in the Olkiluoto 1 and 2 NPP we assert that STPA is suitable to initiate discussions also about already existing and well-established systems. Although we did not exploit available methodologies [33] on mental models, STPA enabled the identification of human factor related loss scenarios.

In our analysis 18 CAs lead to the identification of a significant amount of UCAs and loss scenarios. Comparably high numbers [27], [34], [35] have been retrieved in studies, that investigated complex systems, typically with no simplifications of the various operational states and with considerations of a human controller. In retrospective, the consumption of the resource time could have been minimized by integrating RPN into STPA. However, we argue, that in order to perform cuts at the appropriate places (remove UCAs from analyzing their potential to cause loss scenarios) system experts must be deeply involved throughout the process. In our case, due to restricted availability of system experts, they were mainly involved in the very beginning of the analysis and in cross-checking selected results during the RPN approach. Referring to insights from our NPP experts, a severity rating of 2 is deemed highly significant in the nuclear industry. Consequently, the granularity of evaluation criteria should be tailored to the specific system under investigation. Based on our joint modeling exercise with TVO experts, we can affirm that the criteria themselves have demonstrated suitable for the digital feedwater control I&C system. We hope this aids [10] in investigating the possibility of establishing a universal set of STPA RPN criteria.

The documentation of UCAs and loss scenarios inherently involves numerous repetitions and cross-references, highlighting the importance of robust traceability. Echoing the sentiments of [17], we strongly advocate for the application of STPA using a software tool. We documented our findings in MS Excel, however, the platform's limitations hindered the effective utilization of traceability. We claim that proper tool support enables STPA practitioners to focus on analysis rather than being preoccupied with avoiding confusion among Excel rows. Overall, we recognize the potential of utilizing retrieved loss scenarios as valuable inputs for system design and defining safety requirements.

Left unnoted so far is the role of IT security when digitalizing analog I&C systems. Cyber-attacks could cause digital I&C systems to malfunction in ways that are outside analyzed failure modes, even causing simultaneous failure of multiple Defence-in-Depth levels. Adversaries could also obtain critical data to facilitate sabotage. [36] Attempts to modify or extend the STPA methodology ([37], [38], [39]) to include the analysis of security related aspects deserve further attention.

VI. Conclusion

We acknowledge STPA for its ability to identify risks originating from inadequate control measures. However, performing STPA is a time-intensive process. Industry experts share the opinion, that screening UCAs seems to rather shift the workload towards estimating criteria than reducing it. Nonetheless, we want to highlight, that industry experts do recognize the benefits of integrating RPN approach to STPA. The efforts invested in prioritization become beneficial when using STPA results to formulate system safety constraints, safety goals, or influence system design.

Future research shall encompass how software tools can enhance the application of STPA in digital I&C systems specifically in the nuclear domain. This exploration is intended to be combined with the development of a strategy for structuring and formalizing STPA findings. Aim shall be to produce STPA results that enable safety and design experts in NPPs to accurately interpret and seamlessly translate these results into safety requirements, and system design goals.

Acknowledgment

This work has been funded by the Finnish National Nuclear Safety and Waste Management Research Programme 2023-2028 (SAFER2028). The case study was provided by TVO. We wish to thank Lauri Tuominen and Pekka Nuutinen of TVO for valuable discussions, support, and feedback.

References

[1] IAEA, "Introduction to Systems Engineering for the Instrumentation and Control of Nuclear Facilities - Nuclear Energy Series No.NR-T-2.14," 2022. doi: 978–92–0–128522–5.

[2] IAEA, "Instrumentation and Control (I&C) Systems in Nuclear Power Plants: A Time of Transition - NTR2008 Supplement," 2008. Accessed: Oct. 12, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:18513593

[3] ERPI, "Hazard Analysis Methods for Digital Instrumentation and Control Systems - Technical Report 3002000509," Jun. 2013. Accessed: Nov. 30, 2023. [Online]. Available: https://www.epri.com/research/products/3002000509

[4] International Electrotechnical Commission, IEC 61025:2006 Fault tree analysis (FTA). 2006.

[5] International Electrotechnical Commission, IEC 60812:2018 Failure modes and effects analysis (FMEA and FMECA). 2018.

[6] International Electrotechnical Commission, IEC 62502:2010 Analysis techniques for dependability - Event tree analysis (ETA). 2010.

[7] International Electrotechnical Commission, IEC 61882:2016 Hazard and operability studies (HAZOP studies). 2016.

[8] N. Leveson and J. Thomas, STPA Handbook. 2018.

[9] N. Leveson, Engineering a Safer World. Massachusetts Institute of Technology, 2011.

[10] 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," Proc Inst Mech Eng O J Risk Reliab, vol. 235, no. 1, pp. 92–107, Feb. 2021, doi: 10.1177/1748006X20939717.

[11] R. Flage and T. Aven, "Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA)," Reliability & Risk Analysis: Theory & Application, vol. 132, 2009, [Online]. Available: https://www.researchgate.net/publication/228623141

[12] J. Thomas, F. Luiz De Lemos, and N. Leveson, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants - Research Report: NRC-HQ-11-6-04-0060," 2012. Accessed: Nov. 30, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:9986772

[13] J. Thomas and N. Leveson, "A New Approach to Risk Management and Safety Assurance of Digital Instrumentation and Control Systems," American Nuclear Society Conference, 2013.

[14] M. T. Rowland, L. T. Maccarone, and A. J. Clark, "Using the Information Harm Triangle to Identify Risk-Informed Cybersecurity Strategies for Instrumentation and Control Systems," Nucl Technol, vol. 209, no. 3, pp. 471–487, 2023, doi: 10.1080/00295450.2022.2087841.

[15] A. Shukla, X. Gao, and Y. Z. Ayele, "STPA-Based Safety Approach on the Emergency Ventilation System in Nuclear Power Plant," in Proceeding of the 33rd European Safety and Reliability Conference, Singapore: Research Publishing Services, 2023, pp. 1561–1568. doi: 10.3850/978-981-18-8071-1_P193-cd.

[16] S. H. Lee, S. M. Shin, J. S. Hwang, and J. Park, "Operational vulnerability identification procedure for nuclear facilities using STAMP/STPA," IEEE Access, vol. 8, pp. 166034–166046, 2020, doi: 10.1109/ACCESS.2020.3021741.

[17] M. Rejzek and C. Hilbes, "Use of STPA as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants," Nuclear Engineering and Design, vol. 331, pp. 125–135, May 2018, doi: 10.1016/j.nucengdes.2018.02.030.

[18] C.-M. Park, K.-K. Moon, C. Chang-Hui, and S.-H. Jeong, "Application of STPA Technique to Software Hazard Analysis for Nuclear Safety I&C System," 2017. Accessed: Dec. 04, 2023. [Online]. Available: https://www.kns.org/presentation/lists/sc_field/pp_title/sc_word/application%20of%20STPA

[19] S.-M. Shin, S. H. Lee, S. K. Shin, I. Jang, and Park Jinkyun, "STPA-Based Hazard and Importance Analysis on NPP Safety I&C Systems Focusing on Human–System Interactions," Reliab Eng Syst Saf, vol. 213, Sep. 2021, doi: 10.1016/j.ress.2021.107698.

[20] L. Dawson, A. Muna, T. Wheeler, P. Turner, G. Wyss, and M. Gibson, "Assessment of the Utility and Efficacy of Hazard Analysis Methods for the Prioritization of Critical Digital Assets for Nuclear Power Cyber Security," 2015. Accessed: Dec. 04, 2023. [Online]. Available: https://www.osti.gov/biblio/1252915

[21] A. J. Clark, A. D. Williams, A. Muna, and M. Gibson, "Hazard and Consequence Analysis for Digital Systems-A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants," Nov. 2018. Accessed: Dec. 04, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:215952977

[22] T. Shorthill, H. Bao, H. Zhang, and H. Ban, "A Redundancy-Guided Approach for the Hazard Analysis of Digital Instrumentation and Control Systems in Advanced Nuclear Power Plants," Nucl Technol, vol. 208, no. 5, pp. 892–911, 2022, doi: 10.1080/00295450.2021.1957659.

[23] H. Zhang, H. Bao, T. Shorthill, and E. Quinn, "An Integrated Risk Assessment Process of Safety-Related Digital I&C Systems in Nuclear Power Plants," Nucl Technol, vol. 209, no. 3, pp. 377–389, 2023, doi: 10.1080/00295450.2022.2076486.

[24] H. Bao, H. Zhang, and K. Thomas, "An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants," 2019. doi: 10.2172/1616252.

[25] H. Bao, T. Shorthill, and H. Zhang, "Hazard Analysis of Digital Engineered Safety Features Actuation System in Advanced Nuclear Power Plants Using a Redundancy-Guided Approach," in International Conference on Nuclear Engineering, ICONE, American Society of Mechanical Engineers (ASME), 2020. doi: 10.1115/ICONE2020-16573.

[26] H. Ban, H. Bao, T. Shorthill, and H. Zhang, "Demonstration of Integrated Hazard Analysis for Digital Reactor Trip Systems," American Nuclear Society, Dec. 2019, pp. 485–488. doi: 10.13182/t31017.

[27] N. A. Zikrullah, H. Kim, M. J. P. van der Meulen, G. Skofteland, and M. A. Lundteigen, "A comparison of hazard analysis methods capability for safety requirements generation," Proc Inst Mech Eng O J Risk Reliab, vol. 235, no. 6, pp. 1132–1153, Dec. 2021, doi: 10.1177/1748006X211003463.

[28] M. Chopart and A. Lališ, "System-Theoretic Process Analysis for reliability assessment: Aircraft's wheel braking system case study," Transportation Research Procedia, vol. 65, pp. 230–237, 2022, doi: 10.1016/j.trpro.2022.11.027.

[29] N. A. Zikrullah and H. Kim, "Prioritization Approach for Systems-Theoretic Process Analysis (PA-STPA) : Applied for Subsea Systems," Norwegian University of Science and Technology, Master's Thesis, 2018. Accessed: Dec. 04, 2023. [Online]. Available: http://hdl.handle.net/11250/2562563

[30] S. V. Blindheim, "Risk-aware decision-making and control of autonomous ships," Norwegian University of Science and Technology, 2023.

[31] M. Tsuji, T. Takai, K. Kakimoto, N. Ishihama, M. Katahira, and H. Iida, "Prioritizing Scenarios based on STAMP/STPA Using Statistical Model Checking," in IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2020, pp. 124–132. doi: 10.1109/ICSTW50294.2020.00032.

[32] H. Kothalawala, "Application of System-Theoretic Process Analysis (STPA) in Nuclear Instrumentation and Control systems," Master's Thesis, Aalto University School of Electrical Engineering, 2023. Accessed: Dec. 04, 2023. [Online]. Available: https://urn.fi/URN:NBN:fi:aalto-202310226581

[33] M. E. France, "Engineering for Humans: A New Extension to STPA," Master's Thesis, Massachusetts Institute of Technology, 2017. Accessed: Dec. 04, 2023. [Online]. Available: http://hdl.handle.net/1721.1/112357

[34] H. Kim et al., "Application of systems-theoretic process analysis to a subsea gas compression system," in Safety and Reliability - Safe Societies in a changing world, 2018. doi: 10.1201/9781351174664-186.

[35] N. A. Zikrullah, M. J. P. Van Der Meulen, G. Skofteland, and M. A. Lundteigen, "A Comparison of Hazardous Scenarios in Architectures with Different Integration Types," in Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, 2020. doi: 10.3850/978-981-14-8593-0.

[36] "Computer Security of Instrumentation and Control Systems at Nuclear Facilities," IAEA Nuclear Security Series No. 33-T , 2018.

[37] N. P. de Souza, C. de A. C. César, J. de M. Bezerra, and C. M. Hirata, "Extending STPA with STRIDE to identify cybersecurity loss scenarios," Journal of Information Security and Applications, vol. 55, Dec. 2020, doi: 10.1016/j.jisa.2020.102620.

[38] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," Journal of Information Security and Applications, vol. 34, pp. 183–196, Jun. 2017, doi: 10.1016/j.jisa.2016.05.008.

[39] W. Young and N. Leveson, "Systems thinking for safety and security," in ACM International Conference Proceeding Series, 2013, pp. 1–8. doi: 10.1145/2523649.2530277.