Assessing the Suitability of Software Tools for System-Theoretic Process Analysis of Nuclear Instrumentation and Control Systems

Akira King, Polina Ovsiannikova, Valeriy Vyatkin

Citation:

A. King, P. Ovsiannikova, V. Vyatkin. Assessing the Suitability of Software Tools for System-Theoretic Process Analysis of Nuclear Instrumentation and Control Systems. 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA), Padova, Italy, September 10-13, 2024. IEEE, 2024.

DOI: 10.1109/ETFA61755.2024.10710845

Assessing the Suitability of Software Tools for System-Theoretic Process Analysis of Nuclear Instrumentation and Control Systems

Akira King*, Polina Ovsiannikova*, and Valeriy Vyatkin*†
*Department of Electrical Engineering and Automation, Aalto University, Espoo, Finland
†Department of Computer Science, Electrical and Space Engineering, Lulea Tekniska Universitet, Sweden
Email: akira.king@aalto.fi, polina.ovsiannikova@aalto.fi, vyatkin@ieee.org

***Abstract*—Modernization of currently operational nuclear power plants is becoming increasingly important to maintain their performance and safety. Ensuring the safety of newer Instrumentation and Control (I&C) systems used in modernization efforts requires hazard analysis techniques suitable for the analysis of complex and software-heavy systems. System-Theoretic Process Analysis (STPA) has proven to be a suitable hazard analysis method for these complex I&C systems, however, its practical use is still often limited by its labor-intensive and time-consuming nature, partially due to the limitations of the tools used to perform the analysis: common Office tools such as Microsoft Excel or Visio. Conducting an STPA analysis could be simpler and more attractive with software tools specific to the method. This work introduces the requirements for these software tools and lays the foundation for further work, in which software tools will be evaluated against these requirements.**

***Index Terms*—I&C, nuclear power plant, software tools, STPA, process automation**

I. Introduction

In industrial processes such as those occurring in production facilities or power plants, Instrumentation and Control (I&C) systems are an integral part of their operation. They provide means of controlling the processes used to produce anything from household items to electricity. Significant advancements have been made in the technology used to implement I&C systems, namely, there has been a shift from analog and electromechanical devices to more software-heavy digital approaches.

As systems and their components age, their performance and reliability often degrades. This is also the case with I&C systems in nuclear facilities [1], such as power plants and waste management facilities. Many existing nuclear power plants are decades old and are beginning to show their age, making maintenance increasingly difficult due to the lack of spare parts [1]. In order to address these issues, nuclear power plants will eventually need to be modernized.

However, modernization comes with its own host of challenges, such as a lack of documentation for the original design and the incompatibility between new and old components. In addition, simply trying to reproduce the old system with new means may introduce faults not pronounced in the behavior of the old system but amplified in the system implemented with newer technology. These issues make redesigning a system a favorable approach to modernization. [2]

A key part of designing and developing an I&C system is ensuring that it fulfills its requirements. These requirements could relate to its adaptability, efficiency, or capacity, but in safety-critical systems such as those in the nuclear domain, the primary focus is always to ensure that the system being developed is safe. For this purpose, multiple hazard analysis methods exist and are often used, such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). Traditional methods often rely on the decomposition of the system into smaller and smaller components, and accidents are assumed to be caused by the failure of these components. [3] Accidents are seen as the result of a chain of events. Although these analysis methods are suitable for assessing the hazards related to earlier I&C systems, modern, software-intense I&C systems are more complex and require alternative hazard analysis methods.

The need to ensure that modern, complex systems satisfy their requirements as intended has led to the development of System-Theoretic Process Analysis (STPA), which is based on the System-Theoretic Accident Model and Processes (STAMP) [3]. In addition to the hazards identified using traditional hazard analysis methods, STPA can be used to identify hazards that are not only related to failures in individual components, but also those related to inaccurate process models and problematic interactions within systems [4], [3]. This lends itself well to complex systems, such as nuclear I&C systems, where hazards often emerge from complex interactions rather than the failures of individual components [3]. STPA is one of the methods that could be used during the design and development of new I&C systems for nuclear power plants, and previous work has identified STPA as providing significant and valuable data on nuclear I&C systems [5], [6].

Although STPA is a powerful tool for analyzing systems and making sure that they meet their requirements, it is still often carried out using simple "pen and paper" –approaches or common Office tools such as Excel spreadsheets. This impedes the conduct of the analysis and the utilization of its results, making it harder to implement as a part of the design and development process. A suitable software tool could ease the adoption of STPA throughout the I&C system's lifecycle by improving the manageability of the analysis process and the usability of the results. This work presents the initial findings

on requirements for STPA software tools for I&C system analysis. Further work will explore existing software tools, determine the requirements for STPA software tools to be used in the Finnish nuclear industry, and assess the suitability of existing software tools against these requirements. The remainder of the paper is structured followingly. In Section II the background of the work is elaborated, Section III describes the issues currently faced with STPA, Section IV presents the general requirements for software tools, and Section V concludes the paper.

II. Preliminaries

A. STPA

STPA is a system-theoretic approach to hazard analysis. In this approach, systems are seen to consist of a hierarchical structure of controllers that control a process. A controller may, for example, be a human, an organizational, or a computational entity. Each controller sends control actions to the processes below which, in return, send feedback to the controllers above. In STPA, safety is viewed as a control issue, that is, safety is compromised when the system is unable to control the process adequately. [3]

To clarify the process of conducting an STPA analysis, Figure 1 presents a brief overview of the steps to follow. During Step 1 the purpose of the analysis is determined. This encompasses the definition of system boundaries, losses to be addressed in the analysis, as well as the hazards and constraints of the system. In Step 2, the control structure is modeled. This is a hierarchical view of the system consisting of the processes that are controlled and the controllers. The control actions identified in the control structure are used to generate unsafe control actions (UCAs) in Step 3. Step 4 uses the UCAs as a basis for identifying loss scenarios. Figure 1 also presents how all the results produced by the STPA method can be traced back to the hazards and losses defined at the beginning of the analysis. [3][7]

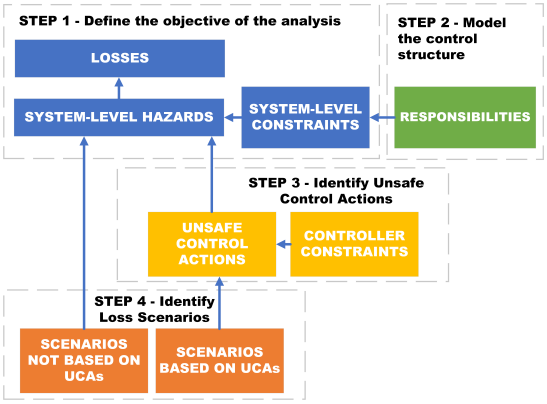

Fig. 1: A diagram demonstrating the steps and the traceability of the results of an STPA analysis.[3] [5]

B. The nuclear domain

The nuclear domain is characterized by many standards and laws that govern it. Different international and national organizations exist to determine guidelines for all aspects of nuclear power from nuclear system design to waste management. On an international level, such organizations include the International Atomic Energy Agency and the World Nuclear Association. At the national level, the Finnish nuclear industry is governed by STUK, the Radiation and Nuclear Safety Authority. They provide the YVL guides, which determine many of the constraints for the nuclear industry in Finland [8].

In the scope of this work, the nuclear domain defines the environment in which STPA could be integrated. The approach to this integration is being investigated in a concurrent work. From a legislative point of view, STUK strictly requires probabilistic risk analyses (PRA). STPA, if used, would be applied in combination with a variety of other risk analysis methods. Rather than a standalone procedure, STPA should therefore be a part of a larger system engineering effort, where it may be referred back to, iterated, or repeated. Ideally, traceability should be easy to confirm from the choices made in system design, implementation, manufacturing, and operation to the hazards and losses identified by STPA.

III. Practical STPA issues

In this section, an overview of identified practical issues in conducting STPA analyses is presented, as well as planned work in identifying further practical issues. Currently, identified practical issues are largely based on the experiences of the authors highlighted in prior work [9][5], however further issues are to be identified from international research literature and through cooperation with industry experts.

One of the key aspects of the STPA method is the traceability of its results. Each of the loss scenarios generated by the method can be traced to its respective unsafe control actions, which can be traced to system-level hazards, which in turn can be traced to system-level losses. Similarly, the responsibilities and safety constraints generated by the method can be traced back to hazards and losses. However, there remains a significant degree of complexity in the results when the analysis is carried out manually. When combined with a low level of abstraction in the control structure that defines the analysis, data can be difficult to manage and understand. This issue also relates to the documents produced and used during the analysis.

Another issue in conducting an STPA analysis is the expansive nature of its final results, namely the loss scenarios produced in Step 4. Even systems analyzed at higher levels of abstraction may generate hundreds of loss scenarios. In the nuclear domain, the Master's thesis by Kothalawala [5] identified *more than 300 loss scenarios* from a reactor feedwater control system. These results are then typically documented in an Excel Spreadsheet, whose deciphering requires a highly focused individual. A comparison of the hazard and operability study method (HAZOP) and STPA [10] identified that the text-heavy nature of STPA hindered group work necessitated by the method. These concerns are also confirmed by a 2013 EPRI technical report, which also points out that the STPA method can produce large tables of intermediate results [4], though the report was published before the revisions to the STPA method.

Although conducting an STPA analysis may be intuitive for those familiar with the method, prior work has identified that it may have a steep learning curve for beginners due to the deep understanding required to employ the method [10]. Understanding the method requires at minimum a basic understanding of system-theoretic concepts and specific knowledge of the method itself. In the context of I&C systems, engineers may be more familiar with other hazard analysis techniques [4]. Those who are experienced with other forms of hazard analysis may have a hard time breaking out of old habits. The handbook addresses many of these common mistakes; for example, in the definition of hazards, it is easy to generate hazards that are too specific [3]. Conducting an STPA analysis also requires the knowledge of experts in multiple fields, as well as someone who facilitates the analysis itself [3]. Previous work has also identified that some of the free and available STPA software tools were more suitable for STPA-experienced users and suggested that new users to the method may benefit more from the rudimentary approaches to conducting the analysis [5]. This highlights the importance of well-thought-out software tools that are approachable to users. Considering these aspects, software tools could also provide a platform for comprehensive guidance on conducting an STPA analysis.

Further issues with STPA will be identified through interviews with STPA experts on its application in I&C system use cases. Some shortcomings of the method itself will be addressed in Section IV in to differentiate them from the issues presented in the current section relating to more practical aspects.

IV. Determining requirements

In this section, the general requirements for a software tool are outlined. These requirements are largely based on the practical issues discussed in Section III. The requirements for a software tool have previously been determined [11], but the requirements were based on a previous version of STPA and were concerned with the needs of agile development. Further work will refine and validate the general requirements presented here in workshop sessions together with STPA practitioners in the nuclear industry. Table I presents key points regarding requirements and their respective sources.

TABLE I: A table demonstrating findings and proposals related to the requirements for an STPA software tool and their sources.

Requirement related findings and proposals	Source
Traceability: Robust traceability is needed to ease the documentation of UCAs and Loss scenarios	[9]
Traceability, Prioritization: It is hard to get a quick overview of the most important hazards	[10]
Traceability, Prioritization: Filtering for example by priority could be beneficial	[5]
Prioritization: Prioritization benefits using STPA results to formulate system safety constraints, safety goals and to influence system design	[9]
Prioritization: Prioritization could help address and use the results of the analysis	[5]
Customizability: Current software tools suffer from limited customizability	[5]
Integration: Software tools should be integrated into the toolchain to reduce human error	[12]

A. Traceability

The built-in approach to traceability in STPA concerns how different results are annotated. Each item, such as a hazard, a constraint, or an unsafe control action, is given an intuitive and unique abbreviation, and their descriptions are followed by the abbreviations of the items they trace back to. For example, an unsafe control action may be written as follows: ”UCA-5-1: The operator increases the pump speed in manual operation, when the pump speed needs to be decreased [H-2]” [5]. Although this form of traceability is simple and unambiguous, it remains difficult to manage in Excel sheets when dealing with large sets of data, and more robust traceability could ease the documentation of UCAs and loss scenarios [7]. The unambiguity of a result may also be easily compromised without the context of the control structure; the example above could be interpreted to concern a single pump, while in the original analysis this UCA was related to a pump controller and 3 separate pumps.

The software that supports the STPA method should make the most of the traceability of the different results produced during the analysis. For example, it could be useful to visualize quickly all the scenarios related to a certain hazard, assumptions upon which requirements are based, countermeasures to a loss scenario, or filter hazards by their relation to the control structure. Moreover, providing a view of the control structure relevant to the results to be inspected could reduce the ambiguity of the results by presenting their necessary context in an accessible manner.

As was pointed out previously in this paper, traceability could be extended beyond the scope of the STPA analysis itself to the decisions made based on the analysis in, for example, system design. This kind of traceability could mean that the software tool should be integrated as a part of a larger software suite used for system engineering [12].

B. Prioritization of loss scenarios

For complex systems such as I&C systems in nuclear power plants, an STPA analysis would likely produce hundreds if not thousands of loss scenarios. The STPA analysis performed on a simple reactor feedwater system produced more than 300 loss scenarios [5], and this system constitutes just one of many subsystems required for the operation of a nuclear power plant.

However, not all loss scenarios are equally critical; some scenarios may be more important to focus on than others. In prior work, prioritization has been recognized as something worth investigating [7][5]. This could be achieved, for example, by combining STPA with other risk assessment methods such as PRA, whose use is required by STUK for nuclear power plant licensees in Finland. In a condensed STPA Guide [7] it is proposed that different risk assessment methods could be used in conjunction with STPA at different stages of development. One approach suggested in the guide is to determine a Risk Priority Number (RPN) for each unsafe control action, and then to each related loss scenario.

Ideally, software tools would be able to help in the prioritization of loss scenarios, or at the very least they should be able

to support some of the methods that may be used to this end. Software tools could provide useful insight by, for example, filtering results by priority. [5]

C. Customizability

In addition to the prioritization of loss scenarios, many other modifications have been suggested to the STPA method to extend its capabilities. For example, STPA-SafeSec was proposed to address both the safety and security of cyber-physical systems [13]. Another proposal suggested an extension to STPA called "STPA-Engineering for Humans", which provides guidance to better take into account human interactions in complex systems [14]. Through personal communication with industry risk analysis experts, it was also found that STPA is not always strictly performed according to the structure described by Leveson in the STPA Handbook [3]. Industry experts may approach STPA in ways that they find convenient, such as by documenting recommended courses of action directly with the loss scenarios. This was demonstrated to the authors by experts working at the Fortum Power Company.

A software tool for conducting STPA analysis should ideally be able to support alternative approaches to STPA and allow the user to have some flexibility in conducting the analysis. Prior work [5] also noted a lack of customizability as an issue in current software tools. In practical terms, the software may benefit from not being excessively restricting in terms of the data fields associated with the STPA results, or it could support plugins for alternative STPA approaches such as STPA-SafeSec or the RPN approach discussed in the previous section.

D. Additional requirements

In addition to customizability, prioritization of loss scenarios, and traceability, other aspects of software tools may be important, such as a well-thought-out user interface, user guidance, or compatibility with existing software and systems. The latter overlaps with some of the points presented in the requirement for traceability, namely that decisions based on the analysis should be traceable back to the analysis and its specific results. Approaches, such as RAAML (Risk Analysis and Assessment Modeling Language) [15], have been developed to better integrate STPA into the larger system engineering effort, and support for such approaches should also be evaluated in software tools.

Additionally, initial tests with existing software tools conducted as part of this work have identified some specific requirements for software tools, such as a requirement for terminology consistent with the STPA method. These tests also confirmed the findings identified in previous work, namely that inappropriate software tools can hinder learning and the use of the STPA method [5]. This emphasizes the importance of identifying the requirements for a suitable software tool and evaluating existing software tools. Further work may refine or expand these additional requirements, or completely new requirements may be identified.

V. Conclusions and future work

Conducting an STPA analysis is often time consuming and labor intensive, especially in the context of analyzing complex I&C systems, but is rapidly becoming more relevant in part due to the need to modernize aging nuclear facilities. Much of the burden of conducting such an analysis could be reduced with an appropriate software tool. Determining the requirements for such a software tool is an important part of selecting or possibly developing a software tool for the purpose of conducting STPA analysis.

The current work has identified some of the many requirements for a suitable software tool. Further work will refine these preliminary requirements into more specific criteria and evaluate existing software tools against these requirements with case study data [5] on a reactor feedwater system.

Acknowledgments

The authors would like to express their gratitude to VTT experts Josepha Berger and Antti Pakonen for sharing their knowledge on the topics presented in this work. This work is part of the SEAMLES project, funded by the Finnish National Nuclear Safety and Waste Management Research Programme 2023-2028 (SAFER2028).

References

[1] IAEA, *Management of Ageing and Obsolescence of Instrumentation and Control Systems and Equipment in Nuclear Power Plants and Related Facilities Through Modernization*, 2022, no. NR-T-3.34.

[2] WNA, "I&C modernization: Current status and dfficulties," World Nuclear Association, Tech. Rep., 2020.

[3] N. G. Leveson and J. P. Thomas, "STPA handbook," *Cambridge, MA, USA*, 2018.

[4] EPRI, "Hazard analysis methods for digital instrumentation and control systems," Electric Power Research Institute, Tech. Rep., 2013.

[5] 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.

[6] 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, 2018.

[7] J. Berger, "STPA Guide," VTT Technical Research Centre of Finland Ltd., VTT Research Report VTT-R-00848-23, 2024. [Online]. Available: https://cris.vtt.fi/en/publications/stpa-guide

[8] STUK, "Regulatory guides on nuclear safety and security (YVL)," Available at: https://stuk.fi/en/yvl-guides.

[9] J. Berger, R. Tiusanen, H. Kothalawala, and A. Pakonen, "Applying priority-informed STPA to a nuclear I&C system," in *Proc. ETFA*, 2024, submitted for publication.

[10] E. Heikkilä, T. Malm, R. Tiusanen, and T. Ahonen, "Hazard analysis of an autonomous container handling system–a comparison of STPA and HAZOP methods," *Scientific Journal of Gdynia Maritime University*, no. 125, pp. 25–39, 2023.

[11] N. Ludvigsen, "Prototyping a digital support tool for an agile implementation of STPA," Master's thesis, NTNU, 2018.

[12] S. S. Krauss, M. Rejzek, and C. Hilbes, "Tool qualification considerations for tools supporting STPA," *Procedia Engineering*, vol. 128, pp. 15–24, 2015.

[13] 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, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212616300850

[14] M. E. France, "Engineering for humans: A new extension to STPA," Ph.D. dissertation, Massachusetts Institute of Technology, 2017.

[15] OMG, "About the risk anaysis and assessment modeling language specification version 1.0," Available at: https://www.omg.org/spec/RAAML/1.0/About-RAAML Accessed: 6.5.2024.