INVESTIGATION OF THE USE OF SYSTEM-THEORETIC PROCESS ANALYSIS AT THE NRC

September 2021

John Thomas*

In collaboration with the U.S. Nuclear Regulatory Commission
Sushil Birla, Bernard Dittman, and Mauricio Gutierrez

Contract Officer's Representative: Mauricio Gutierrez

* E-mail: jthomas@advancedengineeringservices.org

1. Abstract

System-Theoretic Process Analysis (STPA) is a hazard analysis (HA) method based on systems theory and the STAMP (System-Theoretic Accident Model and Process) model of accident (loss) causation. STPA addresses common challenges and deficiencies in modern safety and security efforts, such as common causes that can defeat diversity, dysfunctional interactions between non-failed components, unanticipated instrumentation and controls (I&C) and complex automation behaviors, flaws in design or requirements that elude testing, human errors caused by mode confusion or nontrivial human decisionmaking and causes deeply rooted in social and organizational design and culture. STPA is being used to analyze systems in nuclear power plants and to address these challenges.

This project investigates how the U.S. Nuclear Regulatory Commission (NRC) staff can best build up the capability to independently review STPA submittals from applicants and licensees and to more broadly understand the potential of STAMP-based methods. A series of seminars, workshops, and a discussion forum introduced the NRC staff to STPA and elicited feedback on the benefits, limitations, and applicability for use by the agency. The series included six seminars, four workshops, and a forum to discuss the relationship between STPA and probabilistic risk assessment (PRA).

Key findings from this investigation include the following:

- The NRC staff participants demonstrated the ability to learn the concepts behind STPA; previous experience with other HA methods did not prove to be a significant impediment.[1]
- The NRC staff participants demonstrated the ability to use STPA to discover real flaws in I&C design, requirements, and architecture that were overlooked by teams using traditional methods.
- The NRC staff participants identified and understood the potential benefit to the agency of using STPA and STAMP-based methods.
- The NRC staff participants believe that STPA is a suitable complement to existing regulatory activities and would be beneficial in regulatory reviews and oversight as in the following examples:
    - The NRC could streamline Chapter 7, “Instrumentation and Controls,” of NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (the SRP) [1], because STPA connects the analysis closely to the regulations in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, “Domestic Licensing of Production and Utilization Facilities,” especially Appendix A, “General Design Criteria for Nuclear Power Plants.”
    - The NRC could use STPA to simplify and streamline the regulatory guidance infrastructure for digital I&C (DI&C).

[1] The NRC participants experienced in other hazard analysis (HA) methods had also dealt with the limitations of these methods, which may have been a key factor contributing to their ability to learn STPA.

2. Introduction

This report documents the findings of an NRC-sponsored investigation into the use of STPA at the NRC. STPA [2] is an HA method based on systems theory that has been evaluated and applied within the nuclear industry since roughly 2011 to address unsafe interactions involving complex human, software, digital, and other behaviors in these systems [3–[*13*].

2.1 Objective

This investigation is part of a broader effort to enable the NRC staff to apply STPA [2] for evaluating the HA portion of applicants' or licensees' I&C design submittals (safety analysis report, license amendment request, or design certification document), when these submittals are based on the STPA method. As an independent regulatory agency, the NRC needs to perform an evaluation that is independent of the regulated industry.

2.2 Expected outcomes

The following five outcomes were expected from the efforts described in this report:

(1) Confirm that the STAMP-based methods are learnable as hypothesized.

(2) Identify improvements needed to make the methods learnable and usable with consistency.

(3) Identify the required quality characteristics of the information being analyzed for successful application of the methods.

(4) Identify the competence required of the users.

(5) Result in some combination of items 1–4.

2.3 Potential benefits from the use of STAMP/STPA

The findings from this investigation could lead to improved regulatory practices pertaining to safety-related DI&C. Examples include the following:

- STPA can inform the NRC-adopted risk triplet (what can go wrong? what are the consequences? what is the likelihood?). For each consequence of concern, STPA identifies "what can go wrong," including critical but complex contributing causes and common causes that lead to degradation of a safety function. In the context of networked digital systems, "what can go wrong?" has been the most challenging element of the triplet and includes "unknown unknowns." STPA can provide significant risk insights by discovering unsafe interactions and complex behaviors and by connecting them closely to the consequences (the second element in the risk triplet). It could enable the NRC to evaluate STPA-based risk-informing approaches that may be proposed by industry. The findings from STPA—such as unanticipated human error traps, flaws in design, and undocumented operational assumptions—can also inform the third element of the risk triplet, likelihood.
- Use of STPA-based test cases could improve the effectiveness and efficiency of the Integrated System Validation and Multi-Stage Validation [14] processes used or proposed to be used in the safety assurance of systems in the control room and their interactions with the operators.

- The NRC could review traditional submittals (safety analysis reports, license amendment requests, design certification documents) more efficiently by identifying the information needed for reasonable assurance and formulating requests for additional information more quickly and with less effort.

  Note that for the analysis of hazards rooted in systemic causes, STPA can be more effective than the traditional HA methods (Failure Modes and Effects Analysis, Failure Modes, Effects, and Criticality Analysis, Fault Tree Analysis) used in the nuclear industry. This has been demonstrated in other application sectors, as well as in research independent of developers of the STAMP/STPA method [13].

- The NRC could review submittals in which the applicant's or licensee's safety analysis is based on STPA.

- The NRC could streamline SRP Chapter 7 [1], because STPA connects the analysis closely to the regulations in 10 CFR Part 50, especially Appendix A.

- The NRC could improve, simplify, and streamline the regulatory guidance infrastructure related to DI&C.

Although application to cybersecurity was not within the scope of this project, the NRC staff recognized the potential and expressed interest in learning about STPA-Sec—a method that extends STPA to analyses for cybersecurity [2][15][16].

2.4 Method of investigation

Over 60 NRC staff members participated in this research, as described in Section 5, "The STPA Learning Plan." The research included a series of STPA seminars, workshops, and other engagements to introduce the STPA process, perform group exercises, review existing applications of STPA to a variety of systems and the associated results, discuss NRC needs related to STPA, and collect verbal and written feedback from the NRC staff. See Appendices A and B for feedback from opinion surveys taken at the seminars and workshops. NRC staff feedback provided insights into aspects of STPA learnability, usability, and benefits to the agency, and whether critical NRC needs may be addressed practically with STPA. Many participants also provided feedback through one-on-one discussions with the NRC project manager. The information elicited through these NRC-internal interactions clarified and expanded on feedback obtained by the principal investigator and is reflected in the findings.

3. Principal Findings

The following are the principal findings from the information collected:

- The NRC participants believe that STPA is a suitable complement to existing regulatory activities because STPA systematically analyzes areas that are not well represented in the current NRC regulatory oversight process (e.g., hazards associated with the maintenance and operation of safety systems, as well as the identification of hazards associated with emergent properties). The current version of the NRC's SRP [1] does not provide guidance to review whether such hazardous scenarios are identified and controlled.

- The NRC staff was able to learn the concepts underlying STPA.

- The NRC staff understood the potential benefit of using STPA in regulatory review and oversight.
- A small team consisting of participants with diverse complementary backgrounds, knowledge, experience, and thinking processes can achieve consistent results.

The key learnability and capability-building findings are as follows:

- STPA learning and capability-building require hands-on practice with a qualified facilitator with STPA expertise. Reading materials and standalone presentations may provide limited familiarity, but they do not enable proficiency without facilitated hands-on experience.
- Real-world examples of STPA on a variety of technical systems were important for effective learning.
- Extended question and answer sessions and open discussions with an expert STPA facilitator helped clarify key points.
- Learning can be inhibited if there is a lack of time commitment by participants (e.g., skipped sessions, multitasking during sessions). All NRC participants who were able to attend all sessions were able to meet the learning objectives. Participants who missed a lecture or a discussion reported initial confusion, and those points had to be revisited to clear the confusion.

The facilitator observed no significant learnability barriers for the NRC staff. The principal challenge noted by the facilitator was in accommodating multiple staff schedules and enabling staff attendance across all STPA sessions.

3.1 Limitations

The following limitations of this effort have been recognized:

- The STPA engagements were limited to NRC staff members who were available and able to participate when there were competing priorities and no ability to force a commitment.
- A total of 59 NRC participants attended the STPA engagements. The participants came from the following NRC groups[2]:

    1. Office of Nuclear Regulatory Research (RES)
        a. Division of Engineering
        b. Division of Risk Analysis
        c. Division of Systems Analysis
    2. Office of Nuclear Reactor Regulation (NRR)
        a. Division of Advanced Reactors and Non-Power Production and Utilization Facilities
        b. Division of Engineering and External Hazards

[2] I&C branches are included from the Office of Nuclear Reactor Regulation (NRR) and the Office of Nuclear Regulatory Research (RES).

c. Division of Reactor Oversight
d. Division of Risk Assessment

3. Office of the Chief Information Officer
4. Office of Nuclear Security and Incident Response
    a. Division of Physical and Cyber Security Policy
5. Region II—Division of Reactor Safety
6. Region III—Division of Reactor Safety

- Participants included technical reviewers, regional inspectors, researchers, and managers.

- The areas of expertise of the NRC participants included the following:

    - electrical engineering
    - mechanical engineering
    - nuclear engineering
    - PRA
    - operating experience
    - instrumentation and control
    - cybersecurity
    - information technology

- The level of experience of the NRC participants ranged from summer hires to 20+ years of professional experience.

- The STPA engagements were not designed to replace an extensive 80-hour STPA training class [17]. The STPA engagements were exploratory, designed to provide a basic exposure and familiarity with STPA, and intended to enable observations about STPA learnability, applicability, and capability. Additional training would be needed to produce skilled STPA practitioners and expert STPA facilitators.

3.2 Other observations

Additional observations have been documented in work on STPA industry adoption and best practices. The following observations summarized from Chapter 8 of the “STPA Handbook” [2] are relevant:

- Learning STPA requires practice and a “learning by doing” approach, such as hands-on learning sessions.

- The most effective STPA training is interactive with directed exercises used to reinforce the process.

- Practitioners who have been using traditional HA techniques for a long time may have the most difficulty in learning STPA. Often, some amount of unlearning may be required, and extra training may be necessary for these practitioners.[3]

[3] This is often but not always the case. Some of the top performers in the NRC STPA seminars and workshops were PRA practitioners.

- System engineers, software and digital I&C engineers, human factors, and operations specialists tend to learn STPA quickly.
- It is considered a best practice to include a qualified STPA facilitator on STPA projects. The facilitator provides method expertise, guidance, and oversight (similar to a Hazard and Operability Study (HAZOP)[4] facilitator).
- The facilitator may provide some initial STPA training at the start of the project and should be able to answer any STPA-related questions that arise during the project.
- The facilitator generally reviews the results during and at the end of the process to ensure that the method is being followed correctly and that no gaps are overlooked.
- The most effective way to produce STPA experts who can serve as future trainers and facilitators (see remaining bulleted items in this section) is to immerse candidates in real projects where STPA is actively used.
- Attending a short training class is not enough to produce STPA experts, but those who have been immersed in a few large STPA projects are candidates for future trainers and facilitators.
- One approach that has worked well is to allow one or more facilitators-in-training to shadow other STPA facilitators working on real projects.
- The facilitators-in-training learn a great deal by seeing firsthand the challenges encountered in different projects and the questions that are raised.
- STPA is best performed by an interdisciplinary team that includes expertise across the relevant areas and has access to subject matter experts as needed.
- Personalities matter when forming an STPA team. The best teams include knowledgeable experts who are open to new approaches.
- One approach to avoid a potentially adversarial relationship in an HA is to involve multiple parties (e.g., engineers, designers, and regulators) early before the design is completed and before most critical decisions are finalized and committed. STPA is able to steer critical decisions as they are made and need not be limited to an after-the-fact assessment. Other advantages of involving stakeholders in early STPA efforts include less rework, lower analysis and review costs, and increased solution space (including more effective safety-related solutions).

4. Path Forward

NRC participants in the STPA sessions wrote this section.

[4] See https://www.aiche.org/ccps/resources/glossary/process-safety-glossary/hazard-and-operability-study-hazop

4.1 Additional steps needed

Participants observed that the NRC needs to take the following additional steps to realize the benefits of STPA:

- A larger scale effort, representative of DI&C issues encountered in real-life events, is needed to further develop NRC staff skills to support STPA use in the agency's licensing and oversight activities—for example, in an independent confirmatory HA or in a review of a licensee's or applicant's HA of a safety-related DI&C system.
- Specific staff-recommended next steps include the following:
  - Select NRC projects that would benefit from STPA.
  - Identify NRC participants that should be engaged.
  - Build NRC staff skills to the level needed to perform an independent confirmatory HA or to review a licensee's or applicant's HA of a safety-related DI&C system. For example, the staff who participated fully in the STPA seminar and workshop would learn best with hands-on experience on a real-life project, launched with some coaching by an expert STPA facilitator, and occasional support from the facilitator to overcome any hurdles that may be encountered during the project.

4.2 Capabilities needed within the NRC

After the STPA seminar and workshop series, the NRC staff identified the need to build the capability to obtain risk insights for the cases of concern identified next. The "additional steps" (identified in Section 4.1) would enable the agency to build the capabilities needed.

Cases of concern identified by the NRC staff: When a safety-related system does not incorporate design diversity and its safety assurance is based substantially on a claim that all significant hazards are identified through an STPA, or a similar HA method, in the NRC's integrated risk-informed decisionmaking for licensing reviews [18], such licensing applications fall in the "type 2" category, described in Appendix C to LIC-206, Revision 1, "Integrated Risk-Informed Decision-Making for Licensing Reviews" [18]. Then, uncertainties in the safety evaluation must be reduced to a level at which the staff can conclude that the assurance is comparable to that achievable with the NRC's current criteria [1] with a margin of safety sufficient to cover for the lack of expertise with the new approach. This is the context in which the NRC staff perceived sources of uncertainty as described in the next section.

4.3 Sources of uncertainty perceived by the NRC staff

For the cases of concern identified above (see Section 4.2), the additional steps should include building the capability needed to evaluate the effects of the following sources of uncertainty perceived by the participating NRC staff:

(1) The NRC staff does not have experience in the effective use of STPA (or any similar method) on the cases of concern identified above (see Section 4.2).

(1.1) The NRC staff needs hands-on experience with the use of the HA method to evaluate it and identify the limitations and conditions within which an applicant's or licensee's safety analysis can be evaluated with consistency.

(1.2) Because the safety analysis depends on the competence of the performers or performing team, the staff needs significant hands-on experience with the HA method to understand the competence-sensitivity of the safety analysis.

(1.3) To understand the factors influencing the quality of the safety analysis, the staff needs to exercise the HA method on a real project, facilitated by a method expert.

(1.4) The staff needs additional knowledge to evaluate the effectiveness of test case generation (more generally, verification and validation (V&V) case generation) based on the HA results.

(2) The NRC does not have review guidance to evaluate an HA-based submittal for the cases of concern identified above. Experience from the hands-on, real-life project (item (1.3) above) is needed for creating the review guidance.

(3) The NRC does not have regulatory guidance for an applicant or licensee to use in preparing an STPA-based submittal for the cases of concern identified above. Experience from the hands-on real project (item (1.3)) is needed for creating the regulatory guidance.

(3.1) The Electric Power Research Institute (EPRI) has produced guidance to help industry perform STPA-based development [19][20]. If the industry proposes guidance, the NRC will still need to independently evaluate STPA-based submittals.

(3.2) The automobile and civil aviation sectors are developing standards and guides for using STPA. However, the NRC staff is not yet familiar with these developments and needs to review their evolving guidance and learn from discussion with their experts.

(4) The competence-dependence, mentioned in item (1.2), also cascades through the licensees to their supply chains, including performers, verifiers, and auditors. However, the NRC does not have sufficiently specific criteria and guidance to evaluate whether controls are adequate and personnel are qualified for the cases of concern identified above. The NRC staff does not have a good understanding of the variables affecting the quality of a STPA analysis. Experience from the hands-on, real-life project (item (1.3)) is needed to develop the criteria and guidance. A qualified, certified supply chain of components and services is needed.

(4.1) The NRC staff does not have the knowledge to identify conditions to be controlled to ensure the quality of STPA (e.g., skills to perform STPA, skills to evaluate the results of STPA). That is, the NRC does not have the criteria to evaluate the competence of the personnel performing STPA or verifying its results. The NRC's approach to reactor operator licensing could serve as a reference model.

(4.2) The NRC does not have specific enough technical criteria and guidance to evaluate whether an applicant or licensee has adequate control of HA quality in its supply chain. This includes the allocation of safety requirements down the integration hierarchy and the supply chain and the integration of analysis results up the integration and supply chain hierarchy. The supply chain includes suppliers of components, as well as services to perform HA [21].

(4.3) The NRC does not have specific-enough technical criteria and guidance to evaluate the results of HA.

(5) There are uncertainties in the quality of the information input to HA activities:

Uncertainties introduced through requirements specification: The NRC does not have consistently verifiable criteria and methods for evaluating whether safety requirement specifications are of the quality necessary for deriving the test cases (more generally, V&V cases) needed for system safety assurance, when based on HA results. If system safety assurance is based on test cases (more generally, V&V cases) derived from the requirements and constraints resulting from HA, then these requirements and constraints should be unambiguous and consistently verifiable. Criteria and guidance are needed to evaluate whether safety requirement specifications are adequate to derive the test cases (more generally, V&V cases) needed for safety assurance.

Uncertainties introduced through design and implementation: The flow down from the top-level requirements specification to architectural design, detailed design, and implementation (e.g., coding) may introduce hazardous conditions (e.g., unexpected interactions and emergent behaviors). The NRC staff needs the know-how to confirm that HA on the respective work products will be able to identify these conditions. For example, the characteristics needed for the respective artifacts to be correctly analyzable are not clear to the NRC staff. Experience from the hands-on, real-life project (item (1.3)) is needed to identify these characteristics and create appropriate review guidance.

(6) It is not clear what other evidence is needed for system safety assurance. While STPA has the potential to yield safety requirements and constraints and test cases (more generally, V&V cases) derived from them, evidence will be needed to demonstrate that these requirements are satisfied (i.e., confirmation through verification activities). In the absence of uncertainty reduction through design diversity, the NRC staff believes that current verification practice would not be adequate. Criteria and guidance are needed for verification, which would yield the evidence needed to complement evidence from HA, so that the combined evidence is sufficient for safety assurance for the cases of concern. Experience from the hands-on, real-life project (item (1.3)) is needed to identify the appropriate criteria and guidance.

In summary, the NRC's capabilities must be improved, as identified above, to obtain the risk insights needed during a safety evaluation, especially when the guidance in Appendix C to LIC-206 [18] is applied to a type 2 submittal for the cases of concern identified above.

5. The STPA Learning Plan

A series of 11 STPA sessions were held with NRC staff participants:

(1) six seminars
(2) four workshops
(3) discussion forum on the relationship between STPA and PRA

5.1 STPA Seminars

The first four seminars introduced the principles and foundations of STPA, including STAMP and the STPA process itself. The goal was to provide a basic understanding of the process, to evaluate the learnability of the process, and to equip the participants with the capability (1) to evaluate the potential benefit(s) of using STPA in licensing reviews and regulatory oversight and (2) to identify the potential barriers to its effective use at the NRC.

The STPA seminar series began with case studies in both nuclear and nonnuclear industries to demonstrate modern safety challenges and common fallacies and points of confusion that make these challenges seem intractable. The seminars also demonstrated effective models, solutions, and lessons learned from system theory, system and software engineering, human factors, and integrated (or holistic) analysis.

The STPA seminars explained the STPA process using real-world STPA examples and interactive exercises. Participants learned how the STPA process can identify nontrivial human interactions, digital interactions, and automated behaviors that lead to losses. Some examples included interactive discussions about the ability or inability of other methods to consistently identify real scenarios that caused significant events.

During one seminar, participants were given a description of a real I&C system design and asked to apply STPA individually with limited time and scope. Participants received no information about potential design problems or adverse operating experiences until the exercise was completed. The participants were asked to apply STPA to identify potential design flaws and anticipate future loss scenarios. Participants were able to ask clarifying questions about the STPA method, and the facilitator reviewed results from each individual. The results showed that all participants were able to model a simple control structure, identify basic unsafe control actions, and identify key assumptions and loss scenarios using the STPA process. The STPA results from all participants were then compared to real adverse events and design flaws that had been overlooked when the system was originally designed, reviewed, and put into operation. The results showed that the NRC participants were able to use STPA to discover real flaws and anticipate real events that were overlooked by the original designers and reviewers.

At the end of the STPA seminar series, participants were presented with a set of STPA artifacts (e.g., hazards, control structures, unsafe control actions) and asked to review them and identify any mistakes. The participants demonstrated the ability to identify common mistakes in STPA, find corrections, and use the results to generate significant questions that must be answered. The participants demonstrated a basic comprehension of the STPA process. See additional results in Section 7, “Overall Observations on Learnability.”

Qualitative and quantitative feedback was collected from NRC participants throughout the seminar series to help form the conclusions in this report. For additional information about the feedback collected, see Appendices A and B.

5.2 STPA Workshops

The workshops facilitated more intensive hands-on application of STPA by participants. The goal was to offer additional practice and further observe STPA learnability and use by NRC participants.

Two real systems from the nuclear industry were described, and participants were asked to apply STPA to each of these systems to discover potential design flaws, anticipate hazardous interactions and loss scenarios, and form recommendations. Participants received no information about the real design problems or operating experiences until the exercises were finished and the results were submitted. To conduct the exercises, NRC participants were assigned randomly to groups varying in size from two to eight participants. All groups had the ability to question an expert STPA facilitator about the process if needed. When reviewed, the results showed that the NRC groups were able to use STPA within a limited scope to identify key flaws and hazardous behaviors that had not been adequately considered and controlled by the original design teams and reviews (which did not use STPA).

The workshops ended with a detailed discussion of open questions and insights by participants. See the summary of results in Section 7, "Overall Observations on Learnability." Appendices A and B provide results from participant evaluations and feedback.

5.3 Forum on Relationship between STPA and Probabilistic Risk Assessment

A forum was held for NRC participants to engage in open discussion and ask questions about the similarities and differences between STPA and PRA and their relationship. Participating NRC staff made a number of observations:

- STPA helps to address the "unknown unknown" space, which is increasing with the use of more digital automation.
- PRA usually represents a "typical" or "average" state of a plant and its response to an initiating event (which may be a rare event). However, STPA can address additional unexpected or extreme abnormal conditions that may not be within the scope of a PRA, including plant states that PRA does not define as "failures."
- To date and for U.S. commercial nuclear power plants, PRA has had limited application to modeling control systems and has not needed to model software except very simplistically. STPA models well the potential for hazardous behavior in control systems and software.
- STPA would be very helpful for new systems, as well as for upgrades.
- STPA has different strengths than PRA. The two approaches are complementary.
- It is obvious that STPA is different from PRA and produces different results (some people characterize STPA as qualitative and PRA as quantitative).
- PRA has identified design issues in the past, so it would be incorrect to say that PRA cannot identify design issues. However, STPA seems to be better suited for identifying design issues.
- STPA analysis results may be useful to better inform PRA models about the effects of common causes [22].

5.4 Leadership Seminars

Two leadership seminars were held to brief NRC leadership on the results of this project and allow discussion of the conclusions and recommendations collected from NRC staff. The invited participants included the following:

- RES Division of Risk Analysis
    - Division Director
    - Senior Technical Advisor
    - Senior Reliability & Risk Engineer
    - Branch Chiefs from:
        - Performance and Reliability Branch
        - Probabilistic Risk Assessment Branch
        - Human Factors and Reliability Branch
- RES Division of System Analysis Accident Analysis Branch Chief
- RES Division of Engineering Deputy Director
- NRR Division of Engineering & External Hazards Director

6. Recent Developments

The founders [23] have developed an organization to enable certification in STPA proficiency, as well as accreditation for qualified educational programs.

SAE J3187 [24] was released in February 2022 to provide educational material and recommended practices for the application of STPA within a safety assessment process. The SAE J3187 task force is composed of 74 members from 42 organizations, including STPA practitioners from multiple industries. The draft standard began as an automotive-focused document but was revised to be applicable to all industries that are using and adopting STPA.

7. Overall Observations on Learnability

The differences in participant backgrounds did not appear to be a determining factor in their ability to learn and understand STPA. The strongest determining factor in participants' ability to learn and understand STPA was the level of their attendance and participation in the STPA seminar series.

Feedback was collected from NRC participants throughout the seminar series via open-ended and closed-ended survey questions (see Appendices A and B). The feedback was used to stimulate further debate and raise new questions in later sessions. The conclusions in this report are based on the feedback provided by NRC participants and later inputs by the NRC staff.

All groups were able to follow the STPA process to identify real design or requirements flaws, potential solutions, and potential questions that must be answered. At the beginning, the NRC participants received a general description of a real system. The participants were not told that each system contained real flaws that had been overlooked by standard techniques executed by professional industry teams, leading to one or more events. The participants applied STPA, and the results were compared to the real flaws and the real events that had been originally overlooked entirely without STPA or were considered only superficially without identifying the credible causes of the unsafe behaviors. The results showed that STPA provided the new insights needed to identify and fix the flaws and to prevent the events.

Although all teams were successful in identifying real flaws using STPA, it was observed that the most consistent results were produced by STPA teams of about four or more people. This observation is consistent with the guidance in the "STPA Handbook" [2] that STPA be applied by interdisciplinary teams rather than by individuals working alone. Groups of more than eight participants were not attempted due to potential collaborative overload, as evidenced in prior experience.

Participants noted that access to an expert STPA facilitator was important. This observation is consistent with the guidance in the "STPA Handbook" [2] that STPA teams include an expert facilitator to provide process guidance and expertise.

When asked about the "muddiest" part of the workshops and any lingering points of confusion, participants provided the following additional insights:

- Most participants indicated that the STPA process was clear with no significant points of confusion.
- Most of the points of confusion noted were about the specifics of the system that was analyzed with STPA. The NRC participants came from diverse disciplines and backgrounds, and therefore, some were more familiar with the technical aspects of the systems than others. Formal training classes could address this point of confusion by including additional background material for participants or by selecting only participants who are familiar with the type of system to be analyzed.
- Several participants acknowledged confusion due to missing previous sessions because of unavoidable scheduling conflicts. Follow-on training programs could ensure continuity.
- A point of confusion specific to the STPA process was identified: "keeping the STPA analysis at a high functional level." STPA beginners who are detail-oriented technical experts and may have less experience with top-down processes like STPA or are less skilled in abstraction sometimes encounter this point of confusion. Hands-on training programs could address this point by including additional exercises and experience with abstraction in STPA. An effective way to overcome this barrier is to begin with exercises that are outside the participant's expertise. The level of detail presented in the exercise can be controlled to help participants become more comfortable with high levels of abstraction. Additional exercises can gradually transition to applications that are closer to the participants' area of expertise as the participants become skilled in operating at high levels of abstraction. This point of confusion was not noted in later workshop sessions after the participants had more opportunities to practice STPA.

Appendices A and B summarize the results of the participant surveys.

During the open discussion in the leadership seminars, NRC participants acknowledged that STPA appears to be capable of addressing the infamous software common-cause failure problem. One participant observed that the STPA control structure modeling could capture challenging dynamics that have eluded reviewers and inspectors in the past, including specific events involving unanalyzed interactions by maintenance technicians, ad hoc decisionmaking, and gaps in procedures. One participant observed that STPA results could be used to improve testing by generating critical test cases (more generally, V&V cases). This observation is supported by existing work that has demonstrated test case generation from STPA [25][26][27][28]. NRC leadership acknowledged the need to build competence in STPA. Section 4, "Path Forward," describes competence-building needs.

8. Conclusions

The principal conclusions are as follows:

- The NRC participants recognized that STPA is a good complement to existing regulatory activities because STPA systematically analyzes areas that are not well represented in the current NRC regulatory review and oversight processes (e.g., hazards associated with the maintenance and operation of safety systems, complex software interactions, and identification of hazards associated with emergent properties). The current version of the NRC's SRP Chapter 7 [1] does not provide guidance for reviewing whether such hazardous scenarios are identified and controlled.
- The NRC staff was able to learn the basic concepts underlying STPA.
- The NRC staff was able to use STPA to discover real flaws in I&C design, requirements, and architecture that were overlooked by teams using traditional methods.
- The NRC staff sees the potential benefit of using STPA in regulatory review and oversight.
- For best results, an analysis team should consist of participants with diverse backgrounds, knowledge, experience, and thinking processes.
- NRC staff members provided feedback indicating that they believe that STPA is a suitable complement to existing regulatory activities and would be beneficial in regulatory reviews and oversight. Examples follow:
    - The NRC could streamline SRP Chapter 7 [1] because STPA connects the analysis closely to the regulations in 10 CFR Part 50, especially Appendix A.
    - The NRC could use STPA to simplify and streamline the regulatory guidance infrastructure related to DI&C.

9. Next Steps

The NRC staff observed that additional learning is needed to realize the benefits of STPA use. A larger scale effort, representative of real-life DI&C issues, is needed to further develop NRC staff competence to support STPA use in the NRC's licensing and oversight activities—for example, in an independent confirmatory HA or in a review of a licensee's or applicant's HA of a safety-related DI&C system. The NRC staff has recommended the following next steps:

(1) Select NRC projects that would benefit from STPA.

(2) Identify NRC participants that should be engaged.

(3) Build NRC staff competence to the level needed for reviewing a licensee's or applicant's HA of a safety-related DI&C system or performing an independent confirmatory HA on a traditional submittal, especially for the cases of concern.

10. References

[1] U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Instrumentation and Controls," https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/ch7/index.html.

[2] Leveson, N., and J. Thomas, "STPA Handbook," MIT Partnership for Systems Approaches to Safety and Security, 2018.

[3] Butchart, P., "Use of STPA in the Development of a Reactor Protection System at NuScale Power," NuScale, 2020 STAMP Workshop, virtual workshop July 20 to August 7, 2020, hosted by the MIT Partnership for Systems Approaches to Safety and Security.

[4] Thomas, J., "When STPA Results Surprise You: An industry case study employing STPA, Fault Trees, FMEA, and HAZOP," Massachusetts Institute of Technology (MIT), Engineering Systems Laboratory, 2020 STAMP Workshop.

[5] Thomas, J., and M. Gibson, "Industry Trials To Evaluate STPA's Effectiveness and Practicality for Digital Control Systems," EPRI, 2020 STAMP Workshop.

[6] de Lemos, F., and M. Mitake, "Using STPA on the Assessment of Nuclear Security Culture," Institute for Nuclear and Energy Research, Brazil, 2018 STAMP Workshop, March 26–29, 2018, Cambridge, MA, hosted by the MIT Partnership for Systems Approaches to Safety and Security.

[7] Lee, D., J. Lee, S. Cheon, and J. Yoo, "Application of STPA to Engineered Safety Features of a Nuclear Power Plant," Konkuk University, South Korea, 2013.

[8] Gibson, M., "Integration of STPA into EPRI Risk-Informed Digital Engineering Framework," EPRI, 2020 STAMP Workshop.

[9] Thomas, J., F. de Lemos, and N. Leveson, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants," NRC Technical Report, 2012.

[10] Uesako, D., "STAMP applied to Fukushima Daiichi nuclear disaster and the safety of nuclear power plants in Japan," graduate thesis, MIT School of Engineering, 2016.

[11] Electric Power Research Institute, "Hazard Analysis Demonstration—Generator Exciter Replacement: Lessons Learned," EPRI 3002006956, 2015.

[12] Thomas, J., and N. Leveson, "A New Approach to Risk Management and Safety Assurance in Digital Instrumentation and Control Systems," *Transactions of the American Nuclear Society*, Vol. 109, No. 1, page 1948, November 2013.

[13] Electric Power Research Institute, "Hazard Analysis Methods for Digital Instrumentation and Control Systems," EPRI 3002000509, 2013.

[14] Nuclear Energy Agency, No. 7466, "Multi-Stage Validation of Nuclear Power Plant Control Room Designs and Modifications," 2019, https://www.oecd-nea.org/upload/docs/application/pdf/2019-12/7466-multi-stage-validation.pdf.

[15] MIT Partnership for Systems Approaches to Safety and Security (PSASS), "STAMP Workshop Tutorials," accessed September 2021 at http://psas.scripts.mit.edu/home/mit-stamp-workshop-tutorials/.

[16] William, Y., and N. Leveson, "Systems thinking for safety and security," *Proceedings of the 29th Annual Computer Security Applications Conference*, New Orleans, LA, December 9–13, 2013.

[17] STAMP Safety and Security Consulting, https://stamp-consulting.com/.

[18] U.S. Nuclear Regulatory Commission, "Integrated Risk-Informed Decision-Making for Licensing Reviews," LIC-206, Revision 1, June 2019.

[19] Electric Power Research Institute, "HAZCADS: Hazards and Consequences Analysis for Digital Systems—Revision 1," EPRI 3002016698, July 2021.

[20] EPRI, "DRAM: Digital Reliability Analysis Methodology," EPRI 3002018387, July 2021.

[21] *U.S. Code of Federal Regulations*, "Domestic Licensing of Production and Utilization Facilities," Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," Part 50, Chapter I, Title 10, "Energy," https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html.

[22] U.S. Nuclear Regulatory Commission, NUREG/CR-5485, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment," November 1998, https://nrcoe.inl.gov/publicdocs/CCF/NUREGCR-5485_Guidelines%20on%20Modeling%20Common-Cause%20Failures%20in%20PRA.pdf.

[23] The International Center for STAMP Certification and Accreditation, http://stamp-certification.com/.

[24] Society of Automotive Engineers. "Applying System Theoretic Process Analysis (STPA) to Automotive Applications," SAE J3187, SAE International Functional Safety Committee, February 2022.

[25] Montes, D., "Using STPA to Inform Developmental Product Testing," MIT Dissertation, Cambridge, MA, 2016.

[26] Yang, C., "Software safety testing based on STPA," *Procedia Engineering*, Volume 80, 2014.

[27] Abdulkhaleqa, A., S. Wagnera, and N. Leveson, "A comprehensive safety engineering approach for software-intensive systems based on STPA," *Procedia Engineering*, Volume 128, pp. 2–11, 2015.

[28] Khastgir, S., S. Brewerton, J. Thomas, and P. Jennings, “Systems Approach to Creating Test Scenarios for Automated Driving Systems,” *Reliability Engineering & System Safety*, Volume 215, 2021.

Appendix A:
NRC Participant Responses to Closed-Ended Survey Questions

This appendix provides the quantitative results and summarizes the conclusions from the U.S. Nuclear Regulatory Commission (NRC) participant surveys. During this effort, 54 participants responded to the surveys. In addition to the data in this appendix, qualitative survey results (Appendix B) and independent internal NRC interviews and feedback provided information.

As shown in Figure A-1, the vast majority of NRC participants reported that System-Theoretic Process Analysis (STPA) was understandable and learnable. This finding is reinforced by the results of STPA exercises performed by NRC participants.

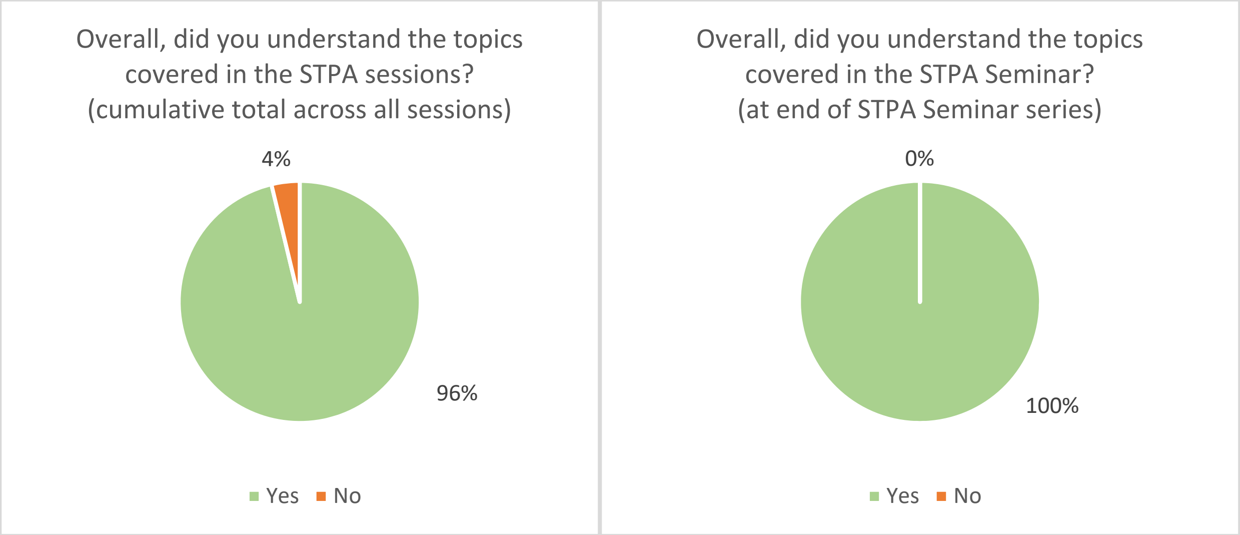

Figure A-1: NRC participant responses showing the differences in understanding during and at the end of the STPA seminar series

Most participants reported that their NRC group would benefit from using or participating in STPA activities, as shown in Figure A-2. Participants were also asked to name specific NRC groups that would benefit; Appendix B summarizes their responses.

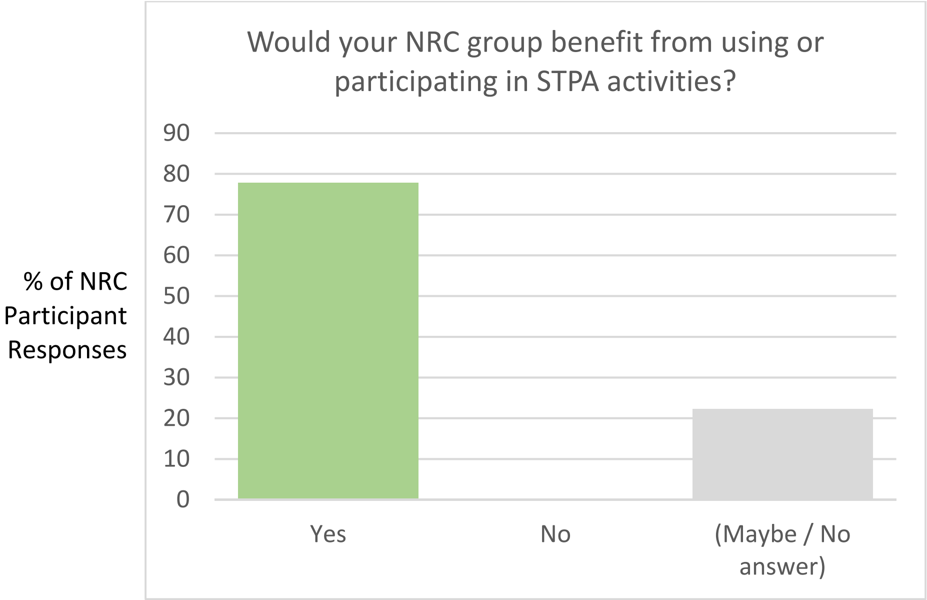

Figure A-2: STPA benefit for specific NRC groups

As shown in Figure A-3, the NRC participants indicated that the agency would benefit from both NRC use and industry use of STPA. These questions evaluate different potential uses of STPA that were suggested by the NRC participants: potential NRC use of STPA, industry use of STPA, and NRC review of industry-performed STPA results. The NRC participants indicated that all potential uses were beneficial.

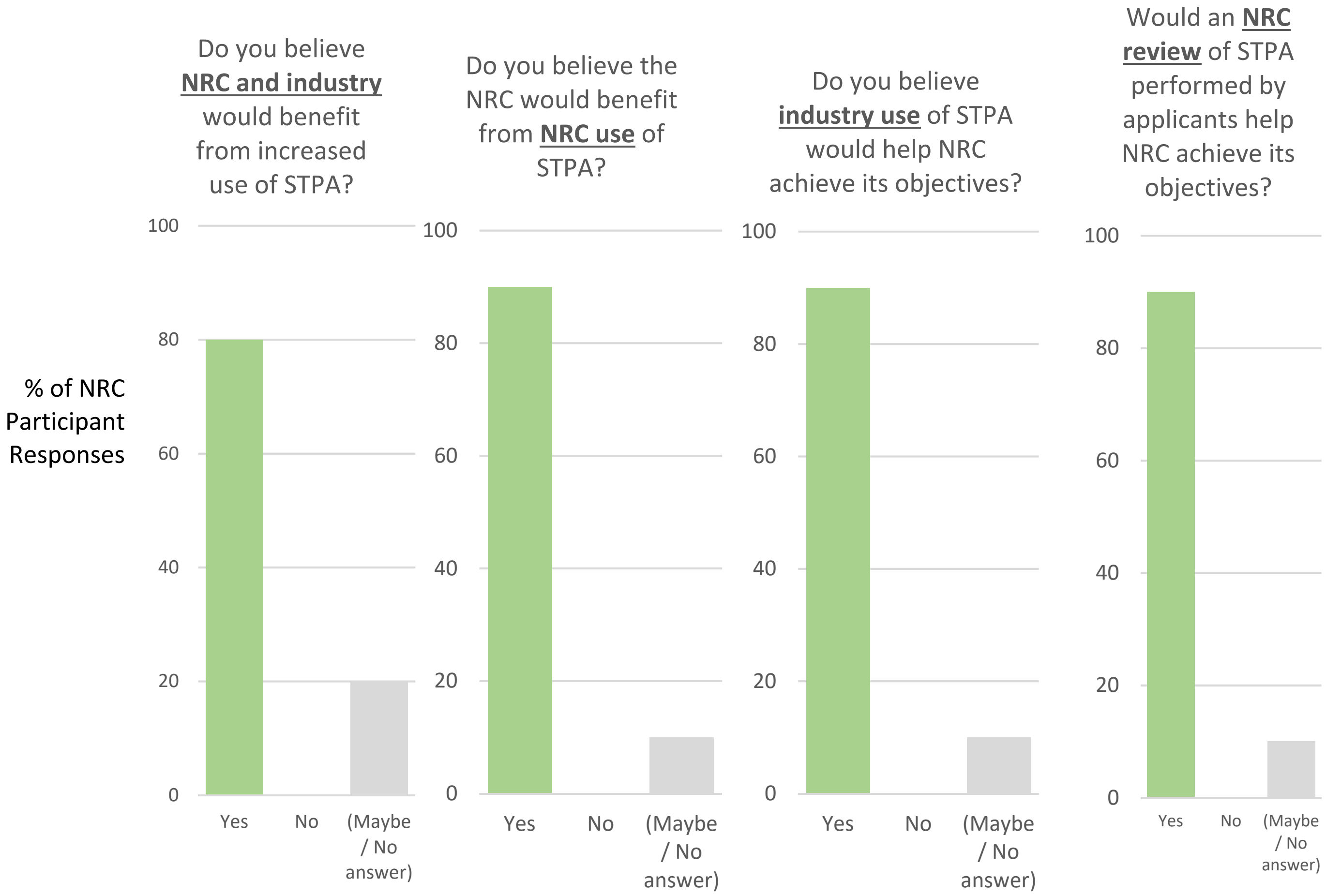

Figure A-3: NRC versus industry benefit and NRC versus industry use of STPA

The NRC participants indicated that STPA will be effective in helping achieve NRC objectives, as shown in Figure A-4.

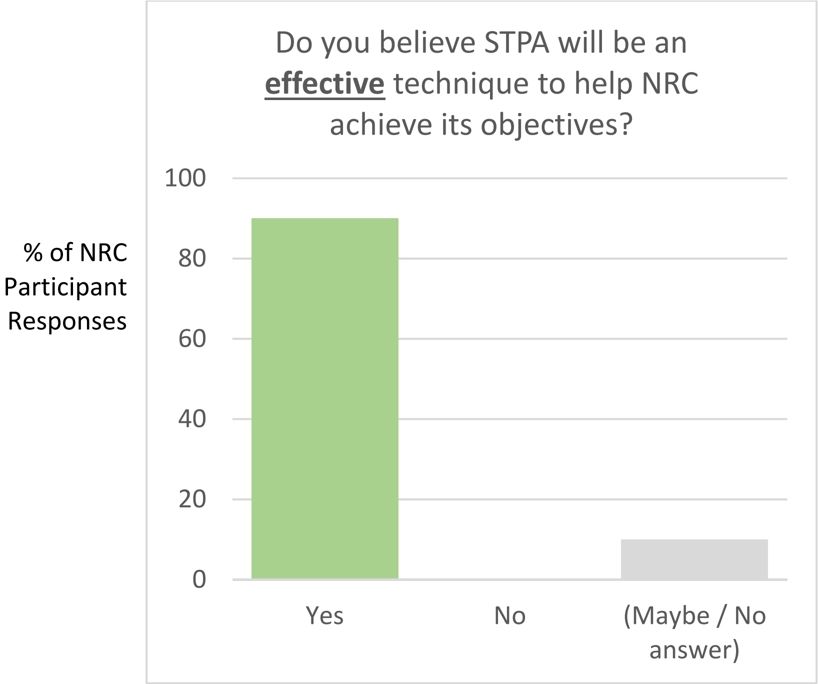

Figure A-4: Evaluation of STPA effectiveness in achieving NRC objectives

The NRC participants reported significant interest in becoming an STPA user or reviewer with additional help and support, as shown in Figure A-5.

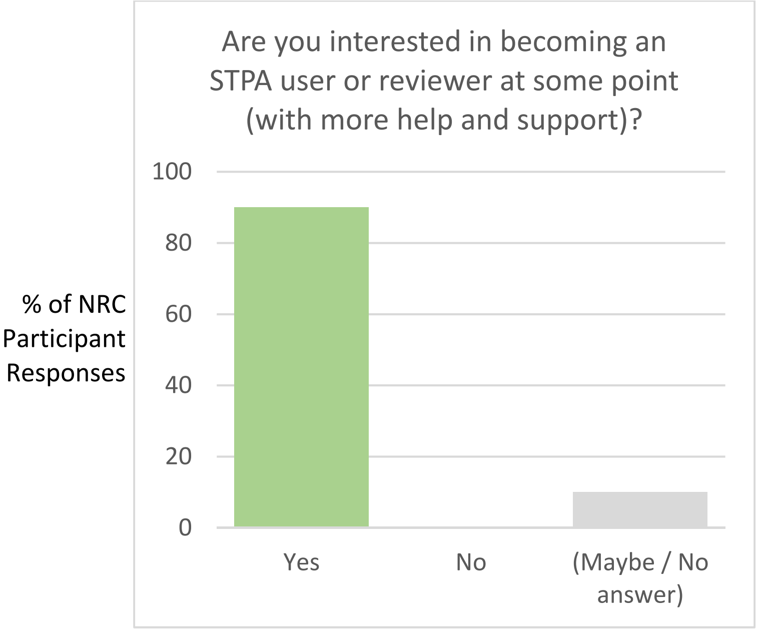

Figure A-5: NRC participant interest in becoming STPA user or reviewer

Most NRC participants reported that they could perform STPA successfully with additional guidance (e.g., training and practice) and with access to a qualified STPA facilitator as described in the "STPA Handbook."[1] A few NRC participants did not. It is unknown how many participants would have answered differently if they had a different role at the NRC or if they had access to a team of qualified STPA practitioners.

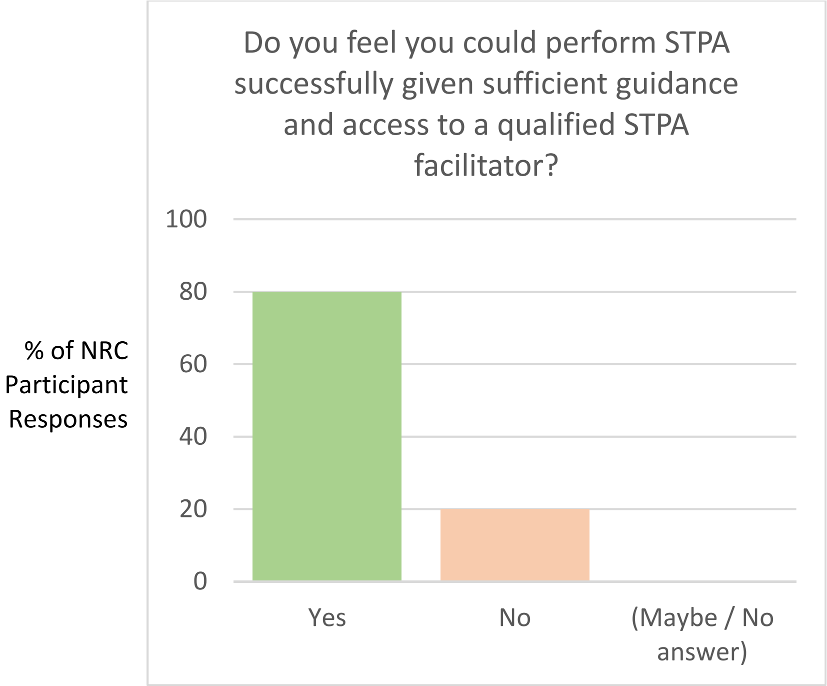

Figure A-6: Participant ability to perform STPA with additional guidance and access to STPA facilitator

[1] Leveson, N., and J. Thomas, "STPA Handbook," MIT Partnership for Systems Approaches to Safety and Security, 2018.

The NRC participants unanimously reported that STPA would produce new insights into nuclear systems beyond those found by current processes, as shown in Figure A-7.

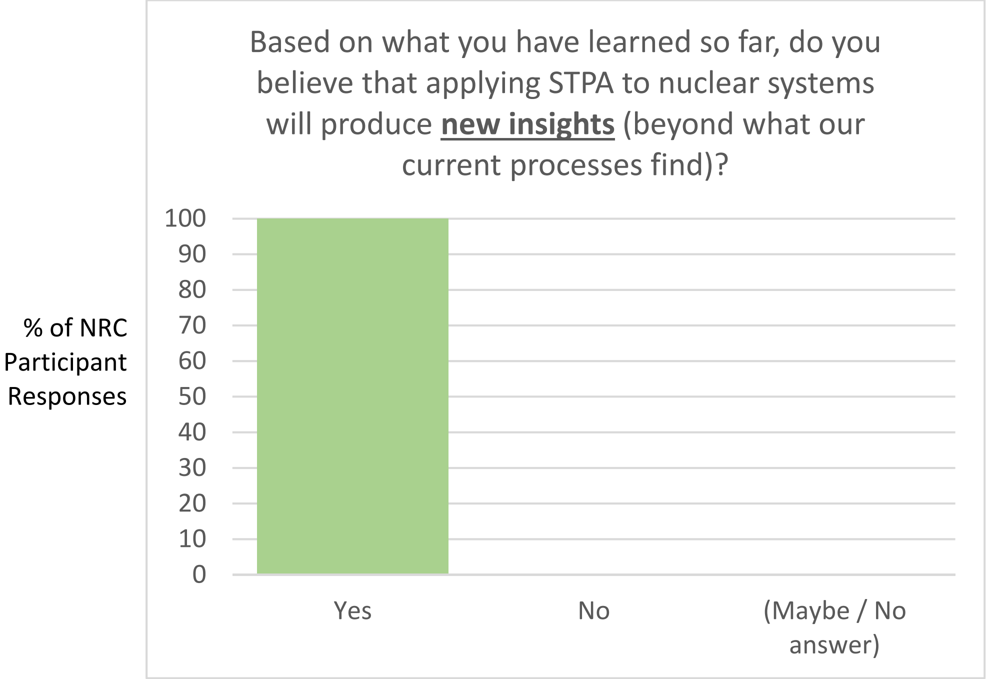

Figure A-7: Evaluation of STPA ability to produce new insights

The NRC participants unanimously reported that STPA would identify practical ways to increase safety, as shown in Figure A-8.

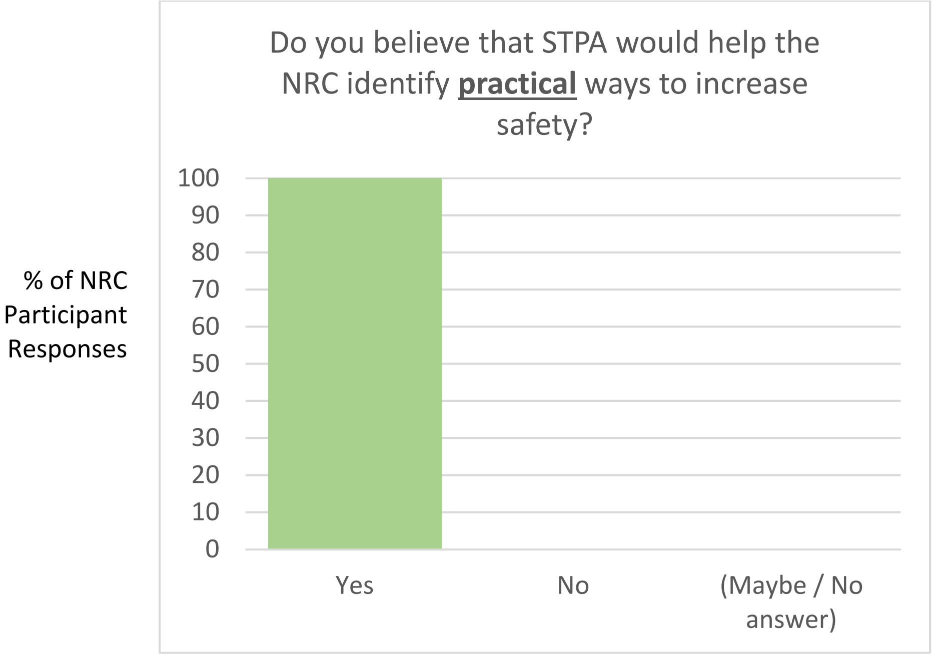

Figure A-8: Evaluation of STPA ability to produce practical solutions

Although the STPA seminar series and workshop series were not intended as formal training classes, most NRC participants reported that they already plan to use what they learned in their future work at the agency.

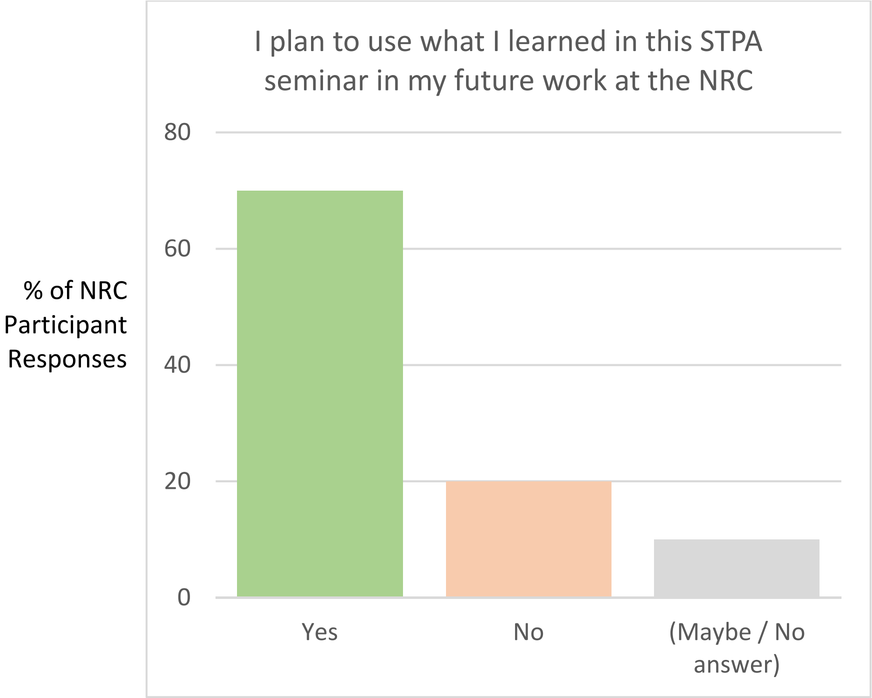

Figure A-9: NRC participant plans to use STPA

Following an extended discussion of potential regulatory and bureaucratic barriers to adoption, the NRC participants were asked if they believe the agency would be willing to incorporate STPA into its processes or materials. As shown in Figure A-10, most participants believed that the NRC would ultimately be willing to incorporate STPA.

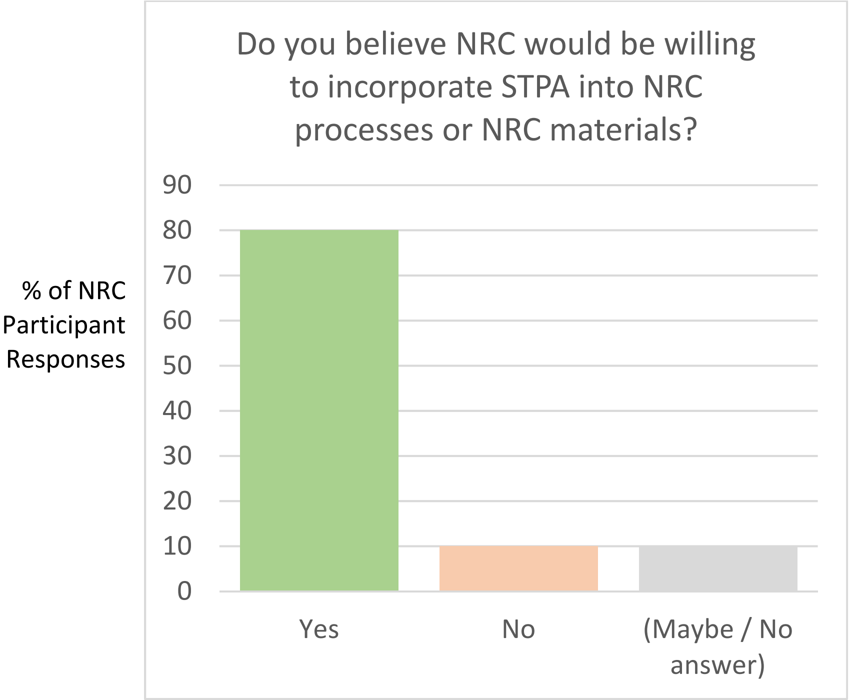

Figure A-10: NRC willingness to incorporate STPA into formal processes and materials

The NRC participants were asked exactly how STPA might help the NRC achieve its objectives. The participants identified four key areas:

(1) STPA provides a way to identify unbounded or unanalyzed events relevant to NRC objectives.

(2) STPA can inform existing likelihood categorizations, such as likelihoods that may be incorrect or based on incorrect assumptions.

(3) STPA can provide a more efficient analysis in terms of the effort needed to review.

(4) STPA can provide a more effective means of development assurance than the current method (i.e., validation of design intent).

The NRC participants were then surveyed to determine the level of support for these NRC-identified areas of potential STPA benefit. As shown in Figure A-11, the majority of NRC participants agreed with all of the NRC-identified benefits.

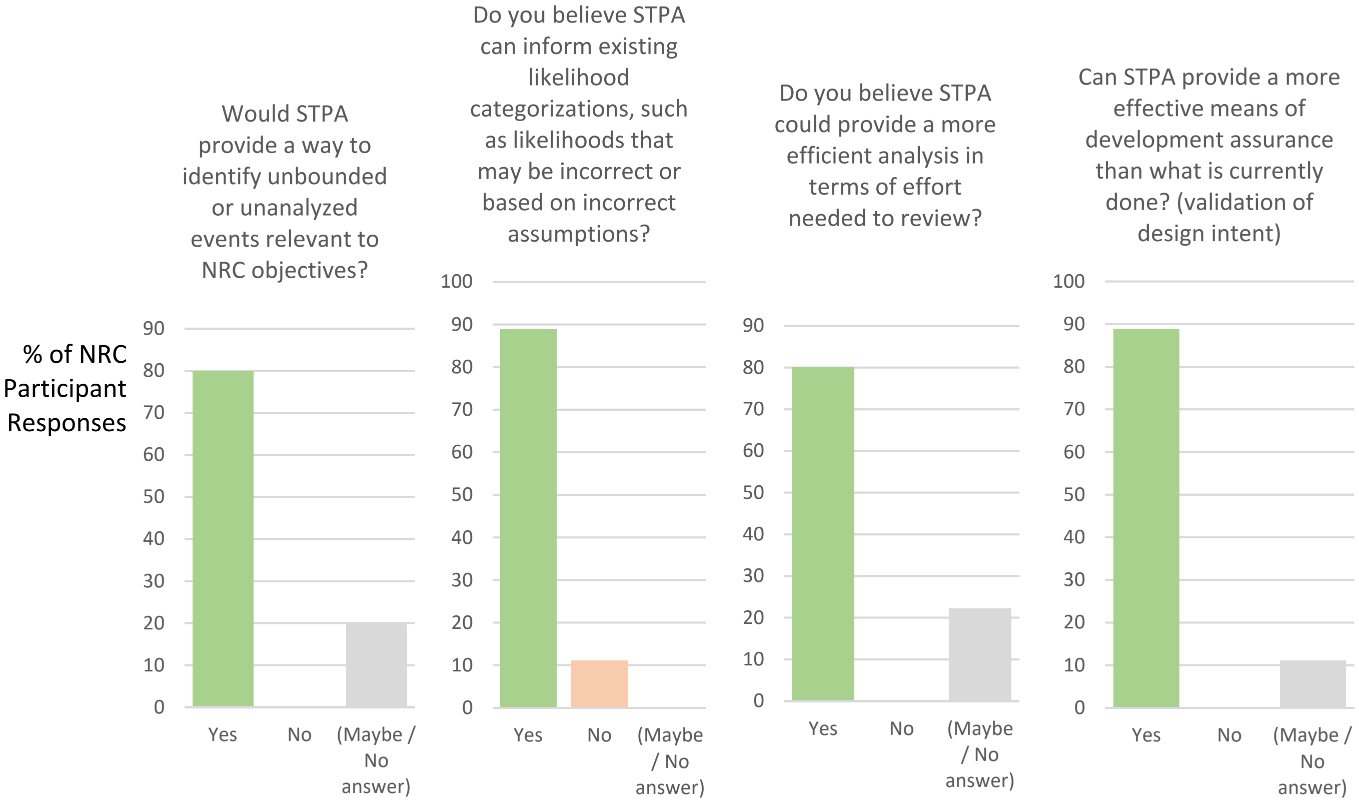

Figure A-11: NRC participant support for specific STPA benefits

Appendix B:
NRC Participant Responses to Open-Ended Survey Questions

This appendix shows the open-ended results from the questionnaires given to U.S. Nuclear Regulatory Commission (NRC) participants. The NRC participants submitted 54 questionnaires during this effort with fields for open-ended responses. In addition to the data in this appendix, quantitative survey results (Appendix A) and independent internal NRC interviews and feedback provided information.

What groups at the NRC would benefit from System-Theoretic Process Analysis (STPA)?

NRC participants' verbatim answers:

- cybersecurity
- software
- any offices that consider risk and design
- licensing folks
- Office of Nuclear Security and Incident Response (NSIR) Cyber Security Branch
- Instrumentation and Control (I&C)
- folks doing research on design
- human factors engineering
- Division of Risk Analysis (DRA) in the Office of Nuclear Regulatory Research (RES)
- inspectors
- licensing reviewers
- management
- licensing
- any risk or management group—especially those who inform regulation
- NRC regional inspectors, cyber inspectors
- any organization that has responsibility for a system or facility that plans to incorporate a significant amount of automation or remote control
- all areas that review
- NSIR
- Office of Nuclear Reactor Regulation (NRR)
- RES
- Office of Nuclear Material Safety and Safeguards (NMSS)
- Just about any process can use this concept to identify situations where the planned thing occurs, but it is not the right thing. The fact that STPA catches incorrect/invalid/incomplete requirements is very valuable.

What activities might STPA help to support at the NRC?

NRC participants' verbatim answers:

- licensing reviews
- generic issue reviews
- inspections
- design review

- data analysis of system safety and integrity
- informing licensing requirements for upgrades with automation
- informing licensing requirements for new reactor designs that cannot borrow from existing designs

<u>General verbatim comments and observations reported by NRC participants:</u>

- “Probabilistic Risk Assessment (PRA) and STPA should be treated as complementary. STPA provides the ‘what can go wrong’ from the perspective of systemic causes (hazardous interactions ... interdependencies). Thus, it could serve as improving the ‘input’ to PRA models.”

- “The control room and the automation in it (HMI) and Digital Instrumentation and Control (DI&C) is in the jurisdiction of different groups. Thus, there is the potential of things falling through the cracks/gaps. STPA would bridge over these gaps.”

- “STPA helps manage complexity through abstraction. For example, finding the fault/defect in the logic diagrams or maintenance procedures or configuration management procedures would be much more time consuming. STPA helps focus the effort.”

- “I think that STPA could be an important & useful complement to PRA. Also, I think that STPA is the only tool that could identify automation/operation control problems.”

- “Because STPA embeds traceability to losses of concern, it seems to provide appropriate regulatory review focus. Unstructured descriptions of design details, especially when presented as components or subsystems, don’t necessarily reveal the context necessary for safety conclusions.”

- “I believe there to be regulatory utility from accessing a licensee’s STPA. With Electric Power Research Institute’s (EPRI’s) Digital Engineering Guide (DEG), Hazards and Consequences Analysis for Digital Systems (HAZCADS), and Digital Reliability Analysis Methodology (DRAM) being adopted, and NuScale’s experience, I expect STPA will be performed in our domain. The question then is how would we credit those, what is required to audit their STPA, and what degree of qualification do we need as regulators to competently review an STPA if it is being relied upon to come to a safety determination.”

<u>What will be needed after this STPA seminar in order to be successful with STPA at the NRC?</u>

- “Need more presentations to further socialize the concept. Perhaps some shorter, higher level condensed ones for upper management as they could be one of the biggest roadblocks (if they are at all).”

- “More exposure of STPA to NRC staff and management. Need to build support to get it implemented as a method that can be used throughout the agency.”

- “More training/workshops and facilitator support (esp. for starting and initial efforts).”

- “A practical application of STPA on a business process to show efficacy to management.”
- “One needs practice to instill the concepts.”
- “Need a specific activity or project for application as a test case; perhaps a joint project between PRA and I&C groups on an upgrade involving new automation features.”

Appendix C:
Additional Project Details

Event Dates and Materials

(1) System-Theoretic Process Analysis (STPA) Seminar: August 16–19, 2021
(2) STPA Workshop: August 23–26, 2021
(3) STPA-Probabilistic Risk Assessment (PRA) Forum: September 1, 2021
(4) Leadership Seminars: September 17 and September 21, 2021

The materials presented at the above events are copyrighted and are restricted to the U.S. Nuclear Regulatory (NRC) staff participants in this research effort. Therefore, the materials are not included in this report or its appendices.

The STPA seminar included foundational information on System-Theoretic Accident Model and Process (STAMP) and STPA (e.g., theoretical basis for STAMP and STPA, steps for performing an STPA, and other basic information) and hypothetical examples of STPA application (e.g., analyzing a cooling system at a nuclear plant, analyzing a rod controller at a nuclear plant).

The STPA workshop consisted of hands-on experience working on examples similar to those presented at the STPA seminar but with greater depth and difficulty.

The STPA-PRA forum consisted of a short presentation followed by a discussion with NRC PRA experts on the similarities and differences between the two methodologies.

The leadership seminars consisted of a presentation based on selected materials from the previous events and a discussion of preliminary results with selected NRC managers and staff.

Public domain content similar to the materials presented at the STPA seminar and workshop can be found at The MIT Partnership for Systems Approaches to Safety and Security (PSASS) Web site. See resources listed below.

Resources

Nancy Leveson and John Thomas, “STPA Handbook,” MIT Partnership for Systems Approaches to Safety and Security,” 2018.

The MIT Partnership for Systems Approaches to Safety and Security (PSASS) Web site: http://psas.scripts.mit.edu/home/mit-stamp-workshop-tutorials/.