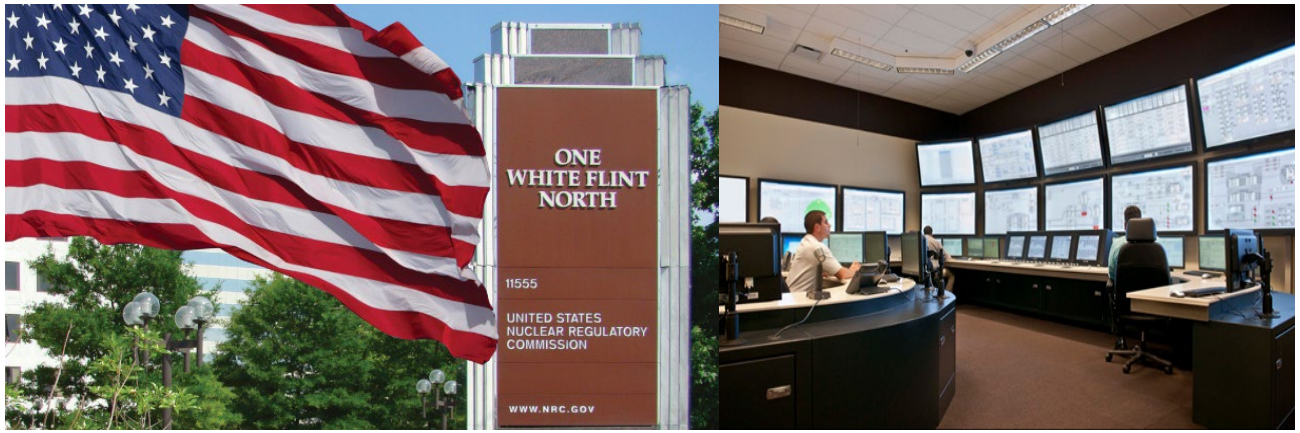
STPA Adoption Hurdles – an Experience-Based Perspective

June 06, 2024

Norbert Carte
Instrumentation and Controls Branch
Office of Nuclear Regulatory Regulation
US Nuclear Regulatory Commission (NRC)
Email: Norbert.Carte@nrc.gov

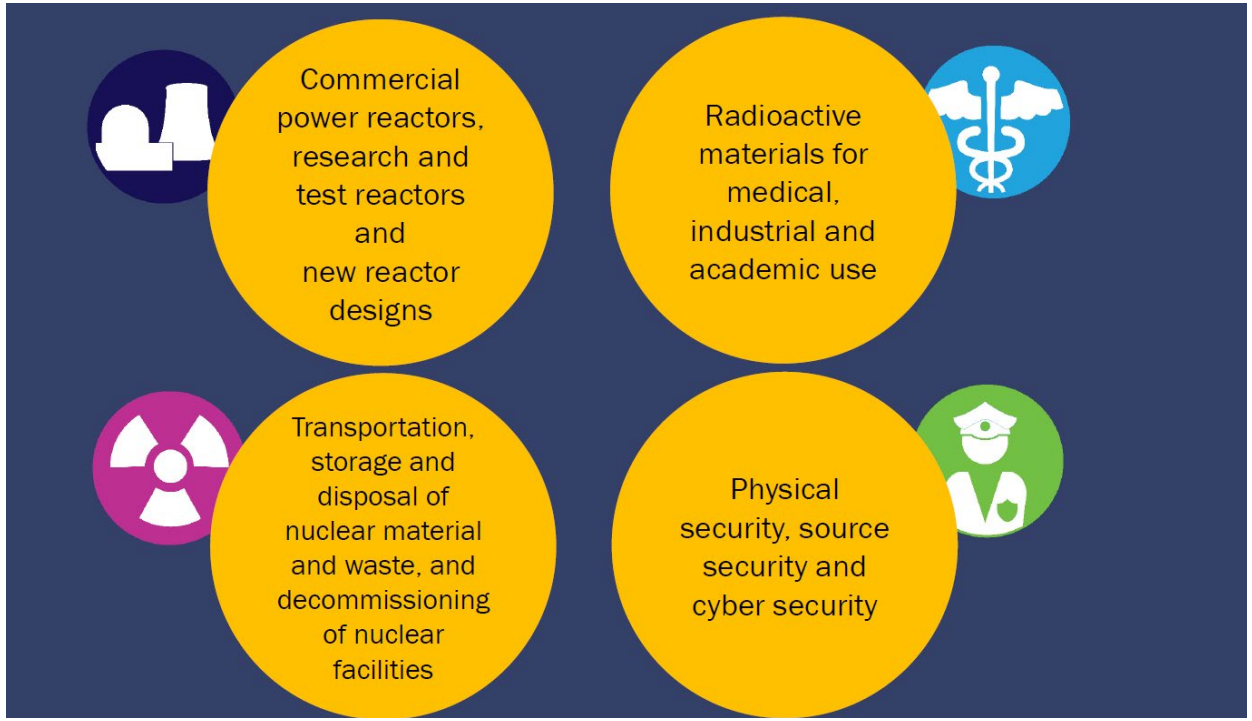
Mauricio Gutierrez & Christopher Cook
Instrumentation, Controls, and Electrical Engineering Branch
Office of Nuclear Regulatory Research
Nuclear Regulatory Commission (NRC)
Email: Mauricio.Gutierrez@nrc.gov
Email: Christopher.Cook@nrc.gov

Sushil Birla
Instrumentation, Controls, and Electrical Engineering Branch
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission (NRC)
Email: Sushil.Birla@nrc.gov



Overview of The NRC

- The Nuclear Regulatory Commission is an independent agency that licenses and regulates civilian use of radioactive materials. NRC's mission is to provide reasonable assurance of adequate protection of people and the environment.
- Approximately 3000 people across four regional offices, headquarters, and on-site inspectors at nuclear power plants and facilities.



Presentation Outline

- The remainder of this presentation will:
  - Provide an overview of the NRC staff's recent efforts to grow the capability to review an applicant's STPA.
  - Summarize lessons learned.

Introduction

- Current practice for the safety evaluation of digital systems is challenged by the increased interdependencies and interactions across systems and components.
- The Nuclear Industry has conveyed that applicants and licensees will increasingly employ System-Theoretic Process Analysis (STPA) to support safety related digital applications. Some advantages identified by industry include:
  - The ability to analyze integrated systems that could have interdependencies among hardware, software, and human systems and operations.
  - The analysis is not limited to analyzing traditional hardware “failures.” STPA can provide insights originating from engineering deficiencies.
- NRC wants to build the capability to review STPA-based or STPA-informed submittals and is interested in learning how STPA can better answer: what can go wrong? and what are the consequences?

Overview of NRC Staff Efforts

- Held seminars and workshops to learn the basics of STPA and CAST.
  - 1 week seminar (lecture style), 1 week workshop (non-nuclear group exercises)
  - See the Agencywide Documents Access and Management System (ADAMS) Accession Numbers: ML22277A013, and ML22272A315
- Following success of seminars and workshops, NRC staff recommended following up with a case study to:
  - Build up NRC staff capability to understand how STPA can be applied to a system that could be reviewed by the NRC (e.g., a reactor protection system design).
  - Grow NRC's capability to review an STPA-based or STPA-informed submittal.
- Case study was performed in 2023 with materials similar to submittals that could be reviewed by the NRC.

NRC's Case Study

- Two teams participated.
  - Team 1 - Interdisciplinary team performed the analysis using the synthetic case study materials. Included aid of a facilitator.
  - Team 2 - Learned the basics of STPA at their own pace and observed the case study group's efforts.
  - Teams included licensing reviewers, researchers, and one inspector.
  - Team assignments were dependent on participant availability and previous knowledge of STPA.
- Case Study Execution
  - Case study materials were primarily based on a subset of materials from a withdrawn nuclear reactor design.
  - Case study focused the analysis on a digital reactor protection system.
  - Project planned around weekly meetings over a 5-month period.

Results – Some Lessons Learned

- Short duration intensive interval worked better than a long interval approach for building STPA review capabilities.
  - Team meetings highlighted the importance of interdisciplinary collaboration.
  - Exposed subject matter experts to insights they might not capture without collaboration.
- Design documentation limitations for applying or reviewing an STPA
  - Design documentation used to create the case-study was encumbered with voluminous materials but was missing key information appropriate for applying STPA.
  - Information in the case study documentation (specifically concept of operations documentation) was not sufficient to include, accurately label, and understand the reasoning for human actions in the control model(s) generated.

Conclusions

- Staff built up an understanding of how nuclear applicants and licensees could use STPA to perform a safety analysis in a nuclear application.
- Staff learned how to more effectively build the capability to review STPA-based or STPA-informed submittals.
  - Group work was more effective than individual work.
  - Concentrated capability-building intervals were more effective than efforts spread out over longer intervals.
- Staff learned that content needed to support a scaled up STPA review would be challenging.
  - Reviewing submittals containing STPA-based or STPA-informed content would be a new paradigm.
  - Information needed to support a scaled up STPA review would draw from numerous experts and sections of a licensee submittal.
  - Inclusion of material not currently provided in early stages of licensing reviews (e.g., concept of operations content) would be needed.
  - The staff has not sufficiently determined what information would be needed on the docket for an STPA-based/STPA-informed review nor what type of information could be audited or inspected.