STPA Standards, Certification, and Accreditation

John Thomas
William “Dollar” Young

Email: JThomas@mit.edu  wyoung@mit.edu
STPA in Industry Standards (2023)

• ISO/PAS 21448: SOTIF: Safety of the Intended Functionality
  • STPA used assess safety of automotive systems
• ASTM WK60748
  • “Standard Guide for Application of STPA to Aircraft”
• SAE AIR6913
  • “Using STPA during Development and Safety Assessment of Civil Aircraft”
• RTCA DO-356A
  • “Airworthiness Security Methods and Considerations”
  • STPA-sec used for cybersecurity of digital systems
• IEC 63187
  • “Functional safety - Framework for safety critical E/E/PE systems for defence industry applications”
• SAE J3187
  • “Recommended Practice for STPA in Automotive Safety Critical Systems”
• SAE J3187A
  • STPA Recommended Practice for Safety-Critical Evaluations in Any Industry”
• EPRI 3002016698 & 3002018387
  • STPA for digital I&C in nuclear power
• NIST SP800-160 Vol2
  • “Developing Cyber Resilient Systems: A Systems Security Engineering Approach”
  • “Attack scenarios can be represented as part of a model-based engineering effort [...] based on identification of loss scenarios from System-Theoretic Process Analysis (STPA).”
• IET 978-1-83953-318-1
  • “Code of Practice: Cyber Security and Safety”
  • Recommends use of STPA for Safety & Security
• NEI 20-07 Rev D
  • “Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems”
  • Outlines STPA process for digital technology at nuclear power stations
• UL 2800-1:2022: Standard for Medical Device Interoperability
  • Explicitly mentions STPA for performing system-level hazard analysis and control loop analysis
Why a certification?

• Standardization to accelerate useful adoption
  • Gain scale without sacrificing quality
  • Provide an organized support community for practitioners
• Need a way to recognize qualified & skilled STPA practitioners vs. a basic familiarity
• Help practitioners understand what is needed to perform STPA correctly
• Help management & leadership recognize the qualifications to perform STPA correctly
• Provide a way for you to verify your credentials when offering STPA support on projects
• Establishes an international board of experienced experts to help scale STAMP/STPA/CAST
  • Globally
  • Responsibly

Standardization, Structure, and Rigor Benefits the Entire Community!
Typical STPA Team Participants

**STPA Core Team**
- STPA Practitioner
- STPA Practitioner
- STPA Practitioner
- STPA Practitioner
- STPA Practitioner

**Practitioners**
- Perform majority of STPA work
- Interdisciplinary team
- Must have STPA training and basic understanding of STPA, but may not be experts

**Facilitator**
- The STPA expert
- Provide STPA method guidance (and other responsibilities)

**SMEs**
- Provide specialized domain knowledge as needed by team
- May have little or no STPA familiarity
- May not be actively involved in STPA, but must be accessible by team
STPA Practitioner Certification Criteria (Proposed)

- **Skill**
  - Basic STPA skill & ability on real project (see next slide)

- **Knowledge**
  - Knowledge of the strengths and limitations of STPA
  - Knowledge of differences between STPA and other HA methods used in their industry
  - Knowledge of how STPA relates to industry objectives (e.g., SOTIF, etc.)

Practitioners must demonstrate Skill and Knowledge
STPA Practitioner Certification Criteria (Proposed)

Must demonstrate skill on STPA project:

- **STPA Step 1**
  - Ability to identify stakeholder losses
  - Ability to identify system-level hazards
  - Ability to identify system-level safety constraints
  - Ability to establish traceability between losses, hazards, safety constraints
  - Ability to identify and correct common mistakes in losses, hazards, and safety constraints

- **STPA Step 2**
  - Ability to model a control structure
  - Ability to distinguish controllers, controlled processes, control actions, and feedback
  - Ability to use abstraction effectively in a control structure
  - Ability to define relevant controller responsibilities and process models
  - Ability to identify and correct common mistakes in control structure modeling

- **STPA Step 3**
  - Ability to identify Unsafe Control Actions (UCAs)
  - Ability to properly construct a UCA
  - Ability to identify effective UCA contexts
  - Ability to identify requirements and safety constraints for each UCA
  - Ability to establish traceability between UCAs and Hazards, requirements, and safety constraints
  - Ability to distinguish between UCAs and Hazards
  - Ability to identify and correct common mistakes in UCAs

- **STPA Step 4**
  - Ability to identify scenarios
  - Ability to properly construct the four scenario types defined in the STPA handbook
  - Ability to evaluate scenario coverage, including component failure and component interaction scenarios
  - Ability to establish scenario traceability
  - Ability to identify and evaluate effective solutions to address scenarios
  - Ability to identify and correct common mistakes in scenarios
Practitioner Rollout

• Standardized foundational curriculum
  • Familiarization Track – No evaluation for certificate (reduced cost)
  • Practitioner Track – Course plus evaluation
  • Emphasizes theory and proven best practices

• Testing
  • Board certifies criteria and samples of behavior

November 2023 is planned rollout for beta course
Summary

• Certification will support community-wide need to recognize qualified individuals
• Designing for community-wide impact
• Scale STAMP/STPA/CAST as fast as responsibly possible

Mission: To enable high-quality STAMP-related work products by recognizing qualified practitioners and defining a uniform standard for education and facilitation.