STPA in Industry Standards and Processes

- 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 (public draft)
  - "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

Others: 26262, 4761/4754