

The First Cross-Industry STPA Standard (SAE J3307)

Presented by

Mark A. Vernacchia, MSES, INCOSE ESEP, PE

Principal and Co-Founder – SSE Group, LLC

Former Technical Fellow – General Motors Company

Chair – SAE STPA Task Force

markv.ssegroup.011@gmail.com

The First Cross-Industry STPA Standard

- This presentation reviews the FIRST STPA Standard (SAE J3307) ever developed by STPA Practitioners and Facilitators for use in ANY industry
- It was created over the last 5 years by numerous experienced STPA practitioners and facilitators from:
 - More than forty-seven (47) different companies
 - Industries such as aerospace, commercial aircraft, automotive, medical, defense, software, and education
- Publication release TODAY from SAE

The First Cross-Industry STPA Standard

- This standard documents what is required to execute a System Theoretic Process Analysis (STPA) of safety-critical products or systems in all industries. The standard defines the terminology, the steps in using STPA, activities flow, and expected deliverables.
- This standard may be used when addressing compliance with contractual or regulatory requirements regarding risk assessments, safety assessments, development assurance, system security engineering, or other similar requirements
- In addition, this standard can be used to demonstrate that an effective STPA evaluation has been conducted when compliance is not of paramount concern

The First Cross-Industry STPA Standard

- This standard is applicable to a broad set of uses including, but not limited to:
 - Product development processes
 - Organizational and Supplier processes
 - Regulatory groups
 - Defense programs (e.g., government awards a contract to a company and the contract mandates STPA) or defense program office (e.g., government safety group applying STPA during a safety review)
 - Healthcare safety researchers (not engineers)
 - Site reliability engineering (e.g., Google Maps, where the “controlled process” is a virtual map)

The First Cross-Industry STPA Standard

- This standard defines a method or technique for using STPA to identify hazards and losses associated with system misbehaviors that lead to unacceptable losses and for determining the scenarios and causes that lead to such misbehaviors
- This standard also addresses the creation of constraints and requirements to prevent or manage causes and/or scenarios associated with identified misbehaviors

The First Cross-Industry STPA Standard

The standard includes content related to:

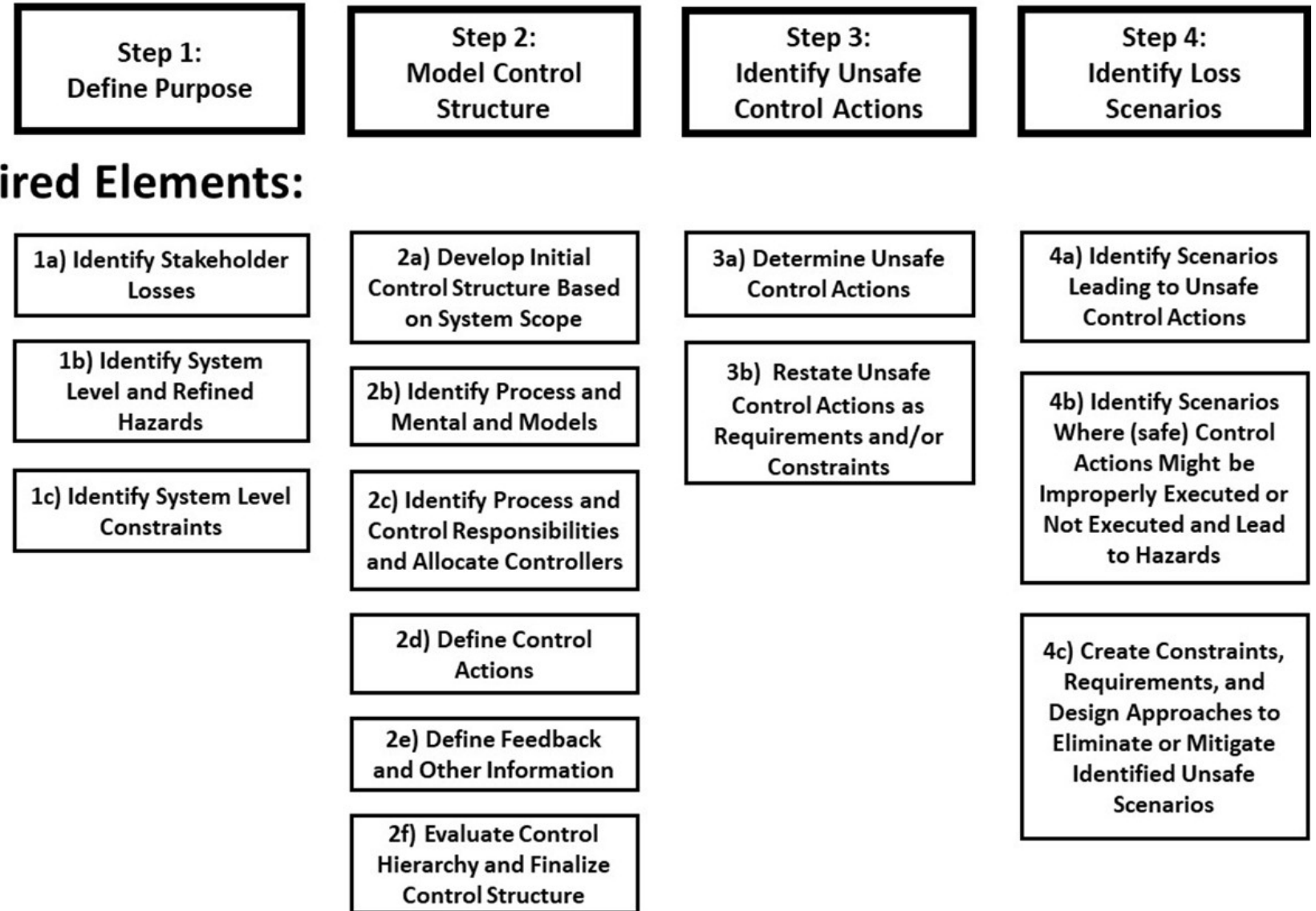
- STPA Management Support
- STPA Evaluation Participants
- STPA Facilitators and High-Quality STPA Results
- STPA Implementation Plan (SIP)
- STPA-Related Activities Before STPA Application
- STPA-Related Activities After STPA Application
- Relations Between Systems Engineering and STPA

The First Cross-Industry STPA Standard

Steps:

- Each STPA sub-step of the four major Steps is organized in three sections:
 - Objectives of this step
 - General Activities
 - Required Work Product Deliverables
- The deliverables of each sub-step shall be documented.

Required Elements:



The First Cross-Industry STPA Standard

Table 1 – Required Work Product Deliverable(s) Summary

Number	Sub-Step Name	Required Work Product Deliverable(s)
1a	Identify Stakeholder Losses	1a-1: The mission statement, the system scope and boundaries, and set of system losses 1a-2: Confirmation of mission statement, system scope and boundaries, and identified losses by the Stakeholders
1b	Identify System High-Level and Refined Hazards	1b-1: High-level hazards traceable to one or more identified losses 1b-2: High-level hazards grouped into major hazard categories as needed
1c	Identify System-Level Constraints	1c-1: System safety/security constraints that prevent hazards from occurring or will minimize losses if hazards do occur 1c-2: System-level constraint(s) traceable to one or more hazards
2a	Develop initial control structure based on system scope	2a-1: Initial control structure showing system elements, control loops, and accommodation of control hierarchy, all based on system scope and the selected level of abstraction
2b	Identify Process and Mental Models	2b-1: Process and mental models identified 2b-2: Summary of critical feedback based on control loop evaluation
2c	Identify process and control responsibilities and allocate controllers	2c-1: Description of the responsibilities and their associated elements, particularly controllers and controlled processes 2c-2: Traceability of the responsibilities to constraints and then to hazards

The First Cross-Industry STPA Standard

- Standard mentions that STPA practitioners and facilitators should be aware of improvements to STPA methodology by staying abreast of the latest developments by way of technical papers, presentations, workshops, etc.

Example:

New Step 4 Scenarios introduced by John Thomas 2024

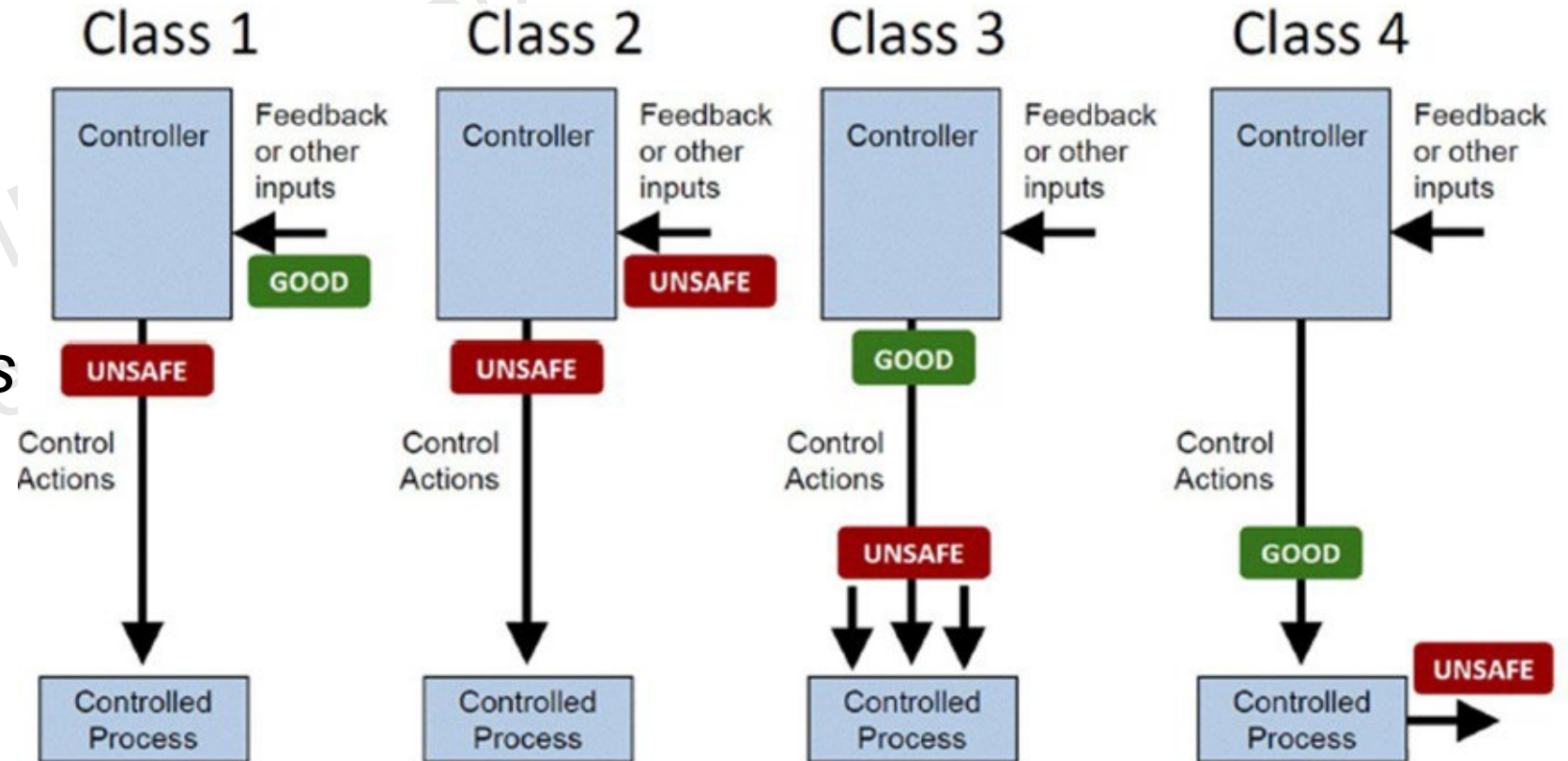


Figure C1 - Updated Step 4 Scenario classes
(Used with permission from Thomas, 2024. All other rights reserved.)

The First Cross-Industry STPA Standard

Various J3307 appendices included:

APPENDIX A - ACTIVITIES THAT APPLY ACROSS AND WITHIN STPA STEPS

APPENDIX B - STPA AND RISK ESTIMATION

APPENDIX C - IMPROVEMENTS TO STPA METHODOLOGY

APPENDIX D - EXAMPLE STPA IMPLEMENTATION PLAN (SIP)

APPENDIX E - STPA STEPS APPLIED BASED ON ABSTRACTION LEVEL

Complimenting Documents

- SAE J3307 STPA Standard - “WHAT” is required
- SAE J3187 STPA Recommended Practices – “HOW”

The First Cross-Industry STPA Standard - Summary

- This standard documents what is required to execute a System Theoretic Process Analysis (STPA) of safety-critical products or systems in all industries
- The standard defines the terminology, the steps in using STPA, activities flow, and expected deliverables
- This standard may be used when addressing compliance with contractual or regulatory requirements regarding risk assessments, safety assessments, development assurance, system security engineering, or other similar requirements
- In addition, this standard can be used to demonstrate that an effective STPA evaluation has been conducted when compliance is not of paramount concern

The First Cross-Industry STPA Standard

CURRENT

ISSUED

2025-03-25

System Theoretic Process Analysis (STPA) Standard for All Industries [J3307_202503](#)

This standard documents what is required to execute a System Theoretic Process Analysis (STPA) of safety-critical products or systems in all industries. This standard defines the terminology, the steps in using STPA, the activities flow, and the expected deliverables. This standard may be used when addressing compliance with contractual or regulatory requirements regarding risk assessments, safety assessments, development assurance, system security engineering, or other similar requirements as appropriate. In addition, this standard can be used to demonstrate that an effective STPA evaluation has been conducted when compliance is not of paramount concern.

This standard is applicable to a broad set of uses including, but not limited to, corporate product development processes, organizational processes, regulatory groups, supplier processes, defense programs (e.g., government awards a contract to a company and the contract mandates STPA), defense program office (e.g., government safety group applies STPA during a safety review on a project), healthcare safety researchers (not engineers), and site reliability engineering (e.g., Google Maps, where the “controlled process” is a virtual map - pure data rather than a physical process) to name a few.