

Learnings from Creation of SAE J3307 The First STPA Standard

Mark A Vernacchia, Principal and Co-Founder - SSE Group, LLC
INCOSE Expert Systems Engineering Professional (ESEP)
Chair - SAE STPA Task Force

Presentation Outline

Content of SAE J3307 STPA Standard For All Industries

Task Force Membership Skill Sets

Keeping Task Force Members Engaged in Effort

Navigating the SAE Hierarchy

Issues Experienced Along the Way and Some Solutions

Summary

Additional Information

- STPA Recommended Practices for All Industries – SAE J3187_202305
- STPA Recommended Practices Appendices J3187-1 thru J3187-5

First Cross-Industry STPA Standard – SAE J3307

- [SAE J3307_202503](#) 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

First Cross-Industry STPA Standard – SAE J3307

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.

SAE J3307_202503 STPA Standard Title Page



| | | |
|--|--------|---------|
| SAFETY CRITICAL SYSTEMS STANDARD | J3307™ | MAR2025 |
| | Issued | 2025-03 |
| System Theoretic Process Analysis (STPA) Standard for All Industries | | |

RATIONALE

This standard defines the steps, tasks, and flow necessary to execute a System Theoretic Process Analysis (STPA) system safety evaluation and outlines the expected deliverables. It is applicable to all industries.

This standard references content from SAE J3187 and the STPA Handbook. This standard utilizes state-of-the-art STPA methodologies developed and successfully used by expert STPA practitioners and facilitators over the past decade.

FOREWORD

This document was developed by a balanced committee and represents state-of-the-art thoughts and practices on the subject from the viewpoint of experienced STPA practitioners and STPA consultants.

TABLE OF CONTENTS

| | | |
|-------|-----------------------------------|---|
| 1. | SCOPE..... | 3 |
| 1.1 | Purpose..... | 3 |
| 2. | REFERENCES..... | 4 |
| 2.1 | Applicable Documents..... | 4 |
| 2.1.1 | SAE Publications..... | 4 |
| 2.1.2 | ISO Publications..... | 4 |
| 2.1.3 | U.S. Government Publications..... | 4 |
| 2.1.4 | Other Publications..... | 4 |
| 2.2 | Related Publications..... | 5 |
| 2.2.1 | SAE Publications..... | 5 |
| 2.2.2 | RTCA Publications..... | 5 |

Excerpts from SAE J3307_202503 STPA Content

Table 1 - Required work product deliverable(s) summary

Steps:



Required Elements:

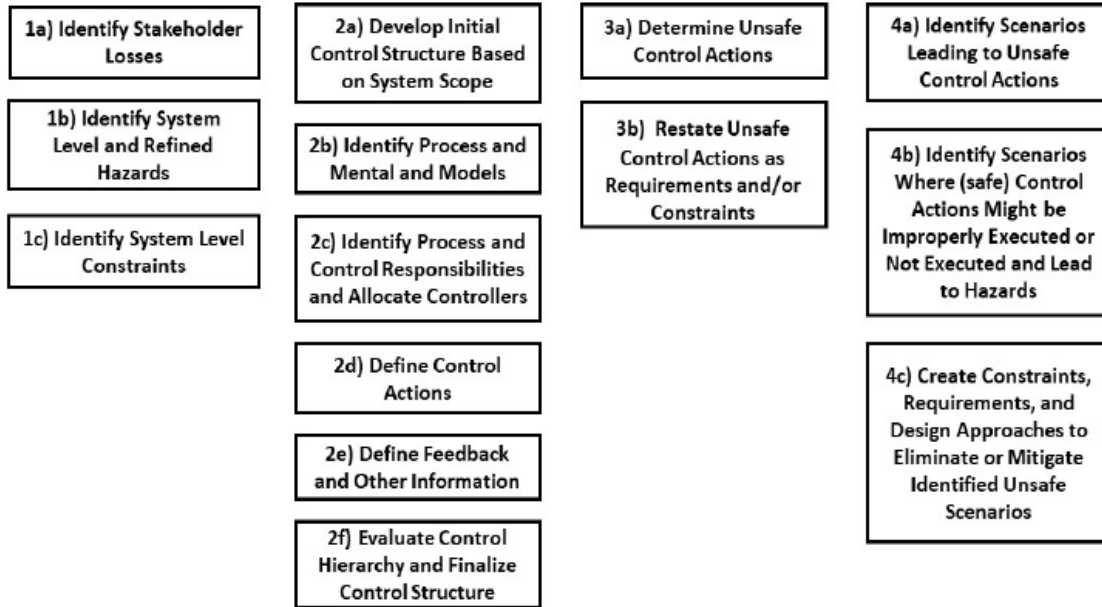


Figure 2 - Main STPA steps and sub-steps

| 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 |
| 2d | Define Control Actions | 2d-1: Identified control actions needed so that each responsibility is executed as intended |
| 2e | Define Feedback and Other Information | 2e-1: Identified necessary feedback and other information each element requires so it may execute its responsibilities |
| 2f | Evaluate Control Hierarchy and Finalize Control Structure | 2f-1: Finalized control structure(s) showing elements with a higher level of control authority higher in the control structure 2f-2: Definition of control actions taking precedence over other control actions when an element receives multiple inputs 2f-3: Appropriate names and labels for each element in the control structure with a brief description |

Task Force Member Skill Sets

- 95% Members are STPA Practitioners (5% Familiar w/STPA)
- Members from multiple organizations
 - General Motors, Ford Motor Company, Stellantis, Audi, Volkswagen, Nissan, Zoox, Google, Virginia Commonwealth University (VCU), WMG - University of Warwick, VOLPE, Edge Case Research, in2being LLC, German Aerospace Center (DLR), MIT, Autonomous Solutions, US Army, Epiroc, Continental, National Research Council of Canada, FAA, Siemens, Elektrotbit Automotive, Boeing, Northrop Grumman, Israel Defense Industry, Security Concepts and Strategic, Waymo, etc.
- Members have collectively hundreds of years of system safety analysis and risk determination experience

Keeping Task Force Member Engaged in Effort

- Allowing members to be active and dormant in Task Force activities as their schedules allow
- Conducting two identical monthly meetings at different times (Tuesday 6:15 pm ET and Thursday 9:00 am ET) to enable better world-wide participation. Minutes were culmination of both meetings.
- Breaking Task Force efforts into sub-groups with their own leader to develop specific documents based on Task Force consensus
- Listening, listening, listening to and supporting members' inputs, criticism, contributions, and opinions during meetings
- Seeking common ground for agreement
- Setting clear goals and flexible timing for document efforts

Navigating SAE Hierarchy and Processes

- Knowledgeable about SAE organizational hierarchy
 - Top Level – Councils (Motor Vehicle, Aerospace, Systems Mgmt)
 - Mid Level – Committees (Answering to one of the three councils)
 - Working Level – Task Forces (Formed by Committee approval)
- Understand SAE document type and templates
 - Individual Papers, Recommended Practices, and Standards
- Coordinate document development with other committees' efforts
- Get formal approval of document type & development from sponsoring committee
- Be very familiar with SAE document review, balloting and approval processes
 - Draft development and consensus within Task Force
 - Review in 28-day (comments and feedback) and 14-day ballots (approval) by sponsoring committee
- Be patient, patient, and more patient with development and approval processes

Issues Experienced Along the Way and Their Solutions

- Creating membership with appropriate skills
 - Participated in STAMP Birds of a Feather sessions
 - Presentations of Task Force activities at various system safety conferences to generate interest
 - Soliciting members for like-minded individuals to join
 - Developing clear vision of what Task Force is to accomplish
- Thinking we were developing a standard when we were not
 - J3187 started in 2018 with intent of creating a standard for STPA
 - Not familiar with SAE “standard” vs “recommended practice” intent
 - Ended up using J3187 content to publish recommended practice first, then realigned to develop standard

Issues Experienced Along the Way and Some Solutions

- Anticipating approval ballot questions and education
 - Used existing SAE FMEA standard J1739 as a template for J3307. This helped when one MVC member thought J3307 should be a recommended practice, not a standard – pure opinion. Showing J1739 as basis handled this.
 - Have organized rationale available to respond to ballot comments
 - Be sure to respond to every ballot comment and seek resolution with voter
- Lack of a “formal motion” in sponsoring committee minutes (even though we had been working on this for years – lost three months in publication time to remedy this with a “new” formal motion)
- Constraining document templates and improperly formatted minutes
- Losing composure when frustrated by approval process
- Remembering everyone has something worthwhile to contribute (even if your first thought is not along those lines)

Summary

- J3307_202503 was released March 26, 2025, after a five-year effort (with a J3187 re-write 😊)
- Understanding approval process within the sanctioning body is critical
- Keeping your cool as process proceeds for your own integrity that will serve you better as process continues
- Never giving up even when it seems you're moving backwards

QUESTIONS??

markv.sseggroup.011@gmail.com

STPA Recommended Practices All Industries

- SAE J3187_202305 describes how to execute a System Theoretic Process Analysis (STPA) of safety-critical products or systems in all industries. It provides recommended practices regarding how System Theoretic Process Analysis (STPA) may be applied to safety-critical systems in any industry.

CURRENT

REVISED

2023-05-22

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry [J3187_202305](#)

This document provides recommended practices regarding how System Theoretic Process Analysis (STPA) may be applied to safety-critical systems in any industry.

STPA Recommended Practices All Industries

- SAE J3187_202305 has published appendices
- The STPA Task Force is currently developing appendices for:
 - STPA and Security Engineering
 - STPA and Medical Devices

Existing STPA Recommended Practices

CURRENT REVISED 2023-05-22

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry [J3187_202305](#)

CURRENT ISSUED 2023-09-06

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Human Machine Interactions (HMIs) [J3187-1_202309](#)

CURRENT ISSUED 2023-09-06

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Safety of the Intended Functionality [J3187-2_202309](#)

CURRENT ISSUED 2023-09-06

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Model-Based Systems Engineering (MBSE) [J3187-3_202309](#)