



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
3.	DEFINITIONS AND ACRONYMS.....	5
3.1	Definitions.....	5
3.2	Acronyms.....	7
4.	STPA INTRODUCTION.....	8
4.1	What is STPA?.....	8
4.2	Why STPA?.....	9
5.	STPA IMPLEMENTATION.....	9
5.1	When is the STPA Performed?.....	9
5.2	Revisions.....	9
6.	STPA EVALUATION PREREQUISITES.....	9
6.1	STPA Management Support.....	9
6.2	STPA Evaluation Participants.....	10

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2025 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3307_202503

For more information on this standard, visit https://www.sae.org/standards/content/J3307_202503/

Documents



Standard, visit Sharing Hub

6.3	STPA Facilitators and High-Quality STPA Results	10
6.4	STPA Implementation Plan (SIP).....	11
6.4.1	STPA-Related Activities Before STPA Application	11
6.4.2	STPA-Related Activities After STPA Application	12
6.5	Relations Between Systems Engineering and STPA	13
7.	THE CORE STPA STEPS	14
7.1	Define Purpose (Step 1).....	16
7.1.1	Identify Stakeholder Losses (Step 1a)	16
7.1.2	Identify System High-Level and Refined Hazards (Step 1b)	17
7.1.3	Identify System-Level Constraints (Step 1c).....	17
7.2	Model Control Structure (Step 2)	18
7.2.1	Develop Initial Control Structure Based on System Scope (Step 2a).....	19
7.2.2	Identify Process and Mental Models (Step 2b)	19
7.2.3	Identify Process and Control Responsibilities and Allocate Controllers (Step 2c).....	20
7.2.4	Define Control Actions (Step 2d)	20
7.2.5	Define Feedback and Other Information (Step 2e).....	21
7.2.6	Evaluate Control Hierarchy and Finalize Control Structure (Step 2f)	21
7.3	Identify Unsafe Control Actions (Step 3).....	22
7.3.1	Analyze Each Control Action to Determine How it Can be Unsafe (Step 3a).....	22
7.3.2	Restate Unsafe Control Actions as Requirements and Constraints (Step 3b)	23
7.4	Identify Loss Scenarios (Step 4)	24
7.4.1	Identify Scenarios Leading to Unsafe Control Actions (Step 4a).....	24
7.4.2	Identify Scenarios Where Control Actions Might Improperly be Executed/Not Executed Causing Hazards (Step 4b).....	25
7.4.3	Create Constraints, Requirements, and Design Approaches to Eliminate/Mitigate Identified Loss Scenarios (Step 4c)	27
7.5	Requirements Summary	27
8.	STPA AND TRACEABILITY	29
9.	SUMMARY	30
10.	NOTES	30
10.1	Revision Indicator	30
APPENDIX A	ACTIVITIES THAT APPLY ACROSS AND WITHIN STPA STEPS	31
APPENDIX B	STPA AND RISK ESTIMATION.....	32
APPENDIX C	IMPROVEMENTS TO STPA METHODOLOGY	33
APPENDIX D	EXAMPLE STPA IMPLEMENTATION PLAN (SIP).....	35
APPENDIX E	STPA STEPS APPLIED BASED ON ABSTRACTION LEVEL SELECTED	37
Figure 1	Systems engineering “V” model and STPA	14
Figure 2	Main STPA steps and sub-steps.....	15
Figure 3	Main STPA Step 1.....	16
Figure 4	Main STPA Step 2.....	18
Figure 5	Hierarchical control structure showing control authority	18
Figure 6	Main STPA Step 3.....	22
Figure 7	Main STPA Step 4.....	24
Figure 8	Traceability between various STPA outputs	29
Table 1	Required work product deliverable(s) summary	28
Table 2	STPA evaluation prerequisite summary.....	29

1. SCOPE

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.

1.1 Purpose

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. This standard may be used to integrate STPA activities into a company-specific development or assurance framework.

This document provides a universal definition of STPA that can be applied to any industry. STPA has over a decade of documented use across industries including defense, aviation, space, automotive, healthcare, nuclear, oil and gas, chemical, and others.

The purpose of STPA is to provide a systems-based analysis using an extended model of accident causality that includes both traditional and modern causes of losses, such as:

- Intended functions or features that inadvertently lead to losses
- Unintended functions or features that inadvertently emerge from lower-level functions and interactions
- Missing functions or features that are necessary to prevent losses
- Interactions among non-failed components, functions, or features that lead to losses
- Known random or systemic failures that may only lead to losses in complex, unanticipated ways
- Operational conditions and assumptions that can lead to losses
- Human interactions, human errors, decision-making, and other human factors
- Automation behaviors, interactions, and decision-making that may lead to losses
- Automation-induced human errors (e.g., mode confusion)
- Missing, dysfunctional, or otherwise flawed requirements
- Missing, dysfunctional, or otherwise flawed procedures
- Flaws across multiple control layers such as the physical layer, data layer, automated detection and response layer, human operator layer, supervisory layers, management layers, organizational layers, and regulatory layers

- Causes of losses related to maintenance, serviceability, adversary behaviors, intentional or unintentional actions, privacy, performance, and other operational considerations
- Common cause failures, errors, or other conditions that defeat planned mitigations
- Flaws introduced throughout the life cycle including the concept, requirements, design, implementation, test, and operational phases

Information marked as “NOTE:” is for guidance in understanding or clarifying associated content.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J1739 Potential Failure Mode and Effects Analysis (FMEA), Including Design FMEA, Supplemental FMEA-MSR, and Process FMEA

SAE J3187 System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry

2.1.2 ISO Publications

Copies of these documents are available online at <https://webstore.ansi.org/>.

These documents are listed as they relate to system safety processes and the use of hazard identification and requirements generation methods like STPA.

ISO 21448 Safety of the Intended Functionality (SOTIF)

ISO 26262 Road Vehicles - Functional Safety

ISO/IEC/IEEE 15288 Systems and Software Engineering - System Life Cycle Process

ISO/IEC/IEEE 16085 Systems and Software Engineering - Life Cycle Processes - Risk Management

ISO/SAE 21434 Road vehicles - Cybersecurity Engineering

2.1.3 U.S. Government Publications

Copies of these documents are available online at <https://quicksearch.dla.mil>.

MIL-STD-882E System Safety

2.1.4 Other Publications

Leveson, N.G. and Thomas, J.P. (2018). *STPA Handbook*. Massachusetts Institute of Technology (MIT) Partnership for Systems Approaches to Safety and Security (PSASS).

Thomas, J. (2024). *STPA Step 4 - Building Formal Scenarios - A New Scenario Approach*. MIT STAMP Workshop, Cambridge, MA, USA.

2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

2.2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

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

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

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

2.2.2 RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

DO-356A/ED-203A Airworthiness Security Methods and Considerations

3. DEFINITIONS AND ACRONYMS

Definitions, examples, and terms clarify words and concepts used in this document that are not otherwise defined in the body of the text. Outside of STPA, other definition descriptions may be used in other industries or methodologies.

3.1 Definitions

ABSTRACTION: A model of the system conceived by the viewer. Higher levels of abstraction represent a simplified system version illustrating major levels of interactions and system content. Levels of abstraction can be used to zoom in on the pieces of the control structure currently being considered. Selecting some factors as relevant to the specific level of abstraction and others as irrelevant is arbitrary and based on the viewer's judgment.

NOTE 1: Systems may be part of a larger system or be divisible into subsystems (viewed as components of the overall system). Control structures use abstraction to help manage complexity. Abstraction principles can also be applied to the control and feedback paths in the control structure.

NOTE 2: High-level abstract control structures can be used to begin STPA and identify the system requirements and constraints. Then STPA results can be used to drive the architecture, preliminary and detailed design, implementation decisions, and refinement of the control structure. Even if details are known, and design decisions have been made, applying STPA at a higher abstract level first can be helpful to provide quicker results and identify broader issues before analyzing more detailed control structure models.

ACCIDENT: An undesired or unplanned event that results in a loss, including loss of human life or human injury (i.e., harm), property damage, environmental pollution, mission loss, reputational damage, etc.

CAUSAL FACTOR: A circumstance, fact, or influence contributing to a causal scenario.

CAUSAL SCENARIO: The reasons, situations, circumstances, or incidents that may cause a control action to occur.

CONOPs: A document describing the characteristics of a proposed system from the viewpoint of individuals who will use that system.

CONSTRAINT: Specified restrictions on the acceptable behavior of a system or a component of a system to prevent or mitigate a hazard; the conditions or behaviors that need to be satisfied to prevent hazards (and ultimately prevent losses).

CONTROL ACTION: A command, instruction, directive, or other information provided by a controller to control a process and achieve goals.

NOTE 1: A control action is an observable output of a controller as opposed to beliefs, responsibilities, functions, and goals that may or may not be directly observable outside of a controller.

NOTE 2: Functions generally define the behaviors intended (or assumed) by designers to achieve and maintain a safe state, whereas control actions define possible actions, safe or unsafe, that controllers can provide to a controlled process to achieve or maintain a state. Control actions emphasize the range of possible controls needed to achieve safety, security, or other goals.

NOTE 3: Control actions can be defined and analyzed at high levels of abstraction (e.g., execute passing maneuver, decelerate vehicle, decrease training budget) and low levels of abstraction (e.g., turn left 5 degrees, apply 50% brake, remove scenarios from simulator training). They can be physical actions (e.g., “open valve”) or virtual (e.g., “set flow rate”).

CONTROL ALGORITHM: A control algorithm specifies how control actions are selected based on the controller’s process model, previous control inputs and outputs, and other factors. For human controllers, the control algorithm is sometimes called decision-making, and different factors like training, procedures, and experience may shape it.

CONTROL STRUCTURE: A hierarchical structure that models the layers of control in a system. Each level imposes constraints on the activities of the levels below, and each level may receive feedback or other information about the levels below. Control structures model the relationships and interactions between controllers, controlled processes, control actions, feedback, and other information (see ABSTRACTION notes).

CONTROLLED PROCESS: Any process such as a physical process, a virtual process, a controller, or other process that receives control actions from and provides feedback to higher-level controllers in a control structure. Processes with specified restrictions that bound the performance of its intended behavior.

CONTROLLER: An entity that forms beliefs, makes decisions, and provides control actions to achieve or maintain a state or goal.

NOTE: Controllers may be implemented as hardware, software, AI, humans, teams, organizations, regulatory bodies, or other forms. They can be abstract entities made up of other controllers. Controllers may provide control actions to any controlled process, including physical processes, virtual or data processes, other controllers, or other entities.

CUSTOMER: Any individual or entity that requests and receives the results of an STPA evaluation.

ELEMENT: System or part of a system including humans, components, controllers, hardware, software, and surrounding environments

FAILURE: Termination of the ability of an element or function to perform as specified.

FAULT: Abnormal condition that can cause an element to fail.

FUNCTION: An intended behavior of a system or an element of a system regardless of implementation

NOTE: Functions may not completely describe the actual behavior of an element - only the intended behaviors. Functions may be safe, unsafe, secured, or unsecured. Functions may not capture all emergent behaviors such as unintended, unplanned, undocumented, unsafe, and interactive. Functions can cause control actions, and control actions can cause functions. Functions may help achieve system goals or may interfere with system goals in non-trivial ways. Some control actions may directly correspond to certain functions, like a Decelerate command and a Decelerate function. Some control actions may only indirectly correspond to certain functions, like a Maintain Speed function and an Automation Off command. Control actions can be used to identify missing functions or to help validate the set of functions. Control actions are also related to system states, responsibilities, beliefs, goals, and other factors.

HARM: Physical injury or damage to the health of persons.

HAZARD: A system state or set of conditions that together with a particular set of worst-case environmental conditions, will lead to a loss (refer to STPA Handbook) or a potential source of harm (refer to ISO 26262).

LOSS: The act or fact of being unable to keep or maintain something valued by a stakeholder. Losses may include harm to people, property losses, environmental losses, mission losses, loss of system performance, reputation losses, or any other relevant losses determined by the stakeholders.

LOSS SCENARIO: Describes why and how causal scenarios or factors can lead to unsafe control actions and hazards.

MALFUNCTION: A condition where an element or function operates in a way that is different than its specified behavior.

MENTAL MODEL: An explanation of someone's thought process about how something works in the real world. It represents the surrounding world, the relationships between its various parts, and a person's intuitive perception about their own acts and consequences.

PROCESS MODEL: A representation of a controller's internal beliefs used to make decisions. Process models may include beliefs about the controlled process or other relevant aspects of the system or the environment. Process models may be partly updated by feedback used to observe the controlled process.

REQUIREMENT: Describes what any element shall do (i.e., is required to do, must be done). A requirement does not necessarily only cover a part of the system (element) but could also cover the whole system.

RESPONSIBILITIES: Responsibilities are a refinement of the safety constraints - what each entity needs to do so that the safety constraints will be enforced together.

RISK: The potential unintentional consequences inherent in a situation or activity, typically assessed using the combination of the likelihood of occurrence and severity of the effect.

NOTE: For more information on risk, refer to SAE J1739 for a discussion of reliability-based risk; refer to ISO 26262 for a discussion of hazard-based risk; and refer to ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 16085.

SAFETY: Absence of losses or, depending on the industry, absence of unreasonable risk based on stakeholders' assessment.

STAKEHOLDER: A stakeholder is a person, group, or organization with a vested interest, or stake, in the decision-making and activities of a business, organization, or project. Stakeholders specify unacceptable losses associated with a system or product, where these losses represent any emergent system property that should be avoided.

NOTE: Stakeholders may include customers, suppliers, owners, investors, creditors, communities, trade unions, employees, government agencies, or others.

UNSAFE CONTROL ACTION: Control action that, in a particular context, will lead to a hazard and may eventually, given worst-case environmental conditions, lead to losses.

NOTE: See Step 3 of the STPA process for other acceptable terms. This standard allows them to be used in place of "unsafe control action" where applicable based on industry.

3.2 Acronyms

CAST	Causal Analysis based on System Theory
DFMEA	Design Failure Mode and Effects Analysis
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis

HARA	Hazard Analysis and Risk Assessment
HMI	Human-Machine Interaction
INCOSE	International Council on Systems Engineering
ISO	International Organization for Standardization
MBSE	Model-Based Systems Engineering
PHA	Preliminary Hazard Analysis
SME	Subject Matter Expert
STAMP	Systems Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
UCA	Unsafe Control Action

4. STPA INTRODUCTION

4.1 What is STPA?

STPA is a hazard analysis technique based on an extended model of accident causation. In addition to functional and component failures, STPA assumes that losses can also be caused by unsafe interactions of system functions and components, none of which may have failed, as well as functional insufficiencies in certain operational situations. STPA treats safety as a dynamic control problem rather than a failure prevention problem.

The basic steps of STPA may be summarized as:

- Defining the purpose of the analysis. What kinds of losses will the analysis aim to prevent? Will STPA be applied only to traditional safety goals like preventing loss of human life, or will it be applied more broadly to security, privacy, performance, and other system properties? What is the system to be analyzed, and what is the system boundary?
- Build a control structure model of the system. A control structure captures functional relationships and interactions by modeling the system as a set of feedback control loops. The control structure usually begins at a very abstract level and is iteratively refined to capture more detail about the system. This step does not change regardless of whether STPA applies to safety, security, privacy, or other properties.
- Analyze control actions in the control structure to examine how they could lead to hazards that may result in the losses defined in the first step. These unsafe control actions create functional requirements and constraints for the system. This step for requirements development remains the same regardless of whether STPA applies to safety, security, privacy, or other properties.
- Identify the reasons why unsafe control occurs in the system. Scenarios are evaluated to explain how:
 - Incorrect feedback, inadequate requirements, design errors, component failures, and other factors could cause unsafe control actions and ultimately lead to losses.
 - Safe control actions might be provided but not followed or executed properly, leading to a loss.

4.2 Why STPA?

STPA is a hazard analysis technique for documenting the hazards that may lead to losses, identifying their causes, including traditional failure-based causes, and creating requirements to prevent or manage the hazards.

STPA enables the exploration of potential causes of losses early in the system concept development phase. Functional and logical architectures may be evaluated when minimum design detail is available.

STPA allows human interactions to be modeled as part of a control system, something not typically captured by traditional methods such as FMEAs and FTAs. STPA enables the evaluation of the interactions between system element functions that may lead to hazards even when nothing has failed.

5. STPA IMPLEMENTATION

STPA is generally performed and reviewed by a cross-functional team with knowledge that spans each part of the control structure. The exact team composition depends on the application and the scope. It may include, for example, individuals with expertise in human factors, engineering, operation, design, analysis, testing, manufacturing, assembly, service, recycling, quality, and reliability. The STPA should be a catalyst to stimulate the interchange of ideas between the functions and disciplines affected and thus promote a team approach.

5.1 When is the STPA Performed?

To achieve the greatest value, the first STPA iteration should be done early in the concept development phase to assist in designing safety or other system properties into the original system design. Spending time upfront to properly complete a high-level STPA early, when product/process changes can be most efficiently and inexpensively implemented, will minimize the impact of changes later in the design process.

However, STPA can be applied at any phase. The STPA hazards, causes, requirements, and solutions can still be identified during later phases. Late application of STPA may identify critical flaws that are expensive to fix in later system design phases. Therefore, applying STPA as early in the process as possible is advantageous to finding these flaws when they are less expensive to fix.

An STPA Implementation Plan (SIP) should define when STPA is first applied, how and when the STPA results will be used, and when each successive iteration will be performed.

NOTE: The SIP can be an integral part of other safety planning documents (e.g., the Safety Plan). See Appendix C.

5.2 Revisions

Due to its iterative and abstraction-based nature, STPAs are revised and enhanced as the system matures and more detailed content emerges.

6. STPA EVALUATION PREREQUISITES

An STPA evaluation includes various activities to support and facilitate its execution within any organization. This section describes the activities, working groups, and information involved in an effective and efficient STPA evaluation.

6.1 STPA Management Support

Management establishes a standard policy regarding applying STPA to the program or the corporation's overall development process, from concept design through validation, start of production, and beyond. This includes STPA planning in relation to engineering project management. Management enables STPA by requiring and prioritizing a proactive hazard analysis of a system that they own, control, or influence.

Management has the authority to manage resources and set priorities to delegate tasks for STPA completion. Management establishes the design and process of STPA ownership for each analysis. Management is responsible for supporting the cross-functional team by monitoring project status and team attendance, participating in the management reviews, and asking thought-provoking questions.

Management ensures that the competence of the individuals involved in the STPA evaluation is commensurate with their responsibilities and roles. Management also ensures that the required resources are provided for STPA analysis.

Management ensures a system is in place for storing and retrieving STPA documents and determines when an STPA is deemed Confidential.

6.2 STPA Evaluation Participants

An STPA Core Team depends on the project scope. The Core Team consists of knowledgeable individuals who perform the STPA analysis, but they need not have the same level of experience as the Facilitator (see 6.3). The Core Team is generally a cross-disciplinary team that includes representatives familiar with different aspects of the system. This may include, but is not limited to, representatives from: operations, system design (systems, software, mechanical, electrical, safety, etc.), manufacturing, suppliers, materials, service, quality, and technical experts. Team members are responsible for preparing STPA results, participating during STPA meetings and reviews, and addressing review comments and feedback.

An STPA Support Team consists of Subject Matter Experts (SMEs) available to the Core Team to provide specialized technical input and answers to questions. The Support Team does not need Core Team STPA qualifications. The STPA Facilitator may invite Support Team members to answer questions, participate in reviews, and participate in other ways as appropriate.

Customer-specific requirements for STPA are discussed at the beginning of a new customer program: scope, timing, deliverables, special rating charts, special forms, etc. If planned to be used, then the customer provides an STPA audit worksheet at the beginning of a project to review the STPA at the end of a project (to avoid misunderstandings).

6.3 STPA Facilitators and High-Quality STPA Results

An STPA Facilitator (moderator, coordinator, coach, etc.) is responsible for properly applying the STPA method. Facilitators provide expert guidance on the STPA method, review the results from an STPA method perspective, answer technical questions from the team about the method, identify inconsistencies in the draft results, identify open areas to address, propose next steps, and help introduce the work to those outside the core STPA team. The STPA Facilitator works to determine meeting agendas, necessary time commitments, and potential support outside the core team that may be needed to meet the project timing.

Experienced STPA facilitators are crucial in achieving high-quality STPA results. While this standard does not specify qualifications for STPA facilitators, it does offer some useful traits of effective facilitators, including:

- Good interpersonal skills and behavior: Ability to convey STPA concepts clearly and effectively.
- Competence in execution: Skillful in executing STPA with precision and quality gained from actual STPA application experience.
- Experience: Having conducted and evaluated STPA, completed all four steps, and produced useful results from multiple STPA evaluations.
- Ability to identify and correct mistakes: Capable of identifying errors in the application of STPA and correcting them efficiently.

These traits help ensure the Facilitator can guide the process effectively, leading to successful outcomes.

NOTE: Outside Facilitators are useful until internal Facilitators can be developed.

6.4 STPA Implementation Plan (SIP)

The STPA Implementation Plan (SIP) defines the STPA-related responsibilities and activities before, during, and after the application of STPA. The SIP describes how the STPA process is implemented in a way consistent with this standard and other applicable guidance documents. Section 7 discusses the activities required during the application of STPA, which is consistent with the guidelines in the STPA Handbook. This section describes systems engineering-related activities before and after the application of STPA.

NOTE 1: The standard does NOT require the activities listed in this section. The required standard STPA activities and deliverables are described in Section 7. These activities are highly encouraged as they have been shown to help organizations attain a high-quality STPA application.

NOTE 2: See Appendix D for more information on the content of the SIP.

6.4.1 STPA-Related Activities Before STPA Application

Various activities occur before the STPA application to organize information and assign appropriately qualified resources to the effort. These activities are listed here to provide an outline of what is expected before an STPA application.

- Define the roles represented on the Core STPA team, consistent with the STPA Handbook. The roles include suitable cross-disciplinary participants, relevant SMEs, a qualified STPA Facilitator, and other roles as appropriate.
- Determine the approximate total size and required effort of the Core STPA team that is considered suitable to ensure STPA is performed correctly and completely.
- Determine the STPA training requirements for the Core STPA team.
- Develop a program timeline for STPA and organizational interactions
- Establish the criteria for conducting internal and external reviews to ensure the quality of STPA, including:
 - The total number of reviews.
 - The relationship between the reviews and each development stage or milestone.
 - The required participants and responsibilities at each review.
 - The format for documenting STPA results and making them easily accessible to interdisciplinary reviewers.
 - How review comments and action items are collected and documented.
 - The process for tracking action items and ensuring they are addressed.
 - The hazard tracking system shall formally track the STPA results.
 - The concurrent and downstream activities that are informed by the STPA results.
- Describe how STPA results will be integrated into safety assessments and other artifacts supporting design reviews.

These activities are typically found in the systems engineering and program management processes of organizations applying STPA. An organization may execute additional activities according to its own systems engineering and program management processes.

6.4.2 STPA-Related Activities After STPA Application

Various activities occur after the application of STPA to organize information and document results of the STPA application and to have the organization accommodate these requirements into its design, development, and testing processes. Such activities are listed here to outline what is expected after an STPA application. Each organization may decide how to accommodate STPA requirements in a manner that best fits the organization's processes and structures.

- STPA results are used to minimize the risk of unplanned rework.
- STPA results are used to minimize the possibility of flaws and weaknesses found during technical reviews.
- STPA results are used to minimize the possibilities of flaws and weaknesses found during testing.
- STPA results are used to design mitigations for hazards and to verify that mitigations don't introduce new unknown risks into the system.

A final report summarizing STPA results is typically written as part of an organization's engineering process. In addition to STPA results, such a summary may include information such as:

- Title/identification of the system/component/program
- Title of document
- Contract number
- Preparing activity or contractor's title
- Security classification, when required
- Distribution statement
- Date of generated document
- System description: This includes summary descriptions of the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation, should be supplied when such documentation is available. The system, components, capabilities, limitations, and interdependence of these components should be described in terms relevant to safety, security, mission assurance, and its operational environment. The description should include:
 - A description of any use of automation and its role(s)
 - A description of any human interactions and responsibilities
 - A description of mission(s), operational environments, and contextual factors
 - A description of any assumptions made during the analysis
- Data: This consists of summaries of data used to determine the safety, security, and mission aspects of design features.

- STPA Reviews conducted, documenting:
 - Scope of each review
 - Summary of participating SME areas of expertise for each review
 - Summary of participating qualified STPA Facilitators for each review
 - Outcome (e.g., accepted with minor changes)
- Remarks: Any information relating to the analysis not covered in other blocks; for example, applicable documents, previous experiences on similar systems, or administrative directions.
- Status: The status of actions to implement the recommended, or other, solutions. The status should include not only an indication of “open” or “closed” but also a reference to the drawing(s), specification(s), procedure(s), etc., that support the closure of the particular action.

6.5 Relations Between Systems Engineering and STPA

The activities associated with each major step of the STPA process provide STPA results that influence, modify, correct, or confirm system content as it matures during the engineering process. STPA activities are closely integrated with an organization's design, development, verification, and validation processes at various points along the system timeline. Figure 1 shows how STPA steps relate to an organization's engineering environment.

At a high level, stakeholder needs and objectives define the system of interest's operational, financial, timing, and performance objectives. Stakeholders identify unacceptable losses associated with the system, document them, and provide them to the STPA Core Team. The STPA Core Team executes the STPA steps. It provides the resulting Loss Scenarios to the product or project group so necessary updates to the system architecture and design are made, and requirements to prevent or mitigate system hazards are documented.

System stakeholders use the system hazards and constraints to determine whether the identified hazards and associated risks are acceptable. If not, they modify the system scope, goals, and objectives accordingly early in the engineering process.

System hierarchy of control information contributes to the creation and modification of system functional decomposition and the allocation of functions to appropriate system elements.

Undesirable system behaviors and loss scenarios contribute to developing system requirements necessary to prevent or minimize risk associated with identified hazards.