

SAE J3187 STPA RECOMMENDED PRACTICES

MIT STAMP WORKSHOP
JUNE 06, 2022

Mark A. Vernacchia, GM Technical Fellow
Making Presentation as the SAE J3187 Task Force Chair

J3187 SAE Recommended Practices for Automotive Safety Critical Applications published Feb 16, 2022 – (SAE website)

The screenshot shows the SAE International website interface. At the top, there is a navigation bar with links for Standards, Publications, News, Attend, Learn, Participate, Membership, and Donate. The main content area displays the document title "System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems J3187_202202" with a "CURRENT" status and an "ISSUED" date of 2022-02-16. Below the title is a brief description of the document's scope. To the right, there is a sidebar for "SAE MOBILUS" with a "Preview Document" button and an "Add to Cart" button. At the bottom, there is a table with one row containing the document ID "J3187_202202", the date "2022-02-16", and the status "Latest Issued".

Browse » Standards » J3187_202202

CURRENT **ISSUED** 2022-02-16

System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems J3187_202202

Scope of this effort intends to provide both educational materials and recommended practices regarding how system theoretic process analysis (STPA) may be applied within a safety assessment process focusing on safety-critical content.

[Revision History](#) [Related Info](#)

J3187_202202	2022-02-16	Latest	Issued	

SAE J3187 Task Force - 75 members - 47 organizations

AeroPacific Consulting LLC
AFRL
Andrew Smart Consulting LLC
ANSYS
APTIV
Autonomous Solutions, Inc
Boeing
Continental (Germany)
Cruise
Cummins Inc
Daimler Truck North America
Dana
Dura Automotive
Edge Case Research
Elektrobit Automotive GmbH
Encoresemi

Exida
FCA
Ford
General Motors
Immersion Corporation
INVENSITY GmbH
ISDEFE
Luminar Technologies
Magna Electronics Inc
Mercedes-Benz USA
MIT
Nissan
Northrop Grumman Corporation
NVIDIA
Omnex
Parthenon

Qualcomm
Rolls Royce
SAE Member
SAE ORAD Working Group
Scopus Systems
Siemens PLM Software Inc.
Stellantis
SZ DJI Technology Co., Ltd.
TIER IV
Toyota
Valeo
VOLPE
Waymo
WMG - Univ Warwick
ZOOX

The publication of J3187 marks the conclusion of a three (3) year effort to develop and publish first authoritative document addressing the use of STPA for system critical system evaluation

While J3187 may have started with an automotive focus, during its development, content making it valuable to other industries has been added to produce a more comprehensive document useful to aerospace, defense, regulatory agencies, etc.

The scope J-3187 intends to provide both educational materials and recommended practices regarding how system theoretic process analysis (STPA) may be applied within a safety assessment process focusing on safety-critical content.

Its purpose is to align industry best practices and translate them across industry regarding the implementation and use of STPA across human- and software-intensive systems (controls, human machine interactions (HMI), autonomous, etc.), and to explore focus areas suited for STPA use, or for supplementing other safety tools.

SAE J3187 - SAE STPA Recommended Practices

J3187 was written by experienced STPA practitioners who shared their collective knowledge on how to perform STPA evaluations and how to develop appropriate safety requirements to prevent or manage potential hazards discovered during the STPA process.

Through the STPA process, these safety requirements can prevent or manage scenarios, that could lead to system misbehaviors, which may produce risk, that may result in unwanted losses, human harm, property damage, etc.

In addition, J3187 includes lessons learned by these practitioners while executing STPA evaluations so that others may benefit from their experiences and missteps.



SURFACE VEHICLE RECOMMENDED PRACTICE	J3187™	FEB2022
	Issued	2022-02
System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems		

RATIONALE

Scope of this effort intends to provide both educational materials and recommended practices regarding how system theoretic process analysis (STPA) may be applied within a safety assessment process focusing on safety-critical content.

Purpose of this task force is to align industry (starting with, but not limited to, automotive/aerospace) best practices and translate them across industry regarding the implementation and use of STPA across human- and software-intensive systems (controls, human machine interactions (HMI), autonomous, etc.), and to explore focus areas suited for STPA use, or for supplementing other safety tools.

SAE J3187 - SAE STPA Recommended Practices

TABLE OF CONTENTS

1.	SCOPE.....	6
1.1	Purpose.....	6
2.	REFERENCES.....	6
2.1	Applicable Documents	6
2.1.1	SAE Publications.....	6
2.1.2	Other Publications.....	6
3.	DEFINITIONS	8
4.	ACRONYMS	10
5.	DOCUMENT ORGANIZATION.....	11
6.	BASIC STPA APPROACH AND LESSONS LEARNED.....	11
7.	SAFETY OF THE INTENDED FUNCTIONALITY (SOTIF) AND STPA	37
8.	HUMAN-MACHINE INTERACTION (HMI) AND STPA	52

SAE J3187 - SAE STPA Recommended Practices

9.	MODEL BASED SYSTEM ENGINEERING (MBSE) AND STPA	70
10.	HIGH-LEVEL USE OF STPA WITHIN SAFETY PROCESSES AND STPA WITH OTHER SAFETY EVALUATION METHODS	89
10.1	Introduction	89
10.1.1	STPA Assistance in Established System Safety Processes and/or Standards.....	90
10.1.2	STPA Within a System Safety Process	99
10.2	Analysis Methodology Perspectives - Inductive, Deductive, and Exploratory	100
10.3	Comments on HAZOP and STPA.....	101
10.4	Interactions versus Interfaces	101
10.5	STPA in Human-Machine Interaction (HMI) Evaluations.....	102
10.6	STPA Compared to Other System Safety Analysis Methods	102
10.6.1	Useful Comparison Studies and Presentations	103
10.6.2	Illustrative Analogy for STPA and Other Methodologies.....	104
10.6.3	High-Level Methodology Comparison.....	104
10.7	Summary.....	106
10.7.1	STPA Value.....	106
10.7.2	STPA Application Perspective	106
10.7.3	STPA Effectiveness for Evaluating Human-Machine Interactions within Operating Scenarios.....	106
10.7.4	STPA and Emergent Properties and Behaviors	107
10.7.5	STPA within Existing Safety Evaluation Processes.....	107
11.	EXAMPLES.....	109

SAE J3187 - SAE STPA Recommended Practices

The cross-industry task force that developed SAE J3187 STPA Recommended Practices hopes the content provides useful information to those who desire to leverage the powerful attributes of STPA for system safety evaluations and looks forward to helpful feedback to improve its content in the future

Initial High Level Task Force 2022 Activities:

- Need to gather feedback from members on existing content (April – June 22)
- Develop updated J-3187 content based on feedback for late summer or early fall balloting by Functional Safety Committee (allows short term enhancements)
- Define and agree on additional content for J-3187 (Software examples, cybersecurity, more non-automotive applications, etc.) and schedule activities to see if additional 2022 release is appropriate or for an early 2023 release
- Develop more non-automotive content and examples in 2022

SAE J3187 - SAE STPA Recommended Practices

The Task Force will be preparing to work on the following items to remove concerns that are under discussion in the SAE Functional Safety Committee as part of initial feedback is that J3187 is thought of as an “automotive only” document:

Keep J3187 as Recommended Practices document:

- Eliminate the “cues” indicating automotive only aspect
- Rewrite J3187 Title, Scope, Purpose, and Introduction sections to clearly communicate that J3187 is a broad, useful document for all industries

Use this updated Recommended Practices document as way to start progression to have J3187 as a standard:

- Explain content to other organizations
- Invite and gain participation from other organizations in creating an SAE J3187 standard
- Understand how being a standard may impact potential users and organizations
- Handle the “state of the art” perspective and arrive at consensus

J3187 Feedback from Follow STPA Practitioners is Welcomed

*Special thanks to all the STPA Task Force
members who made J3187 a reality !!*

Mark A Vernacchia

mark.a.vernacchia@gm.com

?? Questions on Today's Content ??

Mark A Vernacchia

mark.a.vernacchia@gm.com