



SAFETY-CRITICAL SYSTEMS RECOMMENDED PRACTICE

J3187™-2

SEP2023

Issued

2023-09

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

RATIONALE

This document provides recommended practices regarding how System Theoretic Process Analysis (STPA) may be applied to safety-critical systems in any industry in the area of Safety of the Intended Functionality (SOTIF) evaluations.

This appendix takes the specific domain info from the original SAE J3187 Recommended Practice (released February 2022) and puts it into a standalone document.

TABLE OF CONTENTS

1.	SCOPE	3
2.	REFERENCES	3
2.1	Applicable Documents	3
2.1.1	SAE Publications	3
2.1.2	ISO Publications	3
2.1.3	BSI Publications	3
2.1.4	STAMP Workshop Presentations	4
2.1.5	Other Publications	4
3.	ACRONYMS	6
4.	SAFETY OF THE INTENDED FUNCTIONALITY (SOTIF) AND SYSTEM THEORETIC PROCESS ANALYSIS (STPA)	7
4.1	Mapping STPA to SOTIF Clauses	7
4.2	Unique Aspects of SOTIF for Specification and Testing Phase	7
4.3	Specification Phase: Using STPA for Requirements Identification	9
4.4	Identification of Relevant Control Actions	9
4.5	SOTIF Clause 6: SOTIF Hazard Identification and Risk Evaluation	11
4.6	SOTIF Clause 9: Definition of Verification and Validation Strategy	11
4.7	Testing Phase	11
4.8	Testing Phase: Using STPA for Scenario Generation	12
4.8.1	Scenery, Environment, and Dynamic Elements	12
4.8.2	Additional Context	13
4.8.3	Pass Criteria/Validation Targets	13
4.9	Case Study: Low-Speed Automated Driving System (LSAD)	15
4.9.1	STPA Step 1	15
4.9.2	STPA Step 2: Control Structure	16

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 © 2023 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, 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 J3187-2_202309

For more information on this standard, visit
https://www.sae.org/standards/content/J3187-2_202309/

Documents

Document Sharing Hub

4.9.3	STPA Step 3: Unsafe Control Action	19
4.9.4	STPA Step 4: Loss Scenarios.....	19
4.9.5	Scenario Generation Based on STPA Outputs.....	20
5.	NOTES	21
5.1	Revision Indicator.....	21
Figure 1	Mapping steps to SOTIF clauses	7
Figure 2	Scenario quadrants with awareness and safety as axes	8
Figure 3	Scenario quadrant with understanding and awareness as axes	9
Figure 4	ODD and ADS behavior with abstract functionality	10
Figure 5	High-level control architecture of an automated driving system	10
Figure 6	Scenery, environmental, and dynamic elements of a test scenario	12
Figure 7	Dynamic elements components.....	12
Figure 8	Control loop with process model beliefs	14
Figure 9	Low-speed automated driving system	15
Figure 10	Control structure for low-speed automated driving system case study	17
Figure 11	Sub-system under analysis for the case study	18
Table 1	Functionality with ODD attributes and behavior competency (example specification)	10
Table 2	Sub-system under analysis for the case study	19
Table 3	Test scenarios based on STPA outputs.....	21

1. SCOPE

This document provides recommended practices regarding how System Theoretic Process Analysis (STPA) may be applied to safety-critical systems in any industry in the area of Safety of the Intended Functionality (SOTIF) evaluations.

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.

AVSC00002202004 AVSC Best Practice for Describing an Operational Design Domain: Conceptual Framework and Lexicon

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

SAE J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

Khastgir, S., Birrell, S., Dhadyalla, G., and Jennings, P. (2018). *The science of testing: An automotive perspective* (Paper no. 2018-01-1070). SAE International. <https://doi.org/10.4271/2018-01-1070>.

Okada, M. and Christensen, A. (2017, October 25). SAE Recommended Task Force - Group 4 Example.

Suo, D., Yako, S., Boesch, M., and Post, K. (2017). *Integrating STPA into ISO 26262 process for requirement development* (Paper no. 2017-01-0058). SAE International. <https://doi.org/10.4271/2017-01-0058>.

2.1.2 ISO Publications

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

ISO/PAS 21448 Road vehicles—Safety of the intended functionality

ISO 26262 Road vehicles functional safety package

ISO 34503 Road vehicles—Test scenarios for automated driving systems—Specification for operational design domain

2.1.3 BSI Publications

Copies of these documents are available online at <https://www.bsigroup.com>.

PAS 1883:2020 Operational Design Domain (ODD) Taxonomy for an Automated Driving System (ADS)—Specification

2.1.4 STAMP Workshop Presentations

Abrecht, B. (2016). *A new approach to hazard analysis for naval systems* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2016/01/8-BlakeAbrecht-W2016.pdf>.

da Costa Ribeiro, D. (2016). *A systems approach to the development of an aircraft smoke control system* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2016/04/6-DaniloRibeiroNEW.pdf>.

France, M.E. (2017). *Engineering for humans: Human-automation interaction in STPA* [Presentation]. Cambridge, MA: Massachusetts Institute of Technology (MIT). Retrieved from http://psas.scripts.mit.edu/home/wp-content/uploads/2017/04/HumansAndAutomationTutorial_MFrance2017.pdf.

Malloy, N.H. (2017). *Integrating STAMP-based hazard analysis with MIL-STD-882E functional hazard analysis: A consistent and coordinated process approach to MIL-STD-882E functional hazard analysis* [Presentation]. Retrieved from https://psas.scripts.mit.edu/home/wp-content/uploads/2017/04/Nicolas-Malloy_Integrating-STAMP-Based-Hazard-Analysis-With-MIL-STD-882E-Functional-Hazard-Analysis.pdf.

Martinez, R.S. (2015). *A comparison of STPA and automotive FMECA* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-Sotomayor-Comparing-STPA-and-FMEA.pdf>.

Pawlicki, T. (2018). *Experiences with STPA in radiation therapy* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2018/04/Wed-PUB-Pawlicki-STAMP-2018.pdf>.

Silvis-Cividjian, N. (2018). *Application of STPA in radiation therapy: A preliminary study* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2018/04/Application-of-STPA-in-Radiation-Therapy-SILVIS-MIT-STAMP-2018-long.pdf>.

Thomas, J. (2020). *When STPA results surprise you: An industry case study employing STPA, fault trees, FMEA, and HAZOP* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/JThomas-When-STPA-Results-Surprise-You-STPAHAZOPFMEAFTA.pdf>.

Thomas, J. and Gibson, M. (2020). *Industry trials to evaluate STPA's effectiveness and practicality for digital control systems* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/Industry-Trials-to-Evaluate-STPA%E2%80%99s-Effectiveness-and-Practicality.pdf>.

Vernacchia, M.A. (2018). *GM presentation for introducing STAMP/STPA tools into standards: SAE STPA recommended practice task force* [Presentation]. Retrieved from <http://psas.scripts.mit.edu/home/wp-content/uploads/2018/04/SAE-STPA-Recom-Pract-Task-Force-Overview-Mark-Vernacchia-GM-27mar18-Rev1.pdf>.

Young, W. (2018). *STPA in cybersecurity* [Presentation].

2.1.5 Other Publications

Cornelio-Martinez, P., De Pirro, S., Vi, C.T., and Subramanian, S. (2017). Agency in mid-air interfaces. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2426-2439. <https://dx.doi.org/10.1145/3025453.3025457>.

Fleming, C.H., Placke, M.S., and Leveson, N.G. (2013). Technical report: STPA analysis of NextGen interval management components: Ground interval management (GIM) and flight deck interval management (FIM). *Massachusetts Institute of Technology (MIT)*. Retrieved from <http://sunnyday.mit.edu/NextGen-Report.pdf>.

France, M.E. (2017). *Engineering for humans: A new extension to STPA* [Master's thesis, Massachusetts Institute of Technology (MIT)]. Retrieved from <http://sunnyday.mit.edu/megan-thesis.pdf>.

Georgiou, O., Biscione, V., Harwood, A., Griffiths, D., Giodano, M., Long, B., and Carter, T. (2017). Haptic in-vehicle gesture controls. *AutomotiveUI '17*, 233-238. <https://doi.org/10.1145/3131726.3132045>.

Immersion. (2017). Study unveils that TouchSense® ads lead to 50% lift in brand favorability. *Immersion*. Retrieved from <https://www.immersion.com/study-unveils-touchsense-ads-lead-to-brand-lift/>.

- Kalra, N. and Paddock, S.M. (2016). Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability? *RAND Corporation*. Retrieved from https://www.rand.org/pubs/research_reports/RR1478.html.
- Khastgir, S., Brewerton, S., Thomas, J., and Jennings, P. (2021). Systems approach to creating test scenarios for automated driving systems. *Reliability Engineering & System Safety*, 215, 107610. <https://doi.org/10.1016/j.ress.2021.107610>.
- Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety*, 136, 17-34. <https://doi.org/10.1016/j.ress.2014.10.008>.
- Leveson, N.G. and Thomas, J.P. (2018). *STPA handbook*. Cambridge, MA: Massachusetts Institute of Technology (MIT). Retrieved from https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.
- OMG. (2022). RAAML: OMG risk analysis and assessment modeling language. *Object Management Group (OMG)*. Retrieved from <https://www.omg.org/spec/RAAML/>.
- Pope, G.M. (2019). Risk management using systemic theoretic process analysis (STPA) [Conference paper]. 2019 *STAMP Workshop*, Cambridge, MA. Retrieved from <https://www.osti.gov/servlets/purl/1524738>.
- Reason, J. (1995). Understanding adverse events: Human factors. *International Journal for Quality in Health Care*, 4(2), 80-89. <https://doi.org/10.1136/qshc.4.2.80>.
- Ressler, G.E. and Vernacchia, M.A. (2018). *Designing in safety tutorial*. International System Safety Society Conference. Phoenix, AZ: ISSS.
- Ressler, G.E. and Vernacchia, M.A. (2019). *Helping beginners use system safety methodologies*. International System Safety Conference. Norfolk, VA: ISSS.
- Skedung, L., Arvidsson, M., Chung, J.Y., Stafford, C.M., Berglund, B., and Rutland, M.W. (2013). Feeling small: Exploring the tactile perception limits. *Scientific Reports*, 3, 2617. <https://doi.org/10.1038/srep02617>.
- Tellis, L., Engelman, G., Christensen, A., Cunningham, A., Debouk, R., Egawa, K., Green, C., Kawashima, C., Nicols, G., Prokhorov, D., Wendling, B., Yako, S., and Kiger, S. (2016). Automated vehicle research for enhanced safety final report. *National Highway Traffic Safety Administration (NHTSA)*.
- Vernacchia, M.A. (2016). *Defining safety requirements for human-machine interactions*. International System Safety Conference. Orlando, FL: ISSS.
- Vernacchia, M.A. (2016). *Internal General Motors system safety training*. Milford, MI: General Motors Company.
- Vernacchia, M.A. (2017). *System concept analysis methods*. Milford, MI: GM Internal Document.
- Vernacchia, M.A. (2018). *Delivering safety through design using early analysis methods*. International System Safety Conference. Phoenix, AZ: ISSS.
- Vernacchia, M.A. (2019). *Integrating STPA into large organizations - Lessons learned at General Motors*. ISSC37 - International System Safety Conference. Norfolk, VA: ISSS.
- Vincoli, J.W. (2006). *Basic guide to system safety* (Second edition). Hoboken, NJ: John Wiley & Sons, Inc.

3. ACRONYMS

ADAS	Advanced driver assistance system
ADS	Automated driving system
DDT	Dynamic driving task
DFMEA	Design failure modes and effects analysis
FIA	Functional interface analysis
FMEA	Failure modes and effects analysis
FTA	Fault tree analysis
HBT	Hazard-based testing
HMI	Human-machine interaction
INCOSE	International Council on Systems Engineering
ISO	International Organization for Standardization
JASPAR	Japan Automotive Software Platform and Architecture
LSAD	Low-speed automated driving
MBSE	Model-based systems engineering
NASA	National Aeronautics and Space Administration
ODD	Operational design domain
OEDR	Object and event detection and response
OMG	Object Management Group
RAAML	Risk analysis and assessment modeling language
SOTIF	Safety of the intended functionality
SUT	System under test
STPA	System theoretic process analysis
UCA	Unsafe/undesired control action

4. SAFETY OF THE INTENDED FUNCTIONALITY (SOTIF) AND SYSTEM THEORETIC PROCESS ANALYSIS (STPA)

Considering a typical V-cycle of product development, one can consider the left-hand side of the V-cycle as the specification phase, while the right-hand side of the V-cycle is the testing phase. The specification phase involves identifying and illustrating the requirements at a system level, functional level, and unit level. The testing phase involves both the verification and validation of the requirements. In this section, we discuss how STPA can be used for both the specification phase and the testing phase. Refer to ISO/PAS 21448:2019.

4.1 Mapping STPA to SOTIF Clauses

In this section, we demonstrate the mapping of the STPA process to the various SOTIF clauses. Consistent with the V-cycle of product development, the SOTIF clauses can also be grouped into two phases: (1) specification phase, and (2) testing phase.

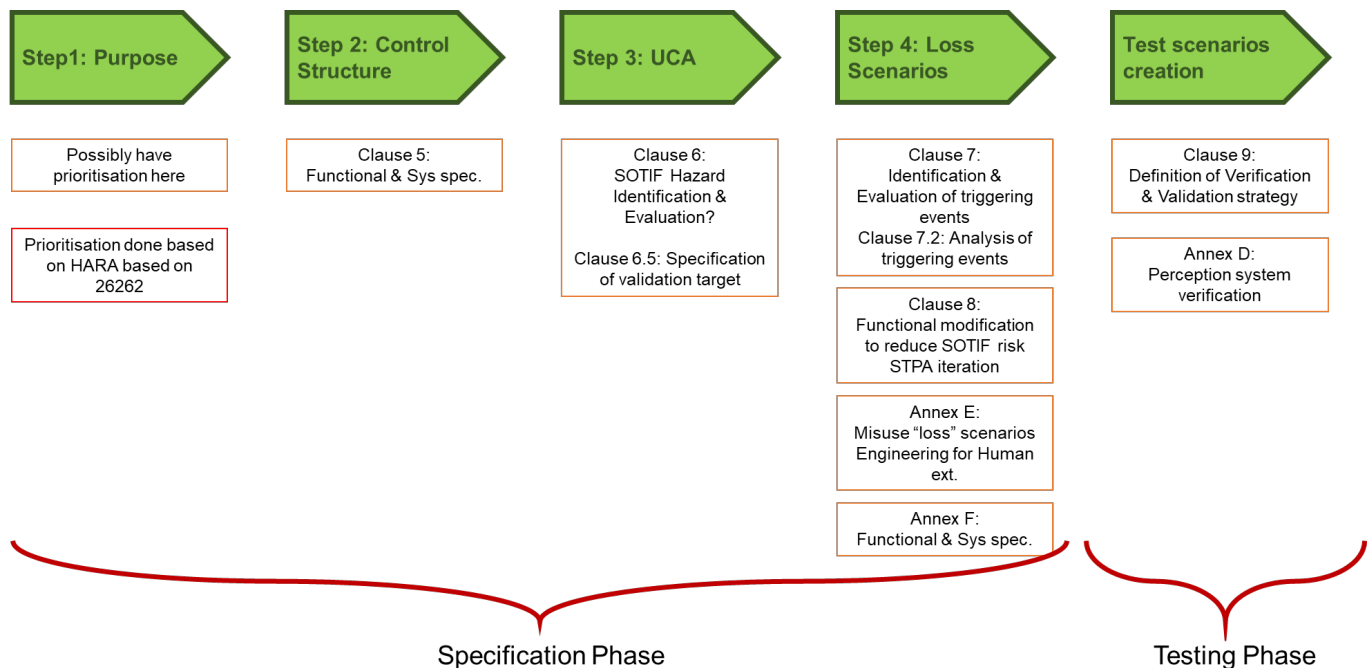


Figure 1 - Mapping steps to SOTIF clauses

The specification phase involves identifying system and functional requirements, while the testing phase focuses on verification and validation involving the identification of test scenarios and safety targets. Steps 1 through 4 form part of the specification phase of the product development life cycle. Additionally, the testing phase of SOTIF specifies the need for identifying test scenarios and pass criteria. The outputs of Steps 1 through 4 can also be used to support this SOTIF need (i.e., the need for test scenarios and pass criteria) as STPA results could help identify those scenarios. [Figure 1](#) illustrates the mapping of the steps to the SOTIF clauses. It is important to highlight that not all SOTIF clauses can be mapped to Steps 1 through 4 or test scenario generation based on Steps 1 through 4. Some aspects of SOTIF remain outside the scope of STPA, and additional methods will need to be adopted to address those clauses. Clauses not addressed by STPA include risk analysis, identification of validation targets, etc.

4.2 Unique Aspects of SOTIF for Specification and Testing Phase

It is suggested that to prove that automated driving systems (ADSs) are safer than human drivers, they will be required to be driven for more than 11 billion miles (Kalra and Paddock, 2016). However, even after driving 11 billion miles, one cannot make a claim for safety without considering the type of scenarios the ADS experienced in the driven miles. For example, if we drive an ADS for 11 billion miles on deserted roads, we have less to gain if our intended deployment area for the ADS is in an urban city center. Therefore, there is a widespread acknowledgment of the need to move away from a number of miles driven to the quality of miles; i.e., scenarios experienced in those miles.