



SAFETY-CRITICAL SYSTEMS RECOMMENDED PRACTICE

J3187™-3

SEP2023

Issued

2023-09

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

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 model-based systems engineering (MBSE) evaluations.

This document 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	STAMP Workshop Presentations	3
2.1.3	Other Publications.....	4
3.	ACRONYMS	5
4.	MODEL-BASED SYSTEM ENGINEERING (MBSE) AND SYSTEM THEORETIC PROCESS ANALYSIS (STPA).....	6
4.1	Modeling STPA	6
4.2	Overview of RAAML and OMG	6
4.3	Overview of Model-Based STPA	7
4.4	Example of Model-Based STPA Applied to an Automotive System	9
4.4.1	Identifying Losses, Hazards, and Control Structure	9
4.4.2	Understanding Operational Contexts/Situations	12
4.4.3	Control Structure Representation	13
4.4.4	UCA Development	16
4.4.5	Loss Scenario Consideration	18
4.4.6	Expanding the Control Structure to Next Level of Detail	22
4.4.7	Transition to MBSE Environment.....	23
4.5	Summary of Benefits of Model-Based STPA.....	24
5.	NOTES	24
5.1	Revision Indicator.....	24

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 J3187-3_202309

For more information on this standard, visit
https://www.sae.org/standards/content/J3187-3_202309/

Documents

Document Sharing Hub

Figure 1	RAAML overview package diagram.....	6
Figure 2	RAAML STPA method overview (RAAML libraries and profiles).....	8
Figure 3	Losses shown in the MBSE domain	10
Figure 4	Hazards shown in MBSE domain	11
Figure 5	Losses (accidents) and hazards in MBSE domain	12
Figure 6	Operational situations in the MBSE domain	13
Figure 7	Initial high-level control structure	14
Figure 8	High-level control structure in MBSE domain	15
Figure 9	UCAs associated with applying brakes when commanded by guidance system	16
Figure 10	UCAs in MBSE domain.....	16
Figure 11	MBSE domain guidewords linked to UCAs.....	17
Figure 12	MBSE domain UCAs linked through contexts to potential hazards.....	17
Figure 13	MBSE domain linkage of system element, functions, and UCAs	17
Figure 14	Scenarios and factors associated with UCAs and initial requirements.....	18
Figure 15	UCAs and loss scenarios in MBSE domain	18
Figure 16	Alternative view of loss scenarios and UCAs in MBSE domain.....	19
Figure 17	Another alternative view of control actions, unsafe control actions, and loss scenarios	19
Figure 18	Factors linked to loss scenarios in MBSE domain	20
Figure 19	Situations corresponding to Step 4 of STPA loss scenario assessment	20
Figure 20	Alternative view of loss scenario linkages.....	21
Figure 21	Scenarios and factors associated with UCAs and initial requirements.....	21
Figure 22	Expanded control structure with brake system sub-elements	22
Figure 23	Expanded control structure in MBSE domain	23
Table 1	Identified losses for intersection example	9
Table 2	Hazards associated with intersection example	10
Table 3	Operational contexts and links to potential hazards	12

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 model-based systems engineering (MBSE) 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.

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

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

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 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].

2.1.3 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 Society Conference. Phoenix, AZ: ISSS.

Vernacchia, M.A. (2019). *Integrating STPA into large organizations - Lessons learned at General Motors*. 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

BS	Brake system
DFMEA	Design failure modes and effects analysis
FIA	Functional interface analysis
FMEA	Failure modes and effects analysis
FTA	Fault tree analysis
GS	Guidance system
HMI	Human-machine interaction
INCOSE	International Council on Systems Engineering
ISO	International Organization for Standardization
JASPAR	Japan Automotive Software Platform And Architecture
MBSE	Model-based systems engineering
NASA	National Aeronautics and Space Administration

OEM	Original equipment manufacturer
OMG	Object Management Group
PS	Propulsion system
RAAML	Risk analysis and assessment modeling language
SOTIF	Safety of the intended functionality
STPA	System theoretic process analysis
UCA	Unsafe/undesired control action

4. MODEL-BASED SYSTEM ENGINEERING (MBSE) AND SYSTEM THEORETIC PROCESS ANALYSIS (STPA)

4.1 Modeling STPA

Using models provides a consistent and machine-readable format. It can be used to answer questions about the composition, completeness, and traceability of elements. Using a model to depict STPA can also be beneficial for these same reasons and allows for multiple analysis views. There is a desire to share data between original equipment manufacturer (OEM) and tier suppliers, which a consistent model-based approach will enable. Many companies develop their own ontology to define a model-based STPA approach that prohibits sharing as the model elements are different, and their relations are not defined the same. If a consistent modeling language and method is used, then it provides the additional benefit of facilitating consistency and sharing the information between companies. This document will discuss one approach using risk analysis and assessment modeling language (RAMML) by Object Management Group (OMG), but there are a myriad of tools that an organization or individual may employ to accomplish the recommended STPA MBSE methodologies.

4.2 Overview of RAAML and OMG

OMG published the RAAML Beta 1 release in December 2020 to support safety and reliability analyses. The purpose of RAAML is to provide a language for defining risk analysis methods that is consistent across industries and multiple tool vendor implementations. In addition, RAAML provides an XML metadata exchange format (.xmi) to exchange analysis data across different tools. There are a number of analysis methods supported in the Beta release of the specification with one of them being STPA, as shown in [Figure 1](#) (OMG, 2022).

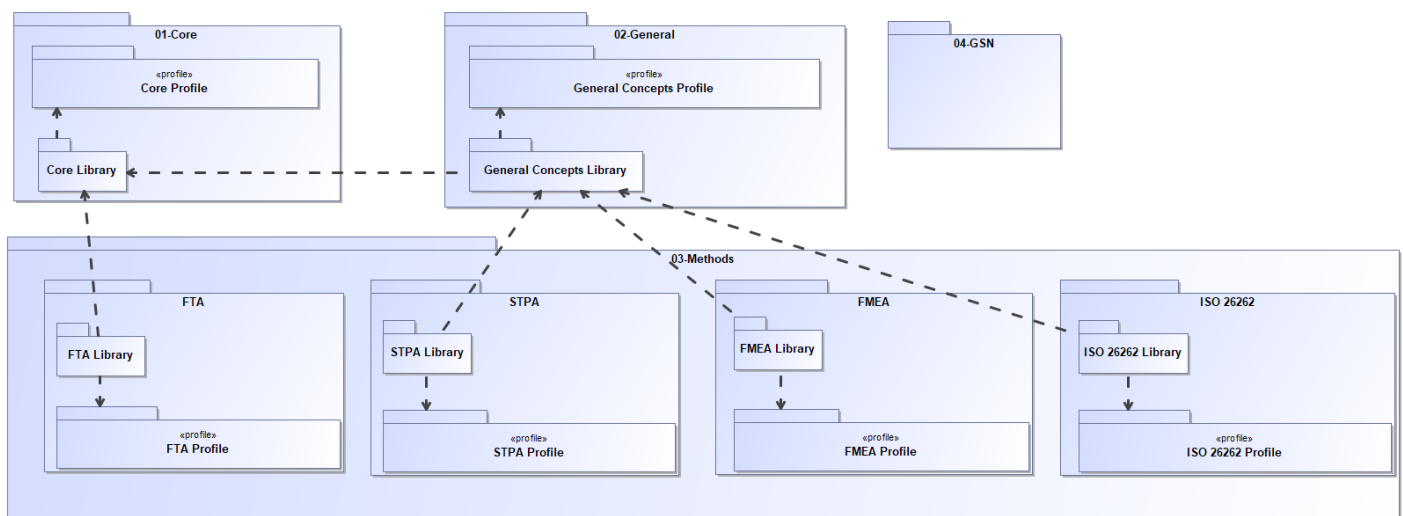


Figure 1 - RAAML overview package diagram (OMG, 2022)
Used with permission from Object Management Group. All other rights reserved.

4.3 Overview of Model-Based STPA

[Figure 2](#) shows the overview of the STPA modeling elements and their relations. The STPA method is defined by using profiles and libraries. This profile and library are built on a number of core and general concepts which are shared across different methods. The shaded blocks in the diagram represent elements that are shared in the general concepts, while the non-shaded blocks represent elements unique to STPA (OMG, 2022).

In addition to elements representing the accident model, there are STPA specific elements to construct the control structure. It should be noted that this is a view that is intended for tool vendors to use when building tools or exporting data to the common format and not something the end-user would need to understand. Definitions, relations, and constraints of each element are detailed in the text of the RAAML specification, so they will not be reiterated here (OMG, 2022).

