



SAFETY-CRITICAL SYSTEMS RECOMMENDED PRACTICE

J3187™-1

SEP2023

Issued

2023-09

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

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 human machine interaction (HMI) evaluations.

This document takes the specific domain information 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.	HUMAN-MACHINE INTERACTION (HMI) AND SYSTEM THEORETIC PROCESS ANALYSIS (STPA).....	6
4.1	Introduction	6
4.2	Human Extension Representation (HER)	7
4.3	STPA Lessons Learned for Human-Machine Interaction Evaluation	9
4.3.1	Understanding Expected System Operation, Behaviors, and Capabilities.....	9
4.3.2	Establishing System Scope	11
4.3.3	Considering Driver Actions	12
4.3.4	HMI Unsafe/Undesired Control Action (UCA) Considerations.....	13
4.4	Example: Shifting Vehicle to Park.....	13
4.4.1	Deciding When to Put Vehicle in Park	14
4.4.2	Conscious Specific Action to Initiate a Park Request.....	15
4.4.3	Assess Results of Request and Respond Accordingly.....	15
4.5	Dealing with Abstraction.....	16
4.6	Consulting with Driver Performance and Behavioral Experts Regarding Causal Scenarios.....	17
4.7	UCAs and Causal Scenarios with HER	17
4.7.1	Feedback in Automotive HMI.....	20
4.7.2	Expansion with ADS.....	21

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 J3187-1_202309

For more information on this standard, visit
https://www.sae.org/standards/content/J3187-1_202309/

Documents

Document Sharing Hub

4.8	Useful Definitions	22
4.8.1	Erroneous Interaction.....	22
4.8.2	Incidental Interaction.....	22
4.8.3	Purposeful Activation	22
5.	NOTES	22
5.1	Revision Indicator.....	22
Figure 1	Driver as part of the control structure.....	7
Figure 2	Human extension of driver element in control structure	8
Figure 3	Detailed view of human extension representation	8
Figure 4	Engineering “V” diagram highlighting concept of operations	9
Figure 5	System diagram	10
Figure 6	High-level system model representation.....	11
Figure 7	System scope outlined by dashed line.....	12
Figure 8	Substituting “driver” with human extension representation.....	14
Figure 9	Mental models.....	14
Figure 10	Control action selection.....	15
Figure 11	Mental model updates.....	15
Figure 12	Abstraction methods to manage complexity	16
Figure 13	Human extension representation example questions and answers	18
Figure 14	More HER example questions and prompts	19

1. SCOPE

This document describes System Theoretic Process Analysis (STPA) approaches to evaluate human-machine interaction (HMI) found effective when conducting STPA human factors and/or a system safety evaluation.

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 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 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.

National ITS Architecture Team. (2007). *System engineering for intelligent transportation systems* (Report no. FHWA-HOP-07-069). U.S. Department of Transportation. Retrieved from <https://ops.fhwa.dot.gov/publications/seitsguide/seguide.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*. 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
APAS	Advanced passenger assistance 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
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
OMG	Object Management Group
RAAML	Risk analysis and assessment modeling language
SOTIF	Safety of the intended functionality
STPA	System theoretic process analysis
UCA	Unsafe/undesired control action

4. HUMAN-MACHINE INTERACTION (HMI) AND SYSTEM THEORETIC PROCESS ANALYSIS (STPA)

4.1 Introduction

This section describes STPA approaches to evaluate HMI found effective when conducting STPA human factors and/or a system safety evaluation.

Objective data aid in and are sometimes necessary for the accommodation of safety requirements into human-machine interaction systems. Engineering teams responsible for the functional aspects and the design studio aspects of the human-machine interaction systems face pressures from many different perspectives such as cost, aesthetics, timing, and safety content. As such, discussions that do not include objective data may tend to become discussions where only opinions, interpretations, and perspectives drive decisions. Objective data should be diverse and relevant. The decision is likely to include a tradeoff of the different perspectives mentioned above, so it is important to obtain objective data about all the aspects that are compared. Add to this the fact that groups making human-machine interaction design decisions may not possess the skillset and experience of human factors scientists or researchers.

The challenge is how to obtain data easily understood by typical functional and design team engineers that support associated safety requirements to be included in the functional and design specifications. One solution is to associate requirements with causal scenarios that could lead to unsafe control actions resulting in hazardous conditions/accidents.

STPA is useful when evaluating systems that contain expected driver and machine interactions as it enables the “driver” (or “vehicle occupant(s)”) to be incorporated in the control structure as a functional element. In this context, the driver has certain expected functions to perform that are evaluated as part of the guideword-driven unsafe control action assessment portion of STPA Step 1. Once this is done, the possible causal scenarios that could lead to these unsafe control actions are evaluated. The constraints and/or requirements necessary to prevent or manage these causes to an acceptable risk level are defined. The evaluation should focus on erroneous and incidental misuse interactions between the driver and system elements that could lead to potential safety hazards, including hazards associated with purposeful activation.

The driver now becomes part of the STPA control structure, as illustrated in [Figure 1](#).

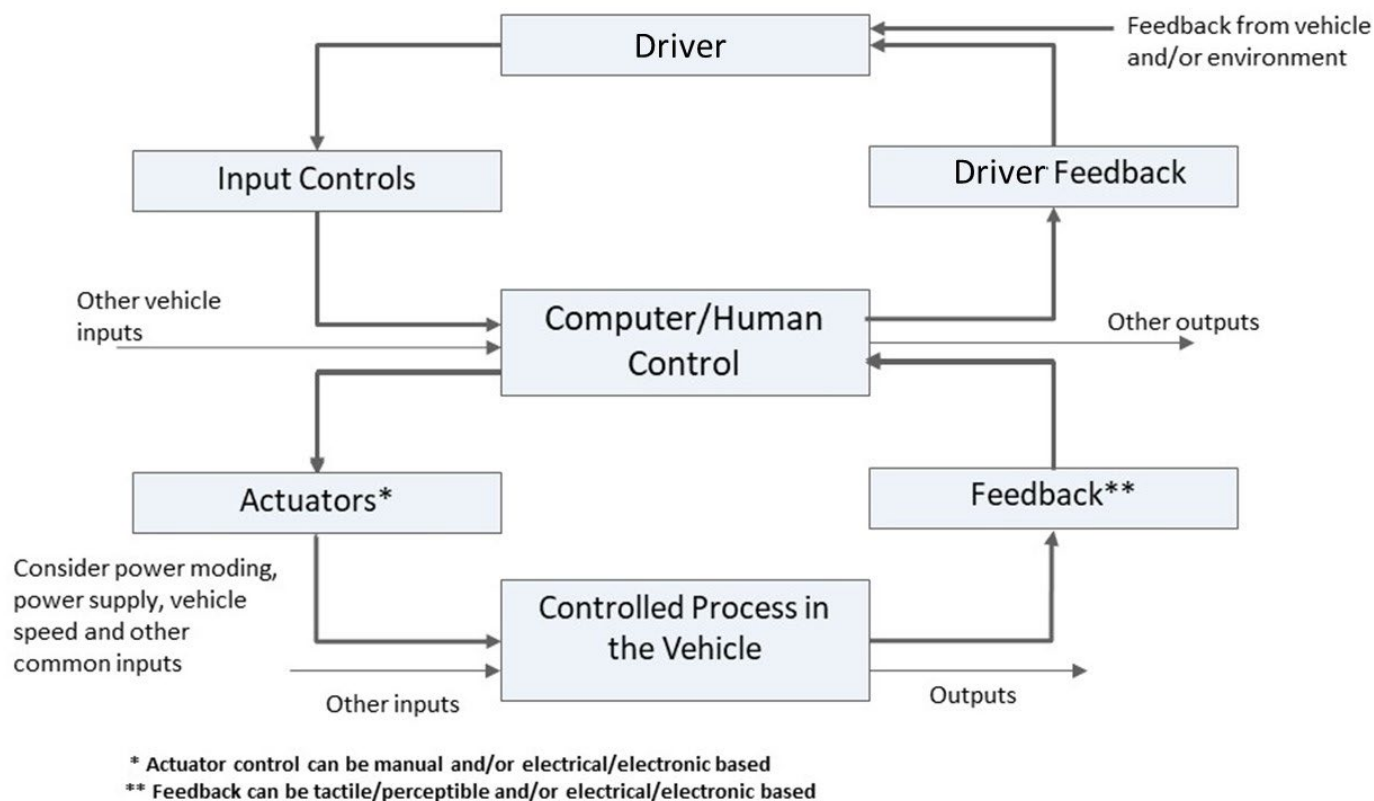


Figure 1 - Driver as part of the control structure

4.2 Human Extension Representation (HER)

The role of human operators is changing. Many tasks now involve supervisory control of automation or human-machine collaboration. Operators may be required to monitor more information with less direct interaction with the controlled process. As system complexity increases, so do risks for mode confusion and automation surprises. The operator's actions are driven by mental models of the controlled process and environment (France, 2017).

This had led to an enhancement to the STPA approach that helps to understand three important constructs. [Figure 2](#) shows the human extension representation (HER) (France, 2017) integrated into a generic representation of the control structure.