

Quality Control for Real-World STPA: Lessons from Auditing Government STPA Efforts

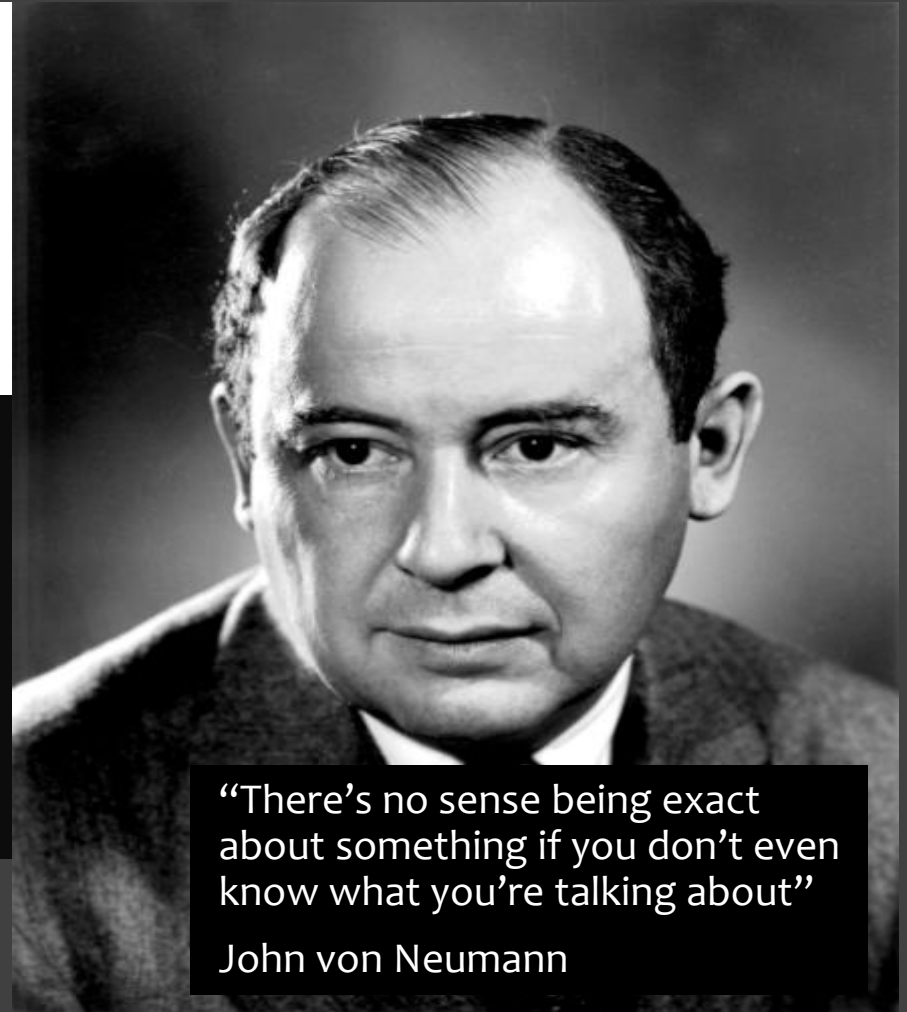
25 March 2026

Dr John Thomas

jthomas4@mit.edu

Dr William “Dollar” Young

William.Young@SCASDConsulting.com



“There’s no sense being exact about something if you don’t even know what you’re talking about”

John von Neumann

Agenda

- Bottom-Line Up Front
- SAE J3307 Origins
- SAE J3307 Application & Findings
- Beyond SAE J3307 – STPA project Oversight

What Difference Does the Standard Make to STPA Practitioners?

BOTTOM LINE UP FRONT (BLUF)

- Contracted to audit a government-funded STPA effort on a *highly consequential* information system that was not meeting sponsor desires and expectations despite very talented performer team
- Evaluating processes and artifacts against SAE J3307 **clearly** illuminated 3 primary contributing factors
 - Facilitation
 - Team STPA training shortfalls
 - Missing STPA Implementation Plan
- Standard helped answer key stakeholder questions on lack of progress that might have otherwise have been attributed to “STPA doesn’t work” (or blamed on humans)
- Audit provided evidence grounded on authoritative, contractually sufficient evidence to support a government decision point

Standard Helped Explain the Performance from A Systems Perspective (and Identify Promising Fixes)

SAE J3307 Origin

- J3307_202503: “STPA Standard for All Industries”
 - Released March 2025
- Why was J3307 developed?
 - STPA is now being required:
 - By government bodies
 - Within large organizations
 - Within supply chains
 - Standard defines what is needed to claim a “compliant” STPA
 - Contractual requirements can reference the Standard
- How was it developed?
 - Written by SAE’s “STPA Task Force” (industry practitioners)
 - Global participation: Automotive, Aviation, Defense, Software, Semiconductors, Regulators, etc.
 - Rigor: Same balloting process as any other SAE Standard

J3307 can be used to show STPA compliance

Audit (1/6): Background

- Government-funded, multi-yr effort to apply STPA to high-consequence information system
- Highly educated, experienced, and talented team of engineers as performers
- Project not producing expected outcomes
- Audit initiated by serendipity and a STPA-knowledgeable and influential internal “champion”

Audit Purpose: Support a Proceed / Pivot / Pause Decision

Audit (2/6): Structure

SAE J3307:2025

Downloaded from SAE International by William Young, Member, Sep 26, 2025

SAE INTERNATIONAL

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 J1187 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

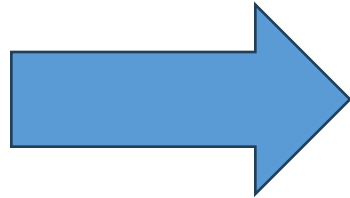
SAE Executive Standards Committee Rules provide that: This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement liability thereon, is the sole responsibility of the user. SAE reserves the right to update this report at any time it is revised, replaced, 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 any kind of data retrieval, or training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-486-7233 (inside USA and Canada)
Tel: +1 724-776-4810 (outside USA)
Fax: 724-776-5799
Email: CustomerService@sae.org
http://www.sae.org

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



Evaluation Worksheet

STPA-SEC Evaluation Worksheet — SAE J3307

Program / Product: _____ **Audit ID:** _____

System of Interest: _____ **Audit Date:** _____

Auditor: _____ **Version: Initial**

Points of Contact: _____ **Location / Business Unit** _____

How to use this worksheet

- Conformance scale: 0 = Not addressed, 1 = Partially addressed, 2 = Mostly addressed, 3 = Fully addressed.

ID	J3307 Area	Step/Sub-Step	Assessment Question	Expected Evidence	Conformance (0-3)	Notes/Findings	J3307 Reference
J3307-6.1-01	Management	STPA Management Support	Is STPA management policy documented and enforced across concept design through validation (and beyond)?	Documented STPA policy; defined ownership roles; program-level mandate for STPA			6.1
J3307-6.1-02	Management	STPA Management Support	Has management provided qualified personnel and sufficient resources to perform the STPA?	Evidence of trained/experienced STPA team members; resource allocations (budget, time) for STPA activities			6.1
J3307-6.1-03	Management	STPA Management Support	Is there a system in place for managing STPA documentation (storing and retrieving results) and handling STPA confidentiality?	Description of STPA document repository or database; confidentiality designation procedures for STPA reports			6.1
J3307-6.1-04	Management	STPA Management Support	Does management monitor STPA progress and participate in key STPA reviews (e.g., by tracking team status and attending STPA review meetings)?	Management review meeting minutes; attendance records of management in STPA reviews; examples of management feedback/questions on STPA results			6.1
J3307-6.2-01	Facilitators & Teams	STPA Evaluation Participants	Is an STPA Core Team established with cross-functional members covering all relevant	Core team roster listing members' domains; evidence of representation from key			6.2

1
©Security Concepts & Strategic Designs, LLC
Version 2.0

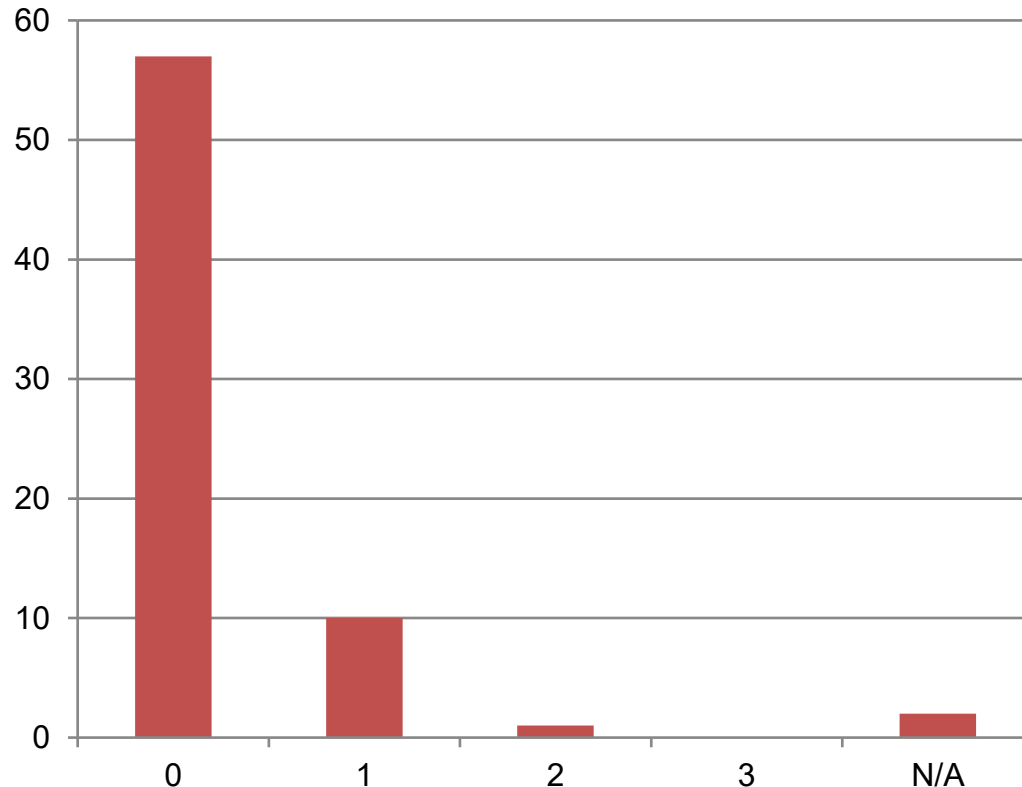
This standard defines the steps, tasks, and flow necessary to execute a System Theoretic Process Analysis (STPA) system safety evaluation and outlines the expected deliverables. It is applicable to all industries.

Audit (3/6):Conduct

Audit Approach	Audit Outcomes
Reviewed project strategy: STPA process and execution	Clear gaps identified
Reviewed STPA & related artifacts <ul style="list-style-type: none">• Control structures• Hazards & losses• UCAs & scenarios• Constraints & traceability	Root causes isolated
Conducted structured interviews <ul style="list-style-type: none">• Program office• Performer team• Adjacent teams	Actionable recovery recommendations Leadership & practitioner debriefs
Applied SAE J3307–based scored worksheet	Evidence-based decision support

Audit (4/6): Data Summary

Executive summary: score distribution



Key takeaway

Out of 70 items: 57 scored 0; 10 scored 1; 1 scored 2; 0 scored 3; 2 are N/A.

Important Alibis

- SAE J 3307 Standard not published until Mar 2025

Conformance scale: 0 = Not addressed, 1 = Partially addressed, 2 = Mostly addressed, 3 = Fully addressed.

Audit (5/6): Key Findings

- Poor initial results were driven by incorrect and incomplete STPA execution
- STPA terminology was used, but most required J3307 activities were not performed
- Several completed activities did not meet J3307 evidence expectations

Audit (6/6): Primary Contributing Factors

- No experienced STPA facilitator (scope, pacing, quality control)
- No formal STPA training for team members
- No STPA Implementation Plan (reviews, participation, and quality assurance)

Compare:

A Successful STPA Project

- 1) STPA Education (2-5 days)
- 2) First Project with STPA Facilitator
 - Invite team members from class to participate
 - Assign deliverables
 - Conduct periodic reviews
- 3) Deliverables
 - Effective presentations with key stakeholders
 - E.g., comparison results, value of each result, cost to fix later (if we didn't try STPA)
 - Results provided to key groups in organization
 - Long spreadsheets are not enough; highlight the most relevant findings and conclusions



**Part of STPA
Implementation
Plan**

Example: USAF followed these steps in about 1-2 weeks to apply STPA before flight test of AI-flown aircraft. See (Bowers & Thomas 2024).

How to Decrease Risk and Improve Outcomes

General advice:

- Consider STPA education
- Consider collaborating with an STPA Facilitator

For high-visibility or high-consequence projects:

- Require STPA Practitioner Certification
- Require STPA Implementation Plan
- Require formal sign-off from lead STPA Engineer



Questions

jthomas4@mit.edu

William.Young@SCASDConsulting.com



BACKUPS





STPA-SEC Evaluation Worksheet — SAE J3307

Program / Product:	Audit ID:
System of Interest:	Audit Date:
Auditor:	Version: Initial
Points of Contact:	Location / Business Unit

How to use this worksheet

- Conformance scale: 0 = Not addressed, 1 = Partially addressed, 2 = Mostly addressed, 3 = Fully addressed.

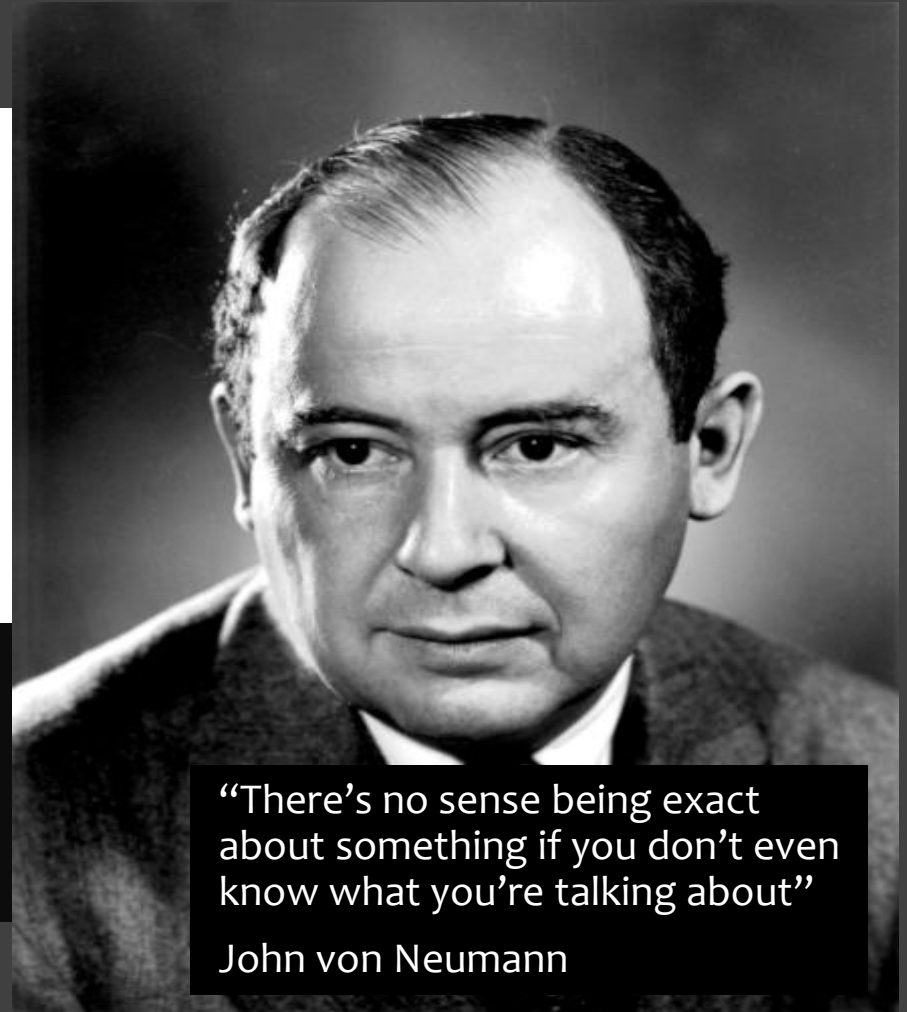
ID	J3307 Area	Step/Sub-Step	Assessment Question	Expected Evidence	Conformance (0-3)	Notes/Findings	J3307 Reference
J3307-6.1-01	Management	STPA Management Support	Is STPA management policy documented and enforced across concept design through validation (and beyond)?	Documented STPA policy; defined ownership roles; program-level mandate for STPA			6.1
J3307-6.1-02	Management	STPA Management Support	Has management provided qualified personnel and sufficient resources to perform the STPA?	Evidence of trained/experienced STPA team members; resource allocations (budget, time) for STPA activities			6.1
J3307-6.1-03	Management	STPA Management Support	Is there a system in place for managing STPA documentation (storing and retrieving results) and handling STPA confidentiality?	Description of STPA document repository or database; confidentiality designation procedures for STPA reports			6.1
J3307-6.1-04	Management	STPA Management Support	Does management monitor STPA progress and participate in key STPA reviews (e.g., by tracking team status and attending STPA review meetings)?	Management review meeting minutes; attendance records of management in STPA reviews; examples of management feedback/questions on STPA results			6.1
J3307-6.2-01	Facilitators & Teams	STPA Evaluation Participants	Is an STPA Core Team established with cross-functional members covering all relevant	Core team roster listing members' domains; evidence of representation from key			6.2

Quality Control for Real-World STPA: Lessons from Auditing a Government STPA Effort

25 March 2026

Dr John Thomas

Dr William “Dollar” Young



“There’s no sense being exact about something if you don’t even know what you’re talking about”

John von Neumann

About Us:

- **Creator of System-Theoretic Process Analysis for Security (STPA-Sec)**
- **31+ years Operational USAF experience**
 - Squadron, Group, Wing Commander
 - Electronic Warfare Officer in Fighters and Bombers
 - Weapon School Graduate and instructor
- **Intrapreneur, Innovator, Disruptioneer**
 - 350th Spectrum Warfare Wing -- Designer & first Commander
 - USAF Cyber College -- Designer and first Director
- **Trusted Advisor**
 - Multiple Silicon Valley Organizations
 - Lincoln Labs
 - National Security Agency
 - DoD Office of Net Assessment & Defense Science Board
 - DARPA Information Systems and Technology (ISAT) Study Group
 - RAND Center for AI Security & Trust



**Dr William "Dollar"
Young**

**My Passion is Delivering Value
and Helping Build a More Secure
World**

About Us:

- **Experience**
 - 26 years in engineering and operating complex systems
- **Industry background**
 - Defense
 - Aerospace
 - Automotive
 - Telecommunications
- **Areas of Expertise**
 - Co-Developer of System-Theoretic Process Analysis (STPA)
 - Introducing STAMP/STPA/CAST to organizations, facilitating STAMP-related projects, accident investigation and analysis
 - Teaching: Software Engineering, System Safety, System Engineering, System Architecture, Human Factors, Discrete Mathematics, Probability Theory, Control Theory
 - Research: Engineering errors and omissions, human error, new approaches to system engineering / system safety, requirements development, formal specifications, etc.
- **Industry Advisor**
 - Google
 - Meta
 - NASA
 - Ford
 - GM
 - EPRI
 - Lincoln Lab
 - US Air Force
 - US Army
 - US Navy
 - US Space Force
 - FAA
 - NRC
 - Sandia National Lab
 - Lawrence Livermore National Lab
 - Northrop Grumman



Dr. John Thomas
Aeronautics and Astronautics Dept.
MIT

Co-Director, Engineering Systems Lab
**Executive Director, Partnership for
Systems Approaches to Safety and
Security**