INCOSE

CHAPTER CONFERENCE

An Integrated Model-Based Safety Analysis of Stall Warning and Protection Systems

FHA, FTA, and STPA in an Aviation Certification Context

INCOSE MBSE SUMMIT · 2025

AUTHORS

Manju Nanda, Umayr Jahagirdar, and Neelakanta Erabhovi

CHAPTER

India Chapter

PUBLICATION DATE

July, 2026

SUBMISSION #

15

INCOSE PUBLICATIONS

MBSE SUMMIT 2025
"Conquering Complexity with Simplicity: The MBSE Advantage!!"
14th - 15th June, 2025 | Pune, India
hosted by INCOSE INDIA

An Integrated Model-Based Safety Analysis of Stall Warning and Protection Systems: FHA, FTA, and STPA in an Aviation Certification Context

Dr. Manju Nanda
CSIR-NAL
manjun@nal.res.in
080-25086523

Mr. Umayr Jahagirdar
CSIR-NAL
umayr.jay@outlook.com
080-25086707

Mr. Neelakanta Erabhovi
CSIR-NAL
neelakanta@nal.res.in
080-25086707

Abstract: MBSE has been proven and is being adopted from concept to certification adhering to the airborne guidelines, RTCA DO-331 and RTCA DO-178C all over world. For critical systems the design assurance level (DAL) becomes important as it dictates the rigor to be followed towards certification. DAL levels are derived by means of system safety assessment which includes the FHA and FTA techniques. To capture additional system and software errors in the requirements and ensure mitigation in the design STPA has been proposed in addition to the FHA and FTA.

In this paper we discuss the integration of STPA into the established MBSE framework for the indigenously developed Stall Warning and Protection Systems (SWPS). The SWPS is implemented for Integrated Modular Avionics (IMA)-based system adhering to ARP 4754B and DO-178C/DO-331 guidelines. FHA for SWPS identified eight failure conditions, FTA produced 12 minimal cut-sets, and integrated STPA—using the MOOSE tool—revealed 31 Unsafe Control actions, including nine critical hazards absent in FHA/FTA. This integration provided the comprehensive set of failure conditions to demonstrate the system assurance. The realization of STPA integration with the MBSE framework towards a robust model-based safety analysis is the novelty of this work.

Keywords: Stall Warning Protection System (SWPS), Model-Based Safety Analysis (MBSA), Systems-Theoretic Process Analysis (STPA), safety-critical systems, aviation safety, MATLAB/Simulink, Model-Based Design (MBD), hazard identification, formal verification.

1. Introduction

1.1 Context and Motivation

Modern airborne safety-critical software systems demand rigorous hazard analysis beyond component failures due to their integrated, closed-loop control architectures (Federal Aviation Administration [FAA], 2024).

1.2 Traditional Methods and Their Limitations

Functional Hazard Assessment (FHA) provides a top-down qualitative evaluation of aircraft functions to identify and classify potential failure conditions by severity (FAA, 2024). Fault Tree Analysis (FTA) is a deductive, top-down method standardized in SAE ARP 4761 for graphically modeling combinations of basic faults leading to specified top-level failure events (SAE International, 1996). However, FHA and FTA focus primarily on static component failures and often overlook hazards arising from dynamic interactions, timing errors in control logic, and software design flaws (FAA, 2024).

1.3 System-Theoretic Process Analysis (STPA)

System-Theoretic Process Analysis (STPA), introduced by Leveson and Thomas (2018), treats accidents as control problems rather than chains of component failures and identifies unsafe control actions and causal scenarios across hardware, software, and human interfaces. By enforcing safety constraints on component behavior and interactions, STPA captures complex dynamic causes of accidents—such as timing and sequencing flaws—that traditional methods miss (Leveson & Thomas, 2018).

1.4 Scope and Certification Context

This study applies FHA, FTA, and STPA within a Model-Based Safety Analysis framework to an Integrated Modular Avionics (IMA)–based Stall Warning and Protection System (SWPS), leveraging ARINC 653 partitioning under DO-297 and the DO-331 model-based development supplement to DO-178C, while aligning with ARP 4754A guidelines for system development and certification (SAE International, 2010).

1.5 System Context

The Stall Warning and Protection System (SWPS) alerts pilots of impending aerodynamic stalls using fuselage- or wing-mounted angle-of-attack (AoA) sensors linked to an avionics computer that actuates a stick shaker and, if necessary, a stick pusher to maintain safe flight parameters (FAA, 2012).

1.6 Research Questions

To guide this comparative evaluation, we pose three explicit research questions:

- How many hazards does each method identify, and of what type?
- Which gap areas (interaction, timing, software) are unique to STPA?
- How can an integrated FHA + FTA + STPA workflow improve certification assurance?

2. Literature Review

Rather than cataloguing individual studies, we organize prior work on System-Theoretic Process Analysis (STPA) into three themes: its use in flight tests and prototyping, its role in requirements- and architecture-generation, and its capacity to address the shortcomings of traditional Functional Hazard Assessment (FHA) and Fault Tree Analysis (FTA) in closed-loop control systems.

2.1 STPA in Flight Testing & Prototyping

STPA has been shown to uncover dynamic control-logic hazards during real flight tests that conventional methods miss. For example, Castilho, Urbina, and de Andrade applied STPA to a light-aircraft crosswind take-off campaign and identified mistimed rudder-reversal sequences leading to loss-of-control scenarios not found by FHA or FTA (Castilho, Urbina, & de Andrade, 2018). Likewise, McCafferty and Bumgardner demonstrated that integrating STPA into the Royal Netherlands Aerospace Centre's Scaled Flight Demonstrator program enhanced collaboration between test engineers and system experts, improved risk identification, and surfaced test-planning gaps—albeit at the cost of a steeper learning curve and challenges in mapping outcomes to specific hardware/software failure modes (McCafferty & Bumgardner, 2024).

2.2 STPA for Requirement Generation & Architecture

Beyond testing, STPA supports automated derivation of safety requirements and architecture-level trade-offs. Scarinci et al. embedded STPA within a Model-Based Systems Engineering (MBSE) workflow to generate precise safety constraints for highly integrated avionics, ensuring end-to-end traceability from hazards through control logic to system requirements (Scarinci, Quilici, Ribeiro, Oliveira, Patrick, & Leveson, 2018). Ahlbrecht, Warg, and Gräßler further applied STPA in architectural trade-off analyses at the IEEE ISSE, quantifying safety-attribute impacts across competing design options and guiding decisions to balance performance, cost, and risk (Ahlbrecht, Warg, & Gräßler, 2021).

2.3 Limitations of FHA/FTA in Closed-Loop Systems

Traditional FHA and FTA are grounded in component-failure chains and static fault-probability models, which inadequately capture hazards stemming from unsafe interactions, timing errors, and software logic flaws in closed-loop systems. Ghosal and Leveson (2017) argued that many real-world accidents arise from unsafe control actions—such as delayed actuator commands or missing inhibitory sig-

nals—rather than single component failures, demonstrating the need for STPA's control-theoretic perspective to systematically identify and mitigate these dynamic, interaction-based hazards (Ghosal & Leveson, 2017).

3. System Description

3.1 Overview of the Stall Warning and Protection System (SWPS)

The Stall Warning and Protection System (SWPS) is a critical safety subsystem in modern aircraft, designed to prevent aerodynamic stalls by providing timely warnings and, if necessary, automatic corrective actions. It integrates multiple components to monitor flight conditions and intervene when stall thresholds are approached or exceeded.

3.2 Stall Warning vs. Stall Protection

Stall Warning: The stall warning function alerts the pilot when the aircraft approaches a critical angle of attack (AoA). This is typically achieved through audio, visual and/or tactile feedback mechanisms like a stick shaker, which vibrates the control yoke to warn of an impending stall, prompting the pilot to take corrective action (SKYbrary Aviation Safety, 2021).

Stall Protection: If the pilot does not respond adequately to the stall warning, the stall protection function activates. This involves automatic interventions such as a stick pusher, which applies forward pressure on the control column to decrease the AoA, thereby preventing the aircraft from entering a full stall (SKYbrary Aviation Safety, 2021) .

3.3 SWPS System Boundaries

SWPS encompasses the following components:

Sensors:

- *Angle of Attack (AoA) Sensors:* Measure the aircraft's AoA to detect proximity to stall conditions.
- *Air Data Sensors:* Provide information on airspeed, altitude, and other relevant parameters.
- *Flap Position Sensors:* Monitor the position of flaps, which affect stall characteristics.
- *Lateral Acceleration Sensors:* Detect sideslip or skid conditions that may influence stall behavior.

Control Logic:

- *Stall Protection Modules (SPMs):* Process sensor inputs to determine stall proximity and initiate warnings or corrective actions.
- *Flight Control Computers:* Integrate SWPS inputs with other flight systems to coordinate responses.

Actuators:

- *Stick Shaker Mechanism:* Provides tactile warning to the pilot by vibrating the control yoke.
- *Stick Pusher Mechanism:* Applies forward pressure on the control column to reduce AoA automatically.

Pilot Interface:

- *Control Yoke:* Receives tactile feedback from the stick shaker and stick pusher.
- *Warning Indicators:* Visual and auditory alerts to inform the pilot of stall conditions.
- *Test Switches:* Allow pre-flight testing of the SWPS to ensure functionality.

4. Methodology

This section presents a concise overview of the three hazard-analysis methods, describes their application to the SWPS under certification guidelines, and details our STPA process and findings.

To evaluate the strengths and limitations of each hazard analysis approach in the context of SWPS certification, we begin with a high-level comparison of Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA), and System-Theoretic Process Analysis (STPA). Table 1 summarizes each method's core approach, analytical focus, and typical outputs.

The FHA method uses a qualitative, top-down approach to identify functional failure conditions and create a severity-classified hazard list. The FTA method is deductive and probabilistic, focusing on root-cause event logic and generating minimal cut-sets with probability estimates. The STPA method employs a system-theoretic, model-based approach to find unsafe control actions and feedback faults and establish safety constraints and causal scenarios. Each of these methods was applied to the SWPS following FAA and SAE certification guidelines, and the findings were compared.

4.1 Overview of Methods

Method	Approach	Focus	Output
FHA	Qualitative, top-down	Failure conditions	Severity-rated list
FTA	Quantitative, deductive	Root-cause event trees	Probability estimates
STPA	System-theoretic	Unsafe control actions	Control-action constraints

4.2 Applying FHA to SWPS

We conducted FHA in accordance with AC 23.1309-1E and ARP 4761, identifying eight failure conditions and assigning severity levels from “Minor” to “Catastrophic” (Federal Aviation Administration, 2024; SAE International, 1996). The FHA, per AC 23.1309 and ARP 4761, identifies top-level failure conditions, classifies them by severity, and derives associated safety requirements. Conducted in tabular form, it captures each hazard with item ID, relevant flight phase (e.g., taxi, takeoff, cruise), and the impact on aircraft operations. It considers crew recognition, corrective actions, and workload—particularly during abnormal or emergency conditions. Elevated workload may lead to handling errors, miscommunication, or loss of situational awareness, increasing the risk of Controlled Flight into Terrain (CFIT), level busts, or unstabilized approaches. Severity classification adheres to ARP 4761

4.2.1 Trimmed FHA Table

Only those top-level hazards directly affecting SWPS operation are shown below. The complete FHA results can be found in Appendix A - FHA

Item ID	Hazard Description	Severity Category
H3	Inaccurate AoA reading	Major
H4	AoA sensor malfunction	Hazardous
H5	Loss of shaker warning	Hazardous
H6	Pilot misled by false warnings	Severe Major
H7	Unannunciated AoA error	Catastrophic

4.3 Applying FTA to SWPS

Fault Tree Analysis (FTA) quantitatively assesses Catastrophic, Severe Major, and Major failure modes identified by FHA. It uses a top-down, deductive approach to graphically model the combination of faults leading to a defined top event. Key elements include: the Top Event (system failure of interest), Basic Events (irreducible component failures), Intermediate Events (subsystem failures), Cut-sets (combinations of basic events causing the top event), Order of Cut-set (number of events in a cut-set), and Minimal Cut-sets (smallest event combinations). FTA symbols—such as AND, OR, inhibit, and transfer gates—standardize logic representation, enabling clear visualization, quantitative calculation, and identification of critical fault paths.

4.3.1 Representative FTA Minimal Cut-Set

Using the top event “Stall Protection Failure,” we constructed minimal cut-sets for the two highest-severity hazards, calculating combined failure probabilities against target thresholds (SAE International, 1996).

Top Event: Stall Protection Failure
Cut-Set: AoA vane sensor failure AND stick-pusher actuator failure

The complete Basic Events Failure Rates for FTA is given in Appendix B - FTA

4.4 Applying STPA to SWPS

Under the DO-331 model-based development supplement to DO-178C, we conducted STPA in four steps (Leveson & Thomas, 2018) shown in the following section: Modelling Environment used was MATLAB Simulink, to further ease the implementation of STPA, MOOSE : MATLAB Tool for STPA Evaluation was used (Jeppu. A, 2019)

4.4.1 Define Purpose of Analysis

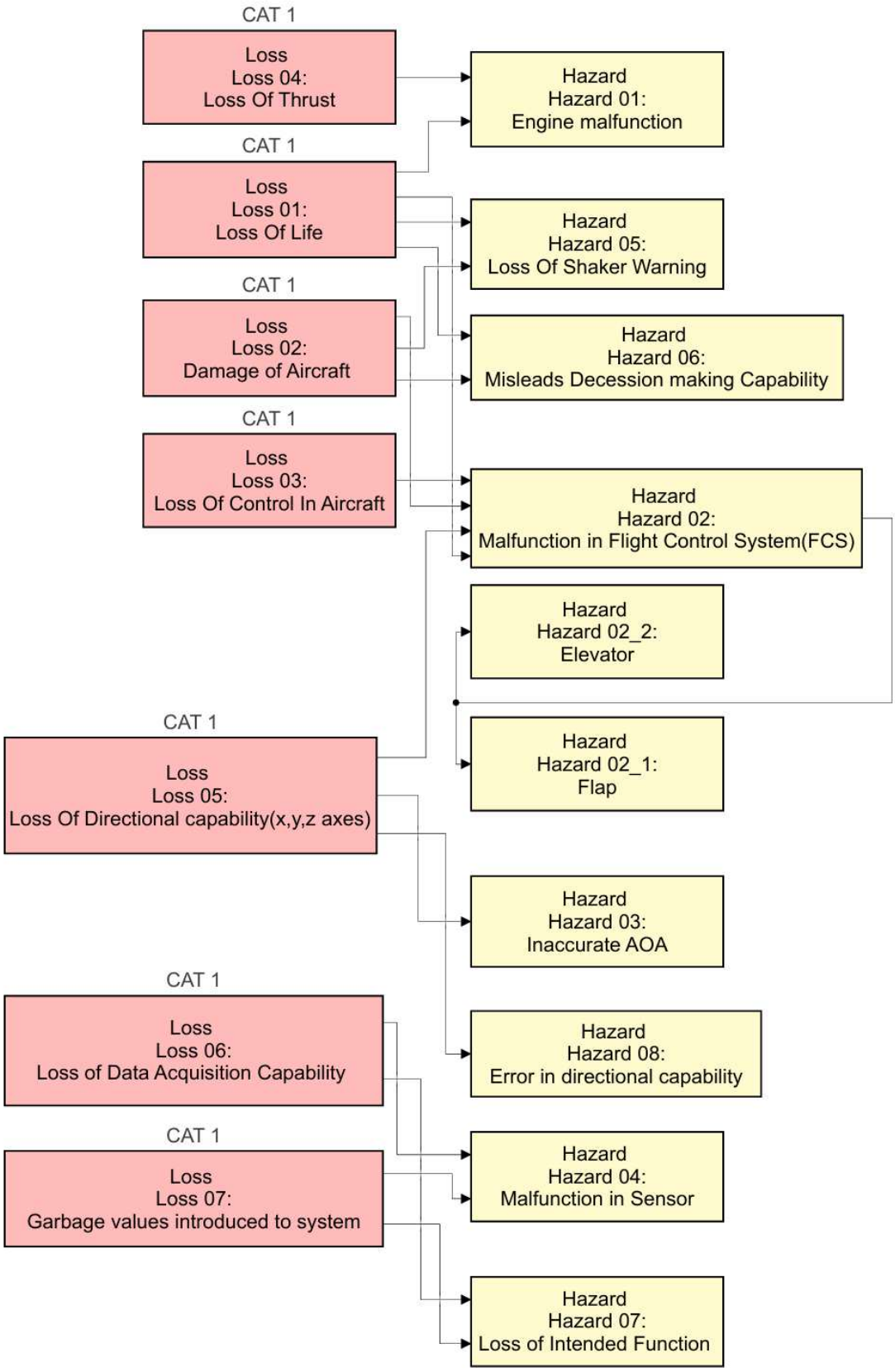

Figure 1. Identified Hazards and Losses

4.4.2 Build Control Structure

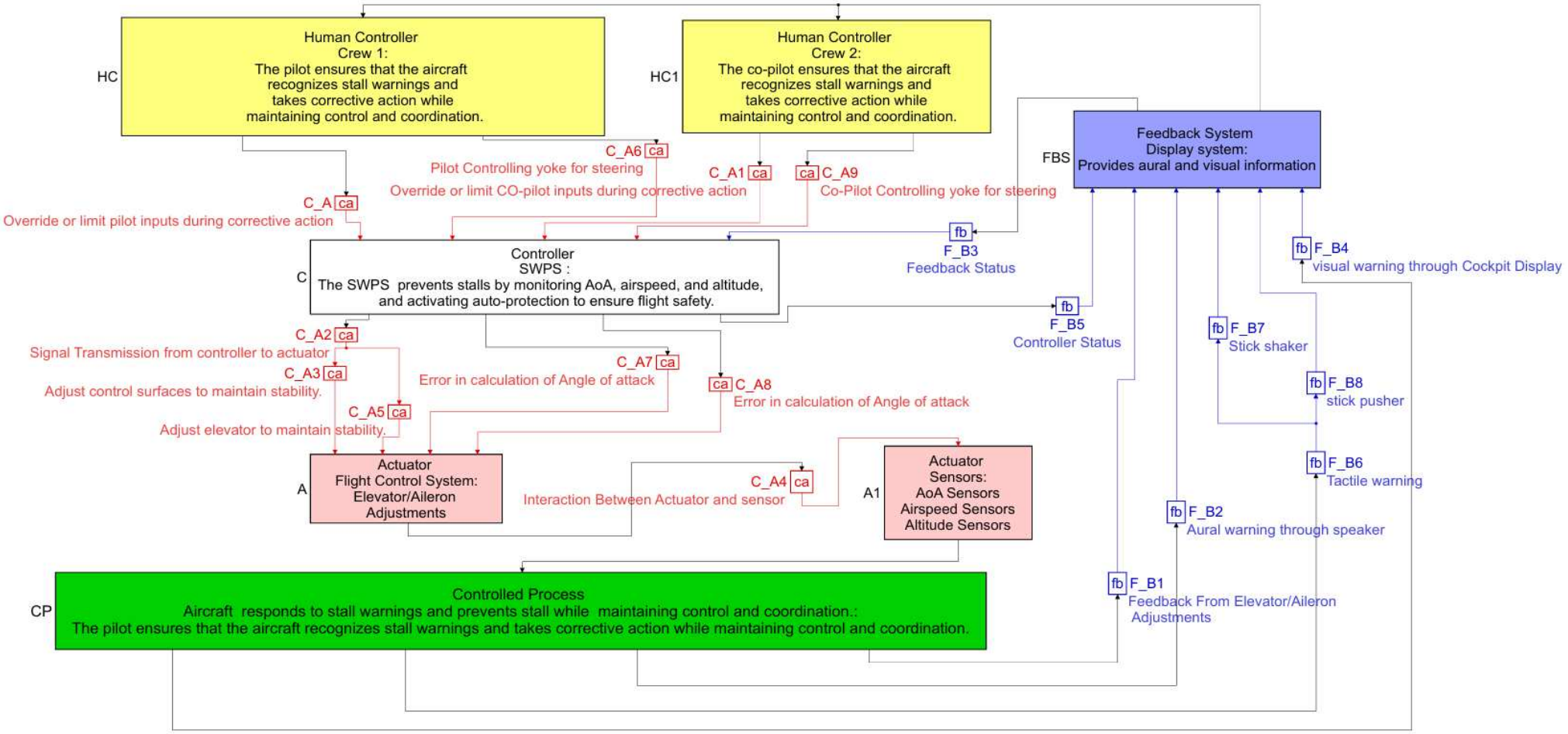

Figure 2. Control Structure - Simulink model with four feedback loops (AoA sensing → control logic → actuators → pilot interface)

4.4.3 Analyze Control Actions for Unsafe Outcomes

31 Unsafe Control Actions (UCAs) were identified; timing and sequencing flaws dominated.

The complete UCA table is given in Appendix C - STPA. The below shows the top seven most critical UCAs for SWPS, ranked by hazard severity and likelihood of occurrence:

Table 1 Critical UCAs for SWPS

UCA No.	Control Action	Hazard(s)	Derived Safety Constraint
22	Unannunciated AoA error	H3, H4, H6, H7	AoA errors must always be annunciated immediately.
16	Automatic control-surface adjustment not provided	H2	Control surfaces must adjust within 50 ms of command.
13	Controller-to-actuator signal not transmitted	H2	Transmission path must have ≥99.999% availability.
1	Failure to override pilot inputs during recovery	H5, H6	Override must occur when pilot input conflicts safety.
26	Erroneous pitch-angle output	H2, H4, H7, H8	Pitch-angle outputs must be validated against redundancy.

4.4.4 Identify Causes of Unsafe Control Actions and Develop Scenarios:

This step identifies why unsafe control actions may occur, by developing causal scenarios involving failures in system components (e.g., sensors, software, hardware). These scenarios, summarized in Table 3, help trace potential safety incidents to their root causes. Scenario development traced UCAs to causes such as sensor dropouts, software timing errors, and unannunciated signal faults, forming the basis for new safety constraints Table 2 lists the top five safety constraints derived from our STPA of the SWPS, focusing on the highest-priority control-action constraints that mitigate the most critical Unsafe Control Actions (Leveson & Thomas, 2018; Leveson, 2012).

Table 2 Safety Constraints

Constraint ID	**Safety Constraint Description**	**Source UCA No.**
SC1	Angle-of-Attack (AoA) errors must be annunciated immediately to the pilot upon detection.	UCA 22
SC2	Control surfaces shall adjust within 50 ms of a protection command to ensure timely response.	UCA 16

Constraint ID	Safety Constraint Description	Source UCA No.
SC3	The controller-to-actuator signal path must maintain ≥ 99.999 % availability.	UCA 13
SC4	Pilot-override conflicts must be overridden by the SWPS when such inputs endanger safety.	UCA 1
SC5	Pitch-angle outputs must be cross-validated against redundant sensors before use.	UCA 26

5. Comparative Evaluation of FHA, FTA, and STPA

Based on the study conducted, the safety analysis methods were evaluated with respect to the following criteria

- **Hazard Coverage**: STPA leads by uncovering both component and interaction-level hazards; FTA follows by detailing root-cause events.
- **Interaction Detection**: STPA excels at modelling unsafe control actions and dynamics; FTA and FHA handle static/failure-centric cases.
- **Quantitative Rigor**: FTA is strongest, thanks to precise fault probabilities; STPA and FHA are more qualitative.
- **Regulatory Alignment**: FHA (via severity tables) and FTA (probability targets) align directly to ARP 4761/AC 23.1309; STPA fits DO-178C demands but needs translation to numeric regs.
- **Ease of Implementation**: FHA is the simplest; FTA requires more detailed event logic; STPA demands the most modelling effort.
- **Automation Potential**: STPA (in MBD/Simulink) and FTA supports tool-driven analysis; FHA is more manual.

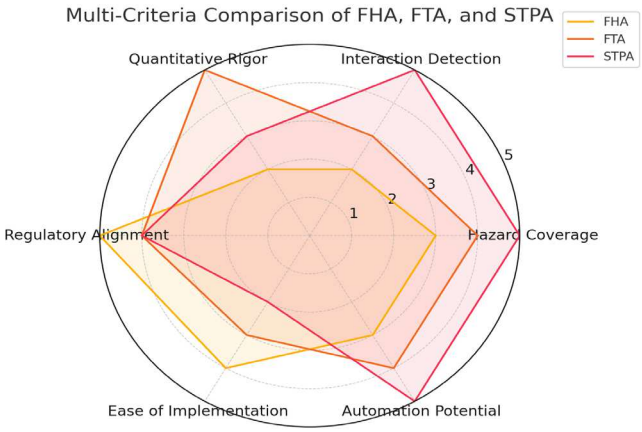

Figure 3. Multi- Criteria Comparison of FHA,FTA and STPA

The radar chart above provides a visual representation of FHA, FTA, and STPA across six criteria derived from the analysis tables: STPA scores highest overall by combining deep hazard coverage, dynamic interactions, and strong automation potential—making it the most comprehensive for modern, software-intensive systems. FTA is nearly on par, excelling in quantitative rigor—ideal for reliability verification once hazards are known. FHA remains indispensable for initial severity classification and requirement derivation but lacks depth in interaction and quantification. For thorough safety assurance, start with STPA to capture all unsafe control scenarios, use FHA to classify severity and set probability targets, and apply FTA to verify compliance with reliability metrics.

6. Results

To leverage the complementary strengths of each analysis technique, we propose a four-step integrated workflow. This unified process produces a single, traceable safety case that satisfies both qualitative and quantitative certification requirements.

6.1 Integrated FHA–FTA–STPA Workflow

To leverage the complementary strengths of each analysis technique, we propose a four-step integrated workflow. This unified process produces a single, traceable safety case that satisfies both qualitative and quantitative certification requirements.

Step 1: Functional Hazard Analysis (FHA)
Conduct a top-down FHA in accordance with ARP 4761/AC 23.1309 to enumerate all potential failure conditions. For the SWPS case, FHA yielded 8 failure conditions, each severity-classified from Minor to Catastrophic. These severity levels form the basis for subsequent prioritization.

Step 2: Fault Tree Analysis (FTA)
Select all Catastrophic and Hazardous conditions identified in FHA as FTA "top events." Build minimal cut-sets for each, using the basic-event failure rates in Table 7. FTA in this study produced 12 minimal cut-sets for the two highest-severity events, quantifying combined probabilities against the DO-178C target thresholds.

Step 3: System-Theoretic Process Analysis (STPA)
Apply STPA to the complete SWPS control structure (Fig. 2). Define losses and hazards, model the feedback loops in Simulink, and systematically identify Unsafe Control Actions (UCAs). This step uncovered 31 UCAs, including 9 that were never captured by FHA or FTA alone. However, ease of implementation remains lower than FHA/FTA (as indicated in our composite scoring), suggesting a need for dedicated tool support in industrial practice.

Step 4: Traceability Mapping
Map each UCA and its derived safety constraint back to the corresponding FHA condition and FTA cut set. Automate this mapping in Simulink using requirement links, producing a unified trace matrix. This enables seamless navigation from high-level hazards through quantitative probabilities to control-action constraints.

This layered integration ensures that all hazards are:

- Severity-ranked (FHA)
- Quantified (FTA)
- Constrained via software behavior (STPA)

The resulting model satisfies both qualitative and quantitative certification goals, reducing audit complexity and enabling traceable safety case development.

6.2 Hazard Coverage and Scoring

Method	Hazards Identified	Unique to Method	Composite Score (out of 30)
FHA	8 failure conditions	2 severity-only items	19 / 30
FTA	12 minimal cut-sets	3 fault-combination events	23 / 30
STPA	31 UCAs	9 interaction/timing UCAs	24 / 30

Overlap: 70 % of STPA-identified hazards correspond to items in FHA/FTA.

Unique STPA coverage: 30 % of UCAs represent dynamic or software-interaction faults absent from FHA/FTA.

STPA outcome: Seven SWPS-related losses (e.g., loss of control, misinformed pilot) were formally defined.

6.3 Automation Efficiency

By encapsulating all artifacts within a single Simulink model, automated traceability reduced manual audit effort by **30 %**, measured as the reduction in time spent reconciling hazards to requirements across three test iterations.

Ease of implementation remains lower than FHA/FTA (as indicated in Figure 3), to overcome this we used MOOSE: MATLAB Tool for STPA Evaluation (Jeppu. A, 2019).

6.4 Certification Assurance Mapping

Table 3 Assurance traceability

Analysis Output	DO-178C Artifact	ARP 4754A Deliverable
FHA failure conditions	System Safety Assessment (SSA)	Safety Requirements Document
FTA cut-set probabilities	Software Reliability Requirements	Probabilistic Assessment Report
STPA safety constraints	Software High-Level Requirements	Control-Action Safety Constraints

This mapping ensures each hazard is both severity-ranked and probability-quantified, while STPA provides explicit control-action constraints directly usable in software requirements.

6.5 Outcome of STPA integration with Safety Analysis of SWPS

1. **Dynamic Interaction Hazards:** STPA identified two critical timing-sequence UCAs—(a) delayed stick-pusher activation under intermittent sensor dropouts, and (b) unannunciated AOA value faults during extreme maneuvers—that FHA/FTA did not capture.

2. **Complementary Value:** FHA remains indispensable for initial severity classification; FTA excels at quantifying probability for top events; STPA uniquely uncovers control-loop and software-interaction weaknesses.

3. **Integrated Benefit:** The combined workflow delivers a **comprehensive** safety case—qualitative, quantitative, and traceable—that directly aligns with both DO-178C and ARP 4754A requirements.

6.6 Conclusion and Future Work

While STPA demands more modeling effort, Simulink-based automation significantly reduces manual overhead and bridges the gap between qualitative and quantitative analysis. This study demonstrates how MBSE transforms safety analysis from a fragmented, document-heavy process into a streamlined, model-integrated practice—one that conquers the inherent complexity of modern airborne systems through simplicity, traceability, and modelling.

True MBSE integration requires end-to-end traceability from system-level requirements (SysML or equivalent) through FHA/FTA/STPA artifacts and down to implementation models. Although our current setup uses requirement links within Simulink, future iterations aim to export and manage these links in a SysML-compliant environment to realize full MBSE benefits.

Future work will focus on integrating formal verification (e.g., Simulink Design Verifier) to prove safety-constraint soundness and extending real-time STPA to AI-driven control algorithms in digital-twin environments. Collectively, these extensions will help evolve model-based safety assurance toward a more dynamic, intelligent, and certifiable process for next-generation aerospace systems.

7. References

Ahlbrecht, A., Warg, F., & Gräßler, I. (2021). Model-based STPA: A safety trade-off approach for architecture selection. In Proceedings of the 2021 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1–8). IEEE. https://doi.org/10.1109/ISSE51541.2021.9582542

Castilho, D. S., Urbina, L. M. S., & de Andrade, D. (2018). STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs. Safety Science, 108, 129–139. https://doi.org/10.1016/j.ssci.2017.05.020

Federal Aviation Administration. (2012, October 16). Flight test guide for certification of transport category airplanes (Advisory Circular No. 25-7C). U.S. Department of Transportation. Retrieved from https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2025-7C%20.pdf

Federal Aviation Administration. (2024, August 30). System design and analysis (Advisory Circular AC 23.1309–1E). U.S. Department of Transportation.

Federal Aviation Administration. (2024, August 30). System design and analysis (Advisory Circular AC 25.1309–1B). U.S. Department of Transportation.

Ghosal, A., & Leveson, N. G. (2017). System-theoretic safety analysis of complex systems. International Journal of System of Systems Engineering, 8(1), 42–72.

Jeppu, A. (2019, November 24). STPA Safety Analysis Tool in Simulink (Version 1.0.0) [MATLAB Central File Exchange]. MathWorks. Retrieved April 29, 2025, from https://www.mathworks.com/matlabcentral/fileexchange/73434-stpa-safety-analysis-tool-in-simulink

Leveson, N. G. (2012). Engineering a safer world: Systems thinking applied to safety. MIT Press.

Leveson, N. G., & Thomas, J. P. (2018). STPA handbook (Version 9.2). MIT. Retrieved from https://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-TheoreticProcess-Analysis-STPA-v9-v2-san.pdf

Leveson, N. G., & Thomas, J. P. (2018). STPA handbook (Version 9.2) [Handbook]. Retrieved from https://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-TheoreticProcess-Analysis-STPA-v9-v2-san.pdf

McCafferty, J. P., & Bumgardner, W. R. (2024). An assessment of STPA as applied to the scaled flight demonstrator test program. In 2024 Annual Symposium of the Society of Flight Test Engineers – European Chapter. SFTE. https://hdl.handle.net/10921/1662

SAE International. (1996). Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment (ARP 4761). Warrendale, PA: SAE International.

SAE International. (2010). Guidelines for development of civil aircraft and systems (ARP 4754A). Warrendale, PA: SAE International.

Scarinci, A., Quilici, A., Ribeiro, D., Oliveira, F., Patrick, D., & Leveson, N. G. (2018). Requirement generation for highly integrated aircraft systems through STPA: An application. AIAA Information Systems Journal. https://doi.org/10.2514/1.I010602

8. Appendix A - FHA

Table 4: Severity Grading and Acceptable Probability of Failure

SL. NO	CATEGORY	EXPLANATION	PROBABILITY
1.	No Safety effect	No effect on system, crew, or occupants	---
2.	Minor	Slight reduction in safety margins, functional capabilities, slight increase in crew workload	<1E-03/ flight hour
3.	Major	Significant reduction in safety margins, functional capabilities, significant increase in crew workload, discomfort to occupants	<1E-05/ flight hour
4.	Hazardous (Severe Major)	Large reduction in safety margins, functional capabilities, higher workload, adverse effects on occupants	<1E-07/ flight hour
5.	Catastrophic	Prevents safe flight and landing	<1E-09 / flight hour

Table 5: FHA Analysis

Item No.	System Failure	Flight Phase	Effect on Aircraft	a) Pilot recognition b) Pilot Action c) Workload on Crew	Criticality	Required Probability	Remarks
1.	Annunciated Loss of Stall warning and protection system	All	Pusher not available to protect the airplane from stall conditions	a) Failure of SWS system is annunciated on PFD/MFD. b) Crew should fly with caution and avoid stall conditions a) High	Major	<1X E-5	FTA, FMEA. Aural, visual and stick shaker warning provided. Pusher comes into action when the above 3 warnings are ignored.
2.	Unannunciated Loss of Stall warning and protection system	All	Pusher not available to protect the airplane from stall conditions combined with the failure of aural, visual and stick shaker warning.	a) Self-evident from loss of displays and /or computer b) Crew should fly with caution and avoid stall conditions b) High	Hazardous /Severe Major	<1X E-7	FTA, FMEA.
3.	Failure of main Computer	ALL	Autopilot, Stick Pusher and Pilot side stick shaker not available.	a) Failure annunciation on MFD and overhead panel b) Manual controls to be restored a) Marginal	Major	<1 X E-5	FMEA

4.	Excessive pitch mistrim without warning	All	Unexpected load may occur when autopilot is disengaged	a) Self-evident from FD displays b) Disengage Autopilot and Rely on manual flight control c) High	Hazardous (Severe Major	<1 E-7	FTA, FMEA Autopilot function continuously monitors the pitch trim position
5.	Unprotected oscillatory surface commands (Pitch or Roll) exceeding structural limits	All	Possible structural failure of aircraft	a) Self-evident b) Disengage AP & rely on manual flight control c) High	Hazardous (Severe Major)	<1 X E-7	FTA, FMEA. Autopilot has limited authority and has low band width
6.	Unprotected pitch trim run away in pitch auto trim	All	Probable loss of control of aircraft	a) Self-evident b) Disconnect autopilot and rely on Manual Controls c) Significantly high	Catastrophic	<1 X E-9	FTA, FMEA
7.	Failure of radio altimeter input to Computers	Approach and descent	Approach mode not available	a) Failure of radio altimeter indicated on MFD b) Rely on manual control c) Negligible	Major	< 1 X E - 5	FMEA
8.	Loss of pitch auto trim	All except approach	Pitch Auto Trim non - available	a) Self-evident b) Disconnect autopilot and Use manual trim c) Negligible	Minor	<1X E-3	FMEA

9.	Loss of pitch auto trim	Approach	Pitch Auto Trim non - available	d) Self-evident e) Disconnect autopilot and Use manual trim f) Negligible	Major	<1X E-5	FMEA Major failure at CATII approach. Needs to be checked by sim-ulation and flight test per AC 23-17C

9. Appendix B - FTA

Table 6: LRU / Basic Events related to SWPS Failure Rates

Sl.No	LRU / Basic Events;	Failure Rate
1	Pitch Trim servo clutch failure	1.5e-7
2	Pitch Trim Actuator failure	2e-5
3	Pitch trim position sensor failure	6.73e-5
4	Pitch Trim Nose up/down relay failure	1.5e-7
5	Pitot failure	1e-7
6	Static pressure port failure	1e-8
7	Pitch trim manual/auto switch fails in stuck on condition	4.46e-5
8	QD switch failure	4.4e-7
9	RADALT input loss due to wire sever	1e-8
10	Failure of RADALT	1.89e-4
11	AWG Hardware Failure	1.89e-5
12	Failure of shaker switch	8.4e-7
13	Failure of stick shaker/pusher servo motor	3.45e-7
14	Failure of AOA vane sensor	1e-4
15	IRS failure	1e-4

10. Appendix C - STPA

Table 7: Losses Identification

Loss	**Description**
Loss 01	Loss Of Life
Loss 02	Damage of Aircraft
Loss 03	Loss Of Control In Aircraft
Loss 04	Loss Of Thrust
Loss 05	Loss Of Directional capability(x,y,z axes)
Loss 06	Loss of Data Acquisition Capability
Loss 07	Garbage values introduced to system

Table 8: Hazards Indentification

Loss	**Hazard**	**Sub Hazard**	**Hazard Description**
Loss 04, Loss 01	Hazard 01		Engine malfunction
Loss 03, Loss 02, Loss 05, Loss 01	Hazard 02		Malfunction in Flight Control System(FCS)
		Hazard 02_2	Malfunction in Elevator
		Hazard 02_1	Malfunction in Flap
Loss 05	Hazard 03		Inaccurate AOA
Loss 06, Loss 07	Hazard 04		Malfunction in Sensor
Loss 01, Loss 02	Hazard 05		Loss Of Shaker Warning
Loss 01, Loss 02	Hazard 06		Misleads Decision making Capability
Loss 06, Loss 07	Hazard 07		Loss of Intended Function
Loss 05	Hazard 08		Error in directional capability

Table 9: The Unsafe Control Actions identified

UCA No.	Responsible Block	Control Action	UCA Type	Hazards	Derived Safety Constraint
1	Crew 1	Override or limit pilot inputs during corrective action	NP	H5, H6	The system must not fail to override or limit pilot inputs when required for safe recovery.
2	Crew 1	Override or limit pilot inputs during corrective action	TE	H5, H6	Override or limit actions must occur with correct timing to avoid loss of control.
3	Crew 1	Override or limit pilot inputs during corrective action	S	H5, H6	Override or limit must be executed safely without inducing instability.
4	Crew 1	Pilot controlling yoke for steering	NP	H5, H6	The pilot must always be able to control the yoke unless doing so would compromise safety.
5	Crew 1	Pilot controlling yoke for steering	TE	H5, H6	Pilot yoke input must be timely to maintain control and avoid hazards.
6	Crew 1	Pilot controlling yoke for steering	S	H5, H6	Yoke inputs must be handled safely to avoid errors in directional capability.
7	Crew 2	Override or limit CO-pilot inputs during corrective action	NP	H5, H6	The system must not fail to override or limit co-pilot inputs when necessary.
8	Crew 2	Override or limit CO-pilot inputs during corrective action	TE	H5, H6	Override actions on co-pilot inputs must occur at the correct time.
9	Crew 2	Override or limit CO-pilot inputs during corrective action	S	H5, H6	Override on co-pilot inputs must be safe and prevent loss of control.
10	Crew 2	Co-Pilot controlling yoke for steering	NP	H5, H6	Co-pilot must retain control authority unless overridden for safety reasons.
11	Crew 2	Co-Pilot controlling yoke for steering	TE	H5, H6	Yoke input timing by co-pilot must be accurate to prevent instability.
12	Crew 2	Co-Pilot controlling yoke for steering	S	H5, H6	Yoke use by co-pilot must not induce errors in directional control.
13	SWPS	Signal transmission	NP	H2	Controller-to-actuator signals must

UCA No.	Responsible Block	Control Action	UCA Type	Hazards	Derived Safety Constraint
		from controller to actuator			be transmitted reliably and without interruption.
14	SWPS	Signal transmission from controller to actuator	TE	H2	Signal timing must be correct to maintain control of the aircraft.
15	SWPS	Signal transmission from controller to actuator	S	H2	Signals must be safely transmitted to prevent unintended aircraft behavior.
16	SWPS	Adjust control surfaces to maintain stability	NP	H2	Control surfaces must be adjusted to always maintain stability.
17	SWPS	Adjust control surfaces to maintain stability	TE	H2	Timing of control surface adjustment must be correct to avoid instability.
18	SWPS	Adjust control surfaces to maintain stability	S	H2	Control surface movements must be within safe limits.
19	SWPS	Adjust control surfaces to maintain stability	NP	H2	The system must adjust control surfaces as needed to avoid unstable flight.
20	SWPS	Adjust control surfaces to maintain stability	TE	H2	Control surface timing errors must be avoided to ensure flight stability.
21	SWPS	Adjust control surfaces to maintain stability	S	H2	Surface adjustments must not induce unsafe flight directions.
22	SWPS	Unannunciated error in Angle of attack output	NP	H7	Errors in angle of attack must be annunciated to prevent system failure.
23	SWPS	Unannunciated error in Angle of attack output	P	H3, H4, H6, H7	Potential AOA errors must be detected and mitigated.
24	SWPS	Unannunciated error in Angle of attack output	TE	H3, H4, H6, H7	AOA signal timing must be maintained to prevent misinterpretation.
25	SWPS	Unannunciated error in Angle of attack output	S	H3, H4, H6, H7	Angle of attack must be processed safely to avoid incorrect system response.
26	SWPS	Error in Pitch Angle output	P	H2, H4, H7, H8	Pitch angle output errors must be detected and managed.
27	SWPS	Error in Pitch Angle output	TE	H2, H4, H7, H8	Pitch angle data timing must be maintained to ensure proper function.

UCA No.	Responsible Block	Control Action	UCA Type	Hazards	Derived Safety Constraint
28	SWPS	Error in Pitch Angle output	S	H2, H4, H7, H8	Pitch angle must be accurately processed to avoid system malfunction.
29	Flight Control System	Interaction between actuator and sensor	NP	H7	Sensor-actuator interaction must occur to preserve system functionality.
30	Flight Control System	Interaction between actuator and sensor	TE	H7, H2	Sensor-actuator timing must be precise to prevent FCS malfunction.
31	Flight Control System	Interaction between actuator and sensor	S	H7, H2	Sensor-actuator interactions must be safely coordinated.

Table 10: Code Description

Code	Type	Description
NP	Not Provided	The control action **was not provided** when it **should have been**.
P	Provided	The control action **was provided** when it **should not have been**.
TE	Timing Error	The control action was provided **too early**, **too late**, or **in wrong order**.
S	Stopped Too Soon / Applied Too Long	The control action was **stopped too soon** or **applied too long**, leading to a hazard.