

A New STPA Standard for Aircraft Safety Assessment and Development Assurance

John Thomas

AIR6913: “Using System-Theoretic Process Analysis (STPA) During Development and Safety Assessment of Civil Aircraft”

- Intended only for companies using ARP4761 (safety) or ARP4754 (development assurance)
 - Standard certification processes used for all civil aircraft worldwide
 - A few military aircraft, and some other applications

AIR6913 Excerpt:

- “By looking through a supplemental lens with STPA and ARP4761A/ARP4754B applied to support each other, organizations may be provided a more holistic set of requirements with which to design safer and more resilient products.”

Contents

**Overall Similarities
and Differences**

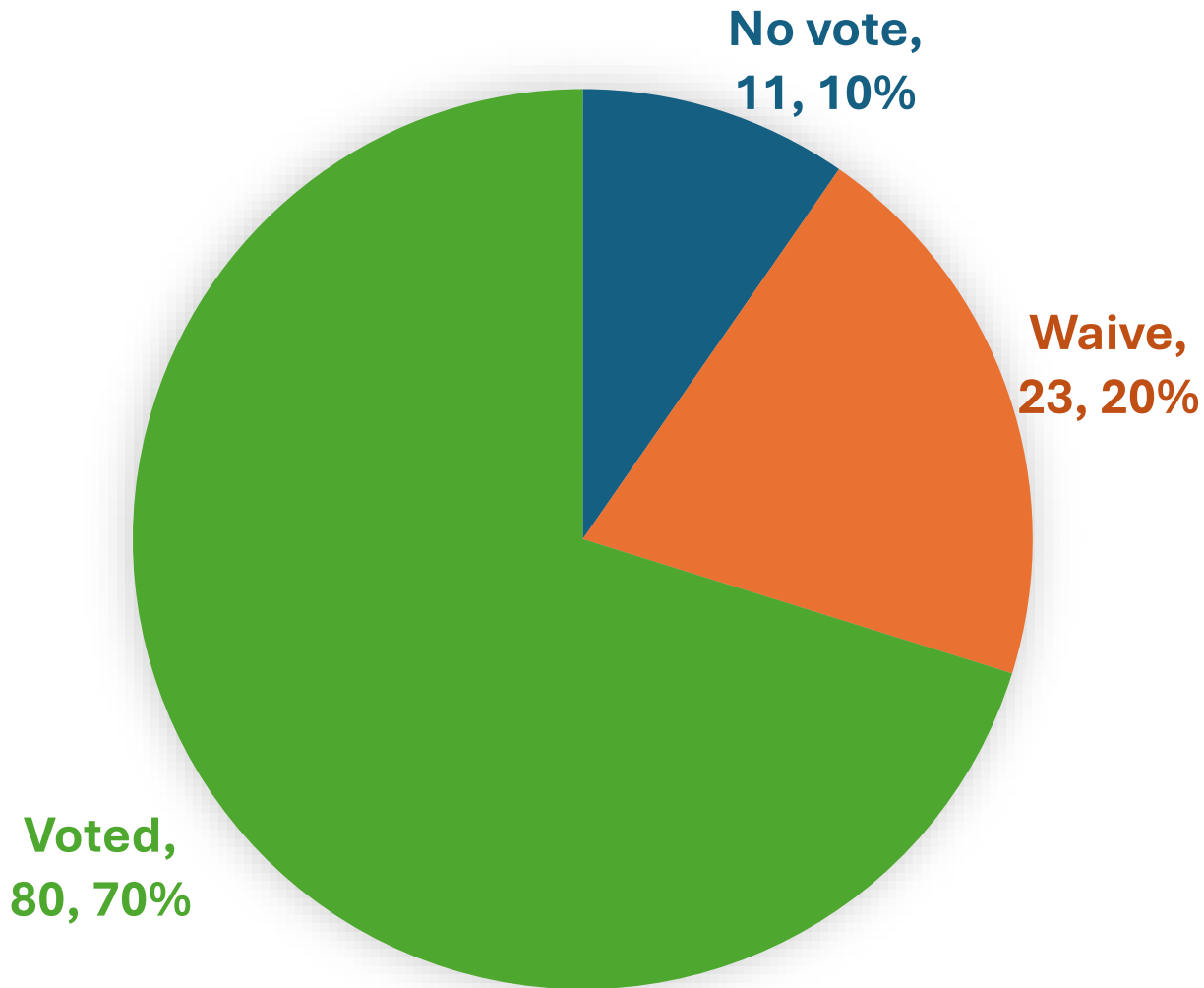
**ARP4761A (Safety)
Supported by STPA**

**ARP4754B
(Development)
Supported by STPA**

**Human Factors
Considerations from
STPA**

3.	INTRODUCTION	7
3.1	STPA Overview	8
3.2	Steps of STPA	9
3.3	ARP4754B and ARP4761A	13
3.4	Similarities and Differences between Approaches	14
3.4.1	Scope	15
3.4.2	Hazards	15
3.4.3	Probability	16
3.4.4	Human Interactions	16
3.4.5	Visualizations	16
4.	ARP4761A SUPPORTED BY STPA	17
4.1	Supporting AFHA/SFHA	19
4.2	Supporting PASA/PSSA	20
4.2.1	Knowledge of system operation	21
4.2.2	Multifunction & Multisystem Analysis	22
4.2.3	Common Mode Failures and Development Assurance Requirements	23
4.3	Additional Considerations	24
4.3.1	Data Integrity	24
4.3.2	Operational Context	25
4.3.3	Human Factors	25
4.3.4	Safety of the Intended Functionality (SOTIF)	25
4.3.5	State Transitions	26
5.	ARP4754B SUPPORTED BY STPA	27
5.1	ARP4754B Objectives Supported by STPA	28
5.2	Concept Development	28
5.3	Development Planning	29
5.4	Aircraft/System Development Processes	29
5.4.1	Aircraft Function and Requirement Development	29
5.4.2	Development of Aircraft Architecture and Allocation of Aircraft Functions to Systems	29
5.4.3	Development of System Requirements	30
5.4.4	Development of System Architecture and Allocation of System Requirements to Items	30
5.4.5	Implementation	31
5.5	Integral Processes	31
5.5.1	Safety Assessment	31
5.5.2	Development Assurance Level Assignment	31
5.5.3	Requirements Capture and Validation	31
5.5.4	Implementation Verification	32
5.5.5	Configuration Management	32
5.5.6	Process Assurance	32
6.	STPA SUPPORT FOR HUMAN INTERACTIONS	32
6.1	Brief introduction	32
6.2	Human Interaction as Considered in STPA	33
6.3	Human Interaction as Considered in ARP4761A	35
6.4	Short Example	36

Ballot Results



SAE S-18 Committee

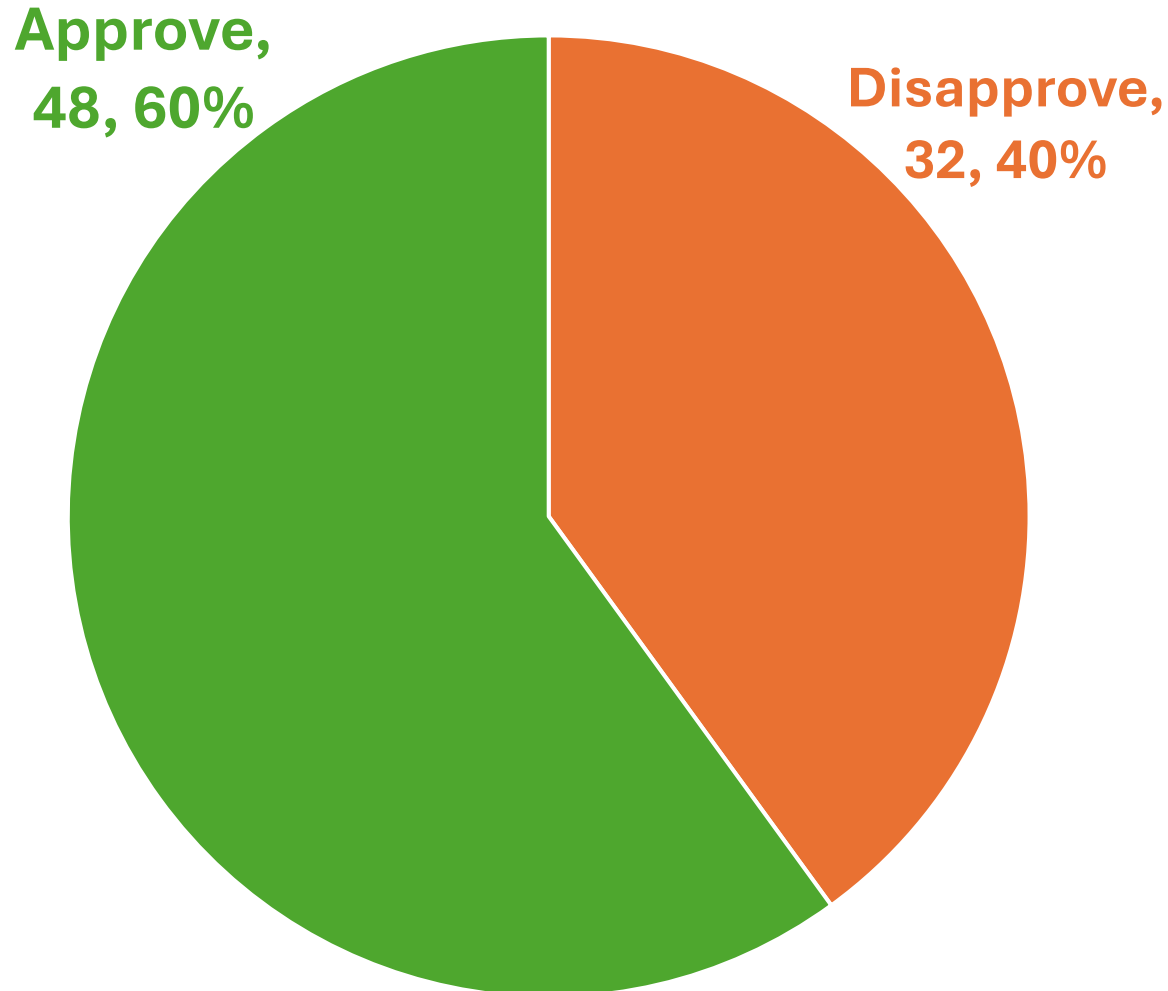
- “Aircraft and System Development and Safety Assessment Committee”
- Same committee that authors ARP4761 / ARP4754
- 114 total voting members

Ballot validity



At least 50% of committee must cast a vote

Ballot Results



Ballot Threshold

- 75% of votes must be “approve” to pass
- Need 12 more “approve” votes to pass (out of 80 votes)

Re-ballot process

- All disapprove votes have proposed alternative language that would be acceptable.
- We need to evaluate each comment to determine whether to accept/reject the comment or how best to address it.
- Monthly meetings to discuss & resolve.
- **We need your help to make these decisions!** Contact jthomas4@mit.edu