MIT STAMP Workshop 2026

Employing STPA to Explore Certification Pathways for Advanced Automation

Copyright © 2026 Boeing. All rights reserved.

Presenters



Matt Jahn
Associate Technical Fellow



Emily Howard
Principal Senior Technical Fellow



Kyle Ryan
Associate Technical Fellow

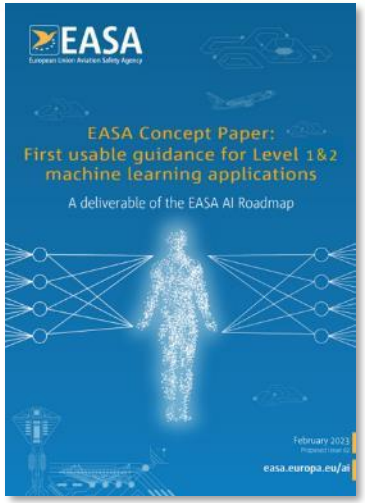
Co-Authors

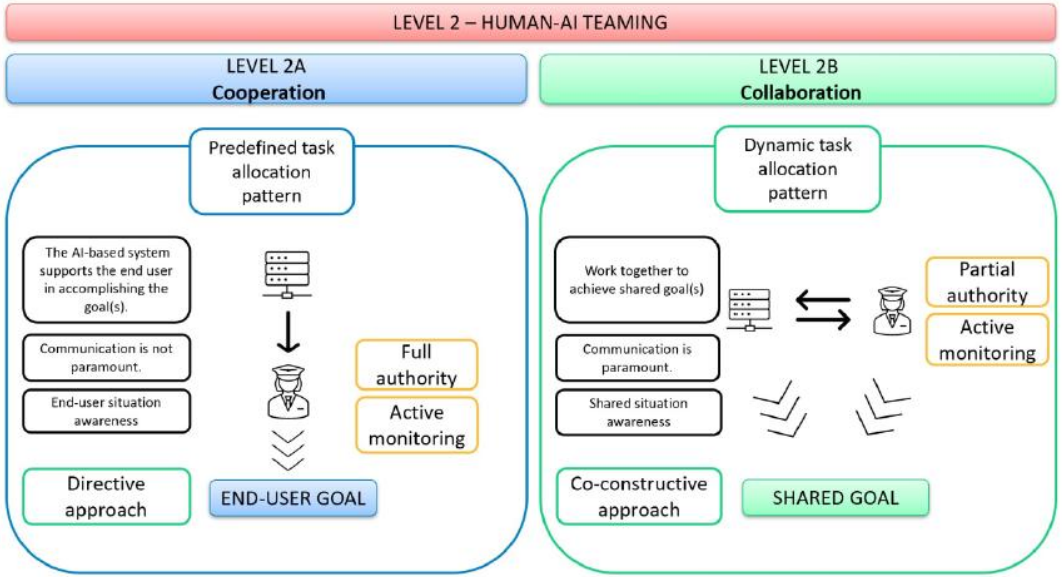
Forest Sutton
Prashin Sharma

Copyright © 2026 Boeing. All rights reserved.

Boeing/EASA Collaboration Project (IPC)

- Innovation Partnership Contract (IPC) will:
  - In collaboration with EASA, establish the regulatory requirements, means of compliance, and V&V strategy for an ML-based system
  - Be based on EASA AI Concept Paper Issue 2 (2024)
  - Lay the groundwork for future certified AI systems
  - Consider both a level 2A (human/machine teaming) system and a level 3A (more autonomous machine) system, per EASA's leveling scheme





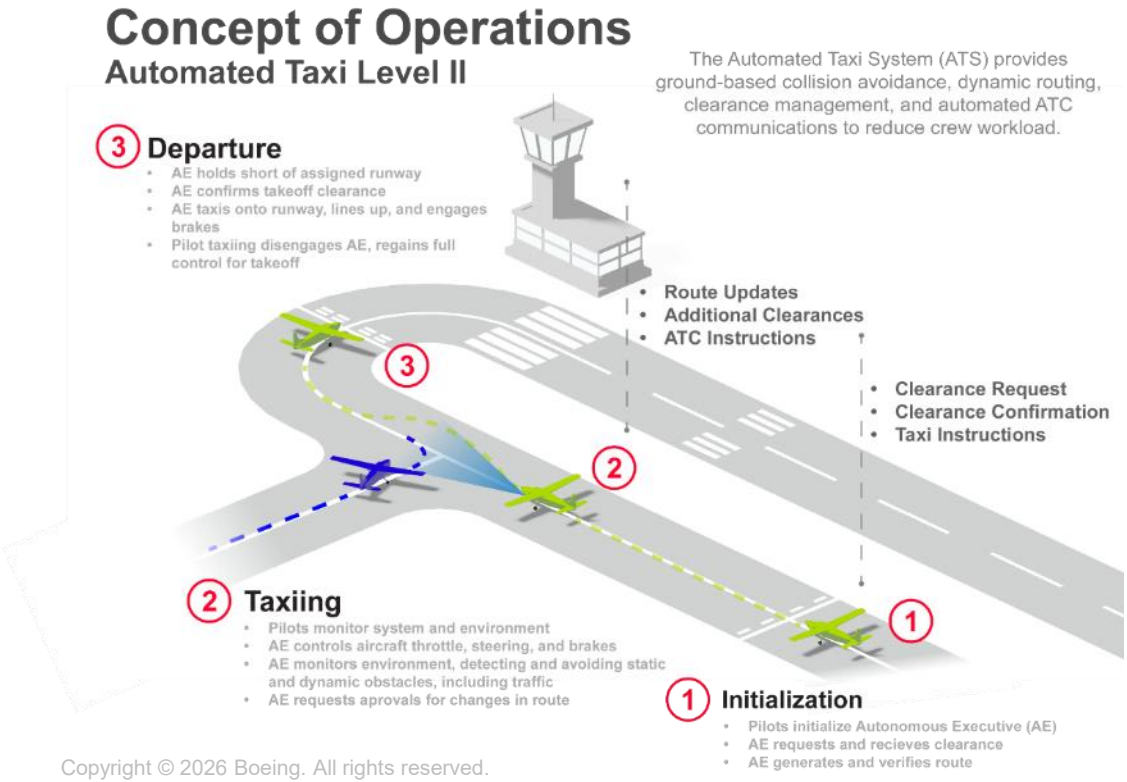
	Phase 1	Phase 2
	Level 1 AI: Assistance to Human	**Level 2 AI:** Human/Machine Teaming	**Level 3 AI:** More Autonomous Machine
	• **Level 1A:** Human augmentation • **Level 1B:** Human cognitive assistance in decision and action selection	• **Level 2A:** Human and AI-based system cooperation • **Level 2B:** Human and AI-based system collaboration	• **Level 3A:** The AI-based system performs decisions and actions, overridable by the human • **Level 3B:** The AI-based system performs non-overridable decisions and actions

Copyright © 2026 Boeing. All rights reserved.

[1] EASA Concept Paper: Guidance for Level 1 & 2 machine learning applications, March 2024

IPC Focus Areas

- Application of Concept Paper Objectives and MOCs, and Validation and Verification approach
- A live demonstration of the systems being explored
- Human Factors and the use of System-Theoretic Process Analysis (STPA) for developing early concept HMI requirements and a partial means of compliance.





Copyright © 2026 Boeing. All rights reserved.

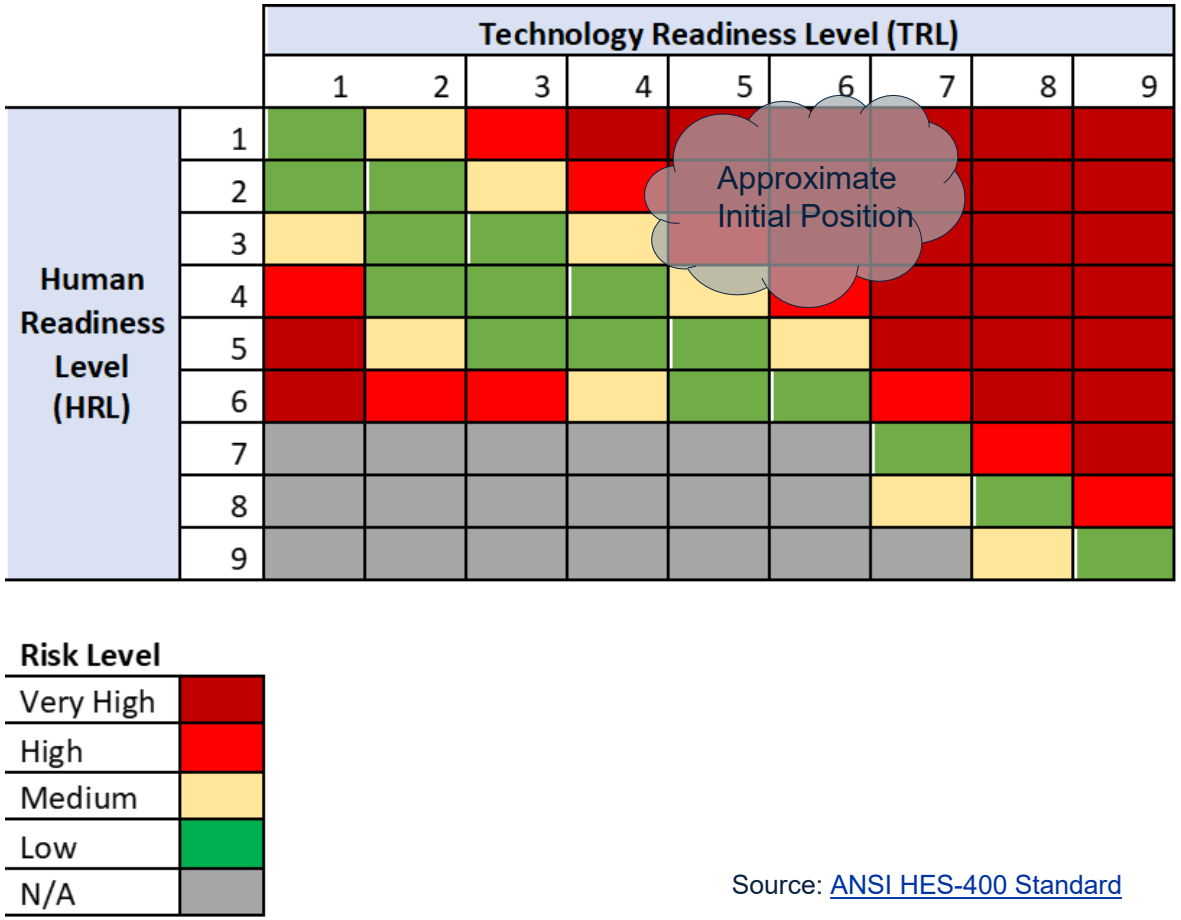
Project began with HRL lagging TRL—STPA was proposed to remediate

Human Readiness Level

Level	HRL
1	Basic principles for human characteristics, performance, and behavior observed and reported
2	Human-centered concepts, applications, and guidelines defined
3	Human-centered requirements to support human performance and human-technology interactions established
4	Modeling, part-task testing, and trade studies of human systems design concepts and applications completed
5	Human-centered evaluation of prototypes in mission-relevant part-task simulations completed to inform design
6	Human systems design fully matured and demonstrated in a relevant high-fidelity, simulated environment or actual environment
7	Human systems design fully tested and verified in operational environment with system hardware and software and representative users
8	Human systems design fully tested, verified, and approved in mission operations, using completed system hardware and software and representative users
9	System successfully used in operations across the operational envelope with systematic monitoring of human-system performance

Technology Readiness Level

Level	TRL
1	Basic principles observed and reported
2	Technology concept and/or application formulated
3	Analytical and experimental critical function and/or characteristic proof of concept
4	Component and/or breadboard validation in laboratory environment
5	Component and/or breadboard validation in relevant environment
6	System/subsystem model or prototype demonstration in a relevant environment
7	System prototype demonstration in an operational environment
8	Actual system completed and qualified through test and demonstration
9	Actual system proven through successful mission operations



Source: ANSI HES-400 Standard

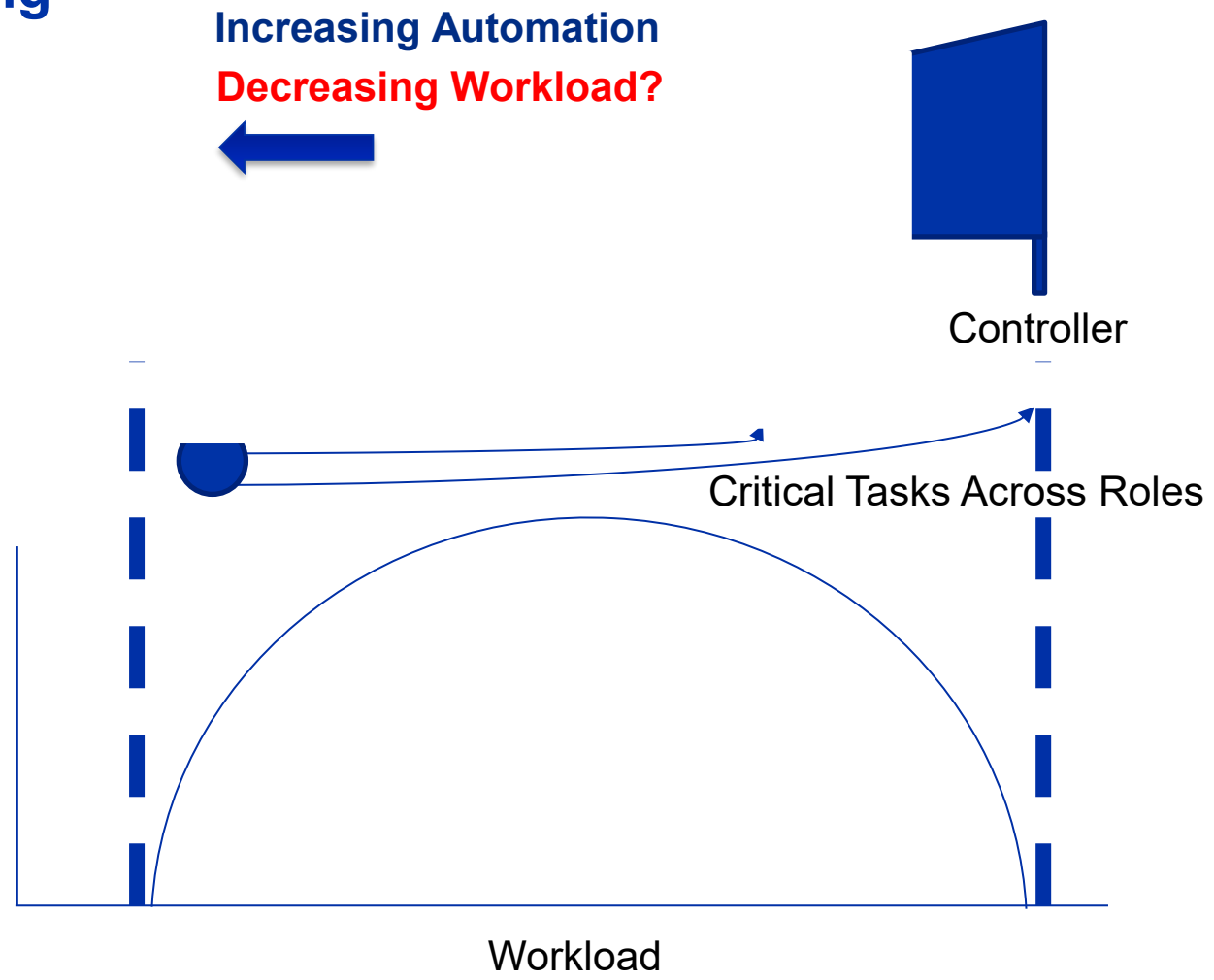
While the TRL scale focuses on technical maturity, the HRL scale emphasizes the readiness of a developing technology for safe and effective human use. The pace of development must align on both scales

Copyright © 2026 Boeing. All rights reserved.

Human-Machine Teaming Roles are Evolving

Human Roles

- **Controller:** Responsible for performing most vehicle & all mission functions
- **Mission Commander:** Responsible for performing key mission and vehicle functions
- **Supervisor:** Responsible for monitoring vehicle & mission functions
- **Contingency Management:** Responsible only for intervening when autonomous functions are erroneous, inadequate, or unsuitable



Key design constraint: Workload and human performance are **nonlinearly** related

For all roles, we must fully understand non-normal, contingency management tasks

Copyright © 2026 Boeing. All rights reserved.

Common Misconception: Interaction vs Interface Design

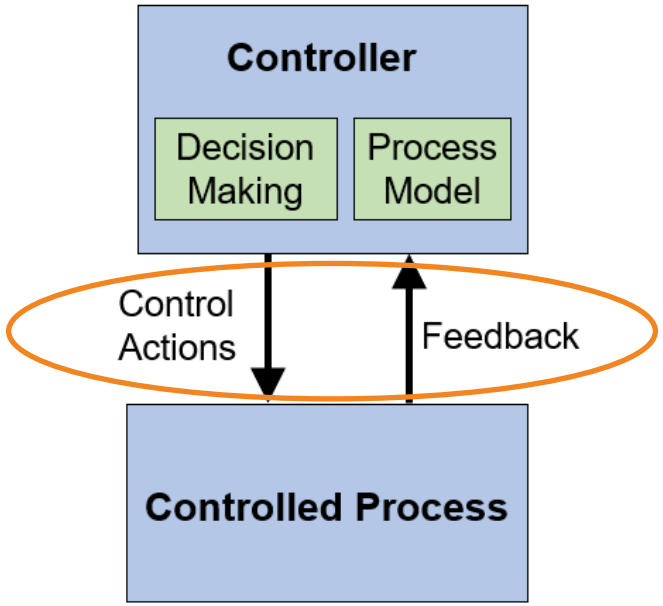
Interaction Design is the determination of:

- **Who** (considering multiple roles) needs or does
- **What** tasks (with associated information or action elements)
- **When** (required or desired) and
- **How Well** (in terms of precision, timeliness, etc.)

Interface Design is informed by Interaction Design, subsequently determining:

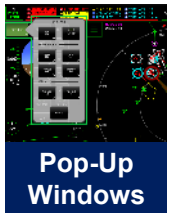
- **Where** (in the space surrounding the human) **and**
- **How** display and control features are provided

While interface design decisions can occur later in development, interaction requirements must be established early

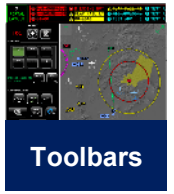










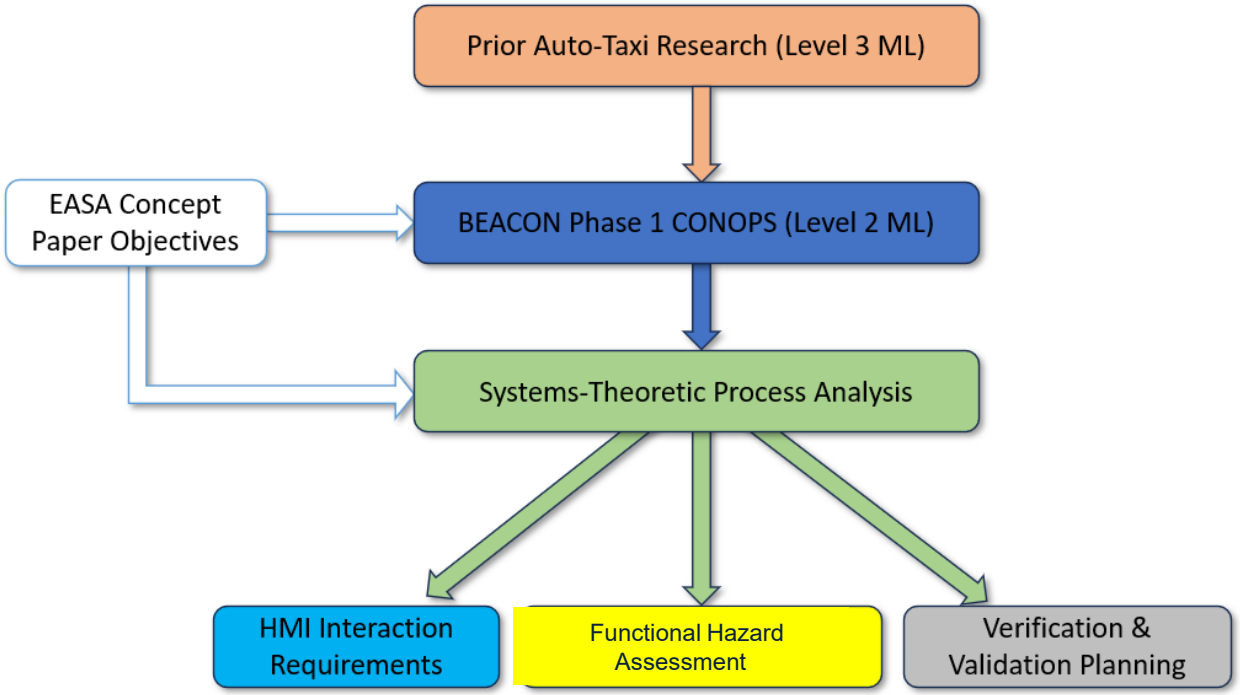


Establishing Interaction Requirements Early Raises Human Readiness Levels

Copyright © 2026 Boeing. All rights reserved.

STPA Provided Significant Benefit to Advance Human Readiness in the IPC

- As a research project, we did not apply our traditional Flight Deck design process.
- Which enabled us to explore the use of STPA to generate flight crew interaction requirements.
- STPA also proved to be valuable for other certification activities as well



Losses

ID	Description	Affected Stakeholders
L1	Disruption to airport or airline operations	airport authority, airline
L2	Loss of human life or injury to humans	airport authority, airline, regulator, ATC, OEM
L3	Damage to aircraft or airport infrastructure	airport authority, airline, regulator
L4	Loss of passenger comfort	regulators, airline
L5	Loss of reputation	regulators, airline, ATC, OEM
L6	Loss of trust in automation	regulators, airline, ATC
L7	Loss of revenue to regulatory fines/enforcement actions	regulators, airline

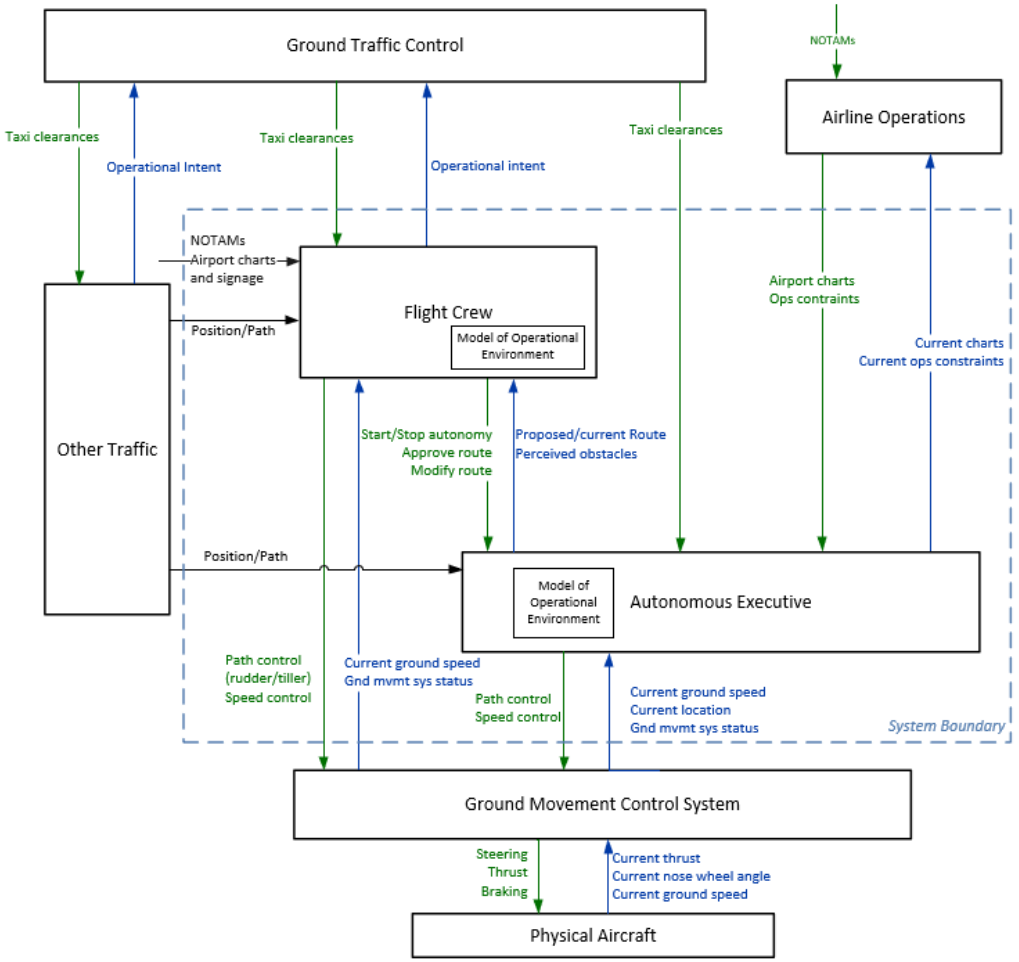
Hazards

ID	Description	Resulting Losses
H1	Aircraft departs designated taxiway (allowable taxiway space)	L1-L7
H2	Aircraft enters unauthorized/uncleared taxiway or runway	L1-L7
H3	Aircraft exceeds proximity threshold to airport infrastructure, people, vehicles, or other aircraft	L1-L7
H4	Aircraft exceeds expected maximum speed constraints	L1, L2, L3, L4, L5, L6
H5	Aircraft creates operational delays (taxiing too slowly)	L1, L4, L5, L6
H6	Aircraft exhibits otherwise safe but unexpected or inefficient behavior	L1, L4, L5, L6
H7	Aircraft autonomous behavior creates additional or excessive workload for humans	L1, L5, L6

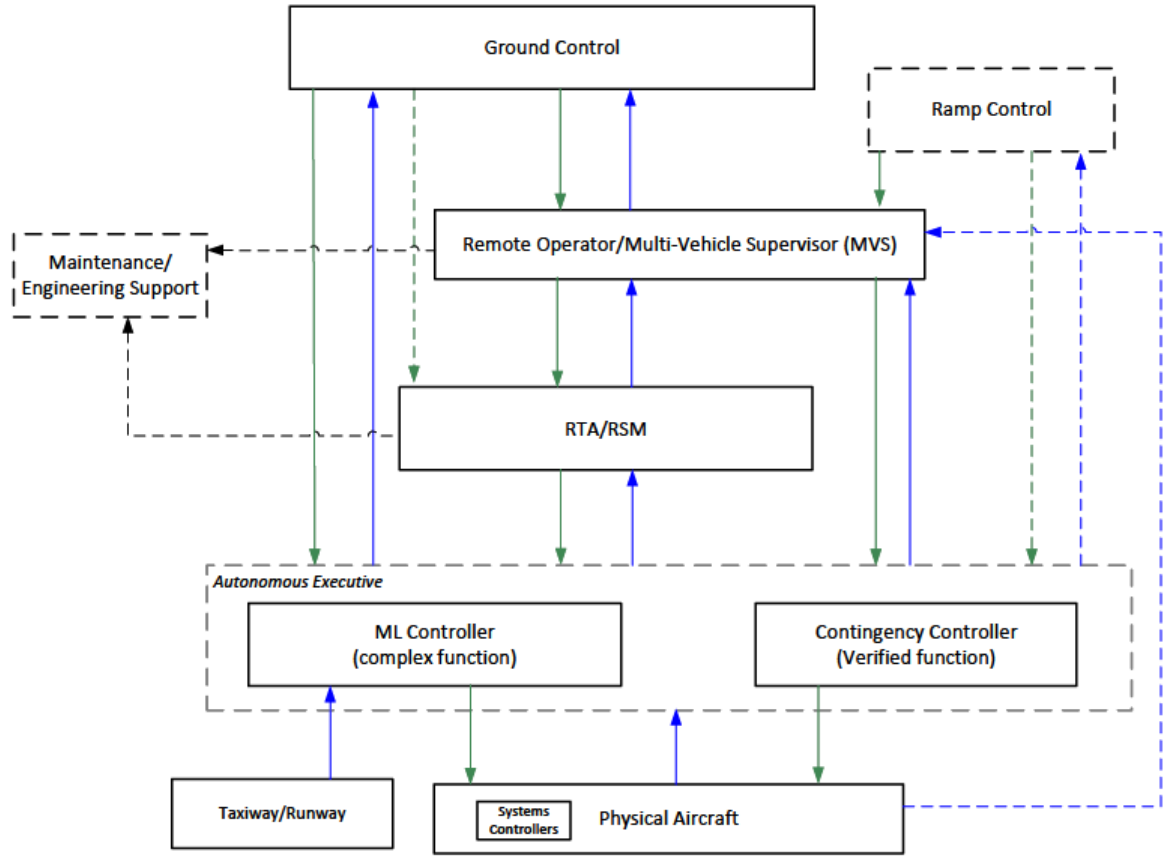
Copyright © 2026 Boeing. All rights reserved.

Applying STPA to Multiple CONOPs

Level 2 Automation (Human/Machine Teaming) Control Structure (Phase 1)



Level 3A Automation Control Structure (Phase 2)

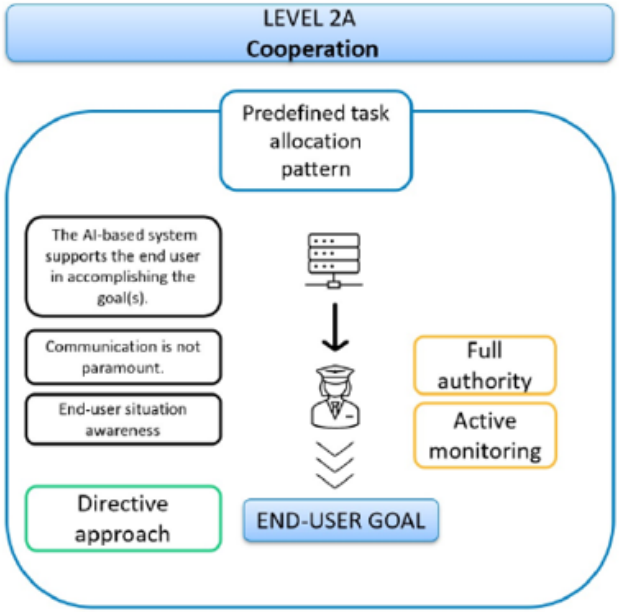


Note: control structures simplified for public release

Copyright © 2026 Boeing. All rights reserved.

Control Authority Implications

EASA Level 2A Description [1]

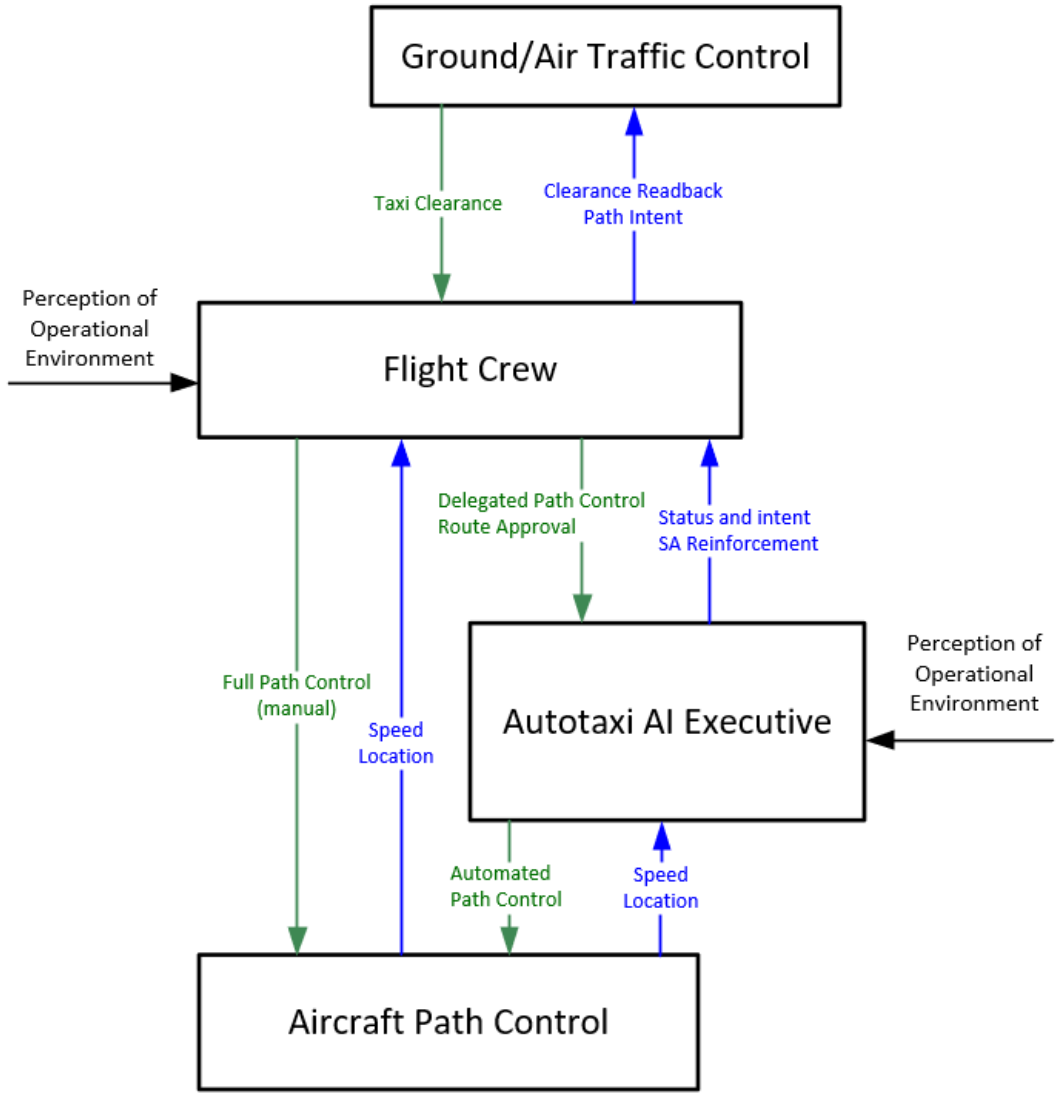


Human-AI cooperation (Level 2A AI): cooperation is a process in which the AI-based system works to help the end user accomplish his or her own goal.

The AI-based system works according to a predefined task allocation pattern with informative feedback to the end user on the decisions and/or actions implementation. The cooperation process follows a directive approach. Cooperation does not imply a shared situation awareness between the end user and the AI-based system. Communication is not a paramount capability for cooperation.

[1] EASA Concept Paper: Guidance for Level 1 & 2 machine learning applications, March 2024

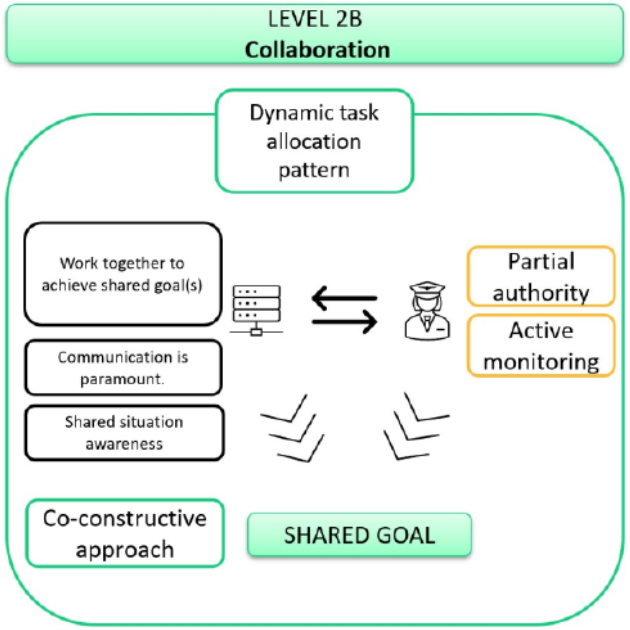
STPA 'Mini' Control Structure Level 2A - Cooperation



Copyright © 2026 Boeing. All rights reserved.

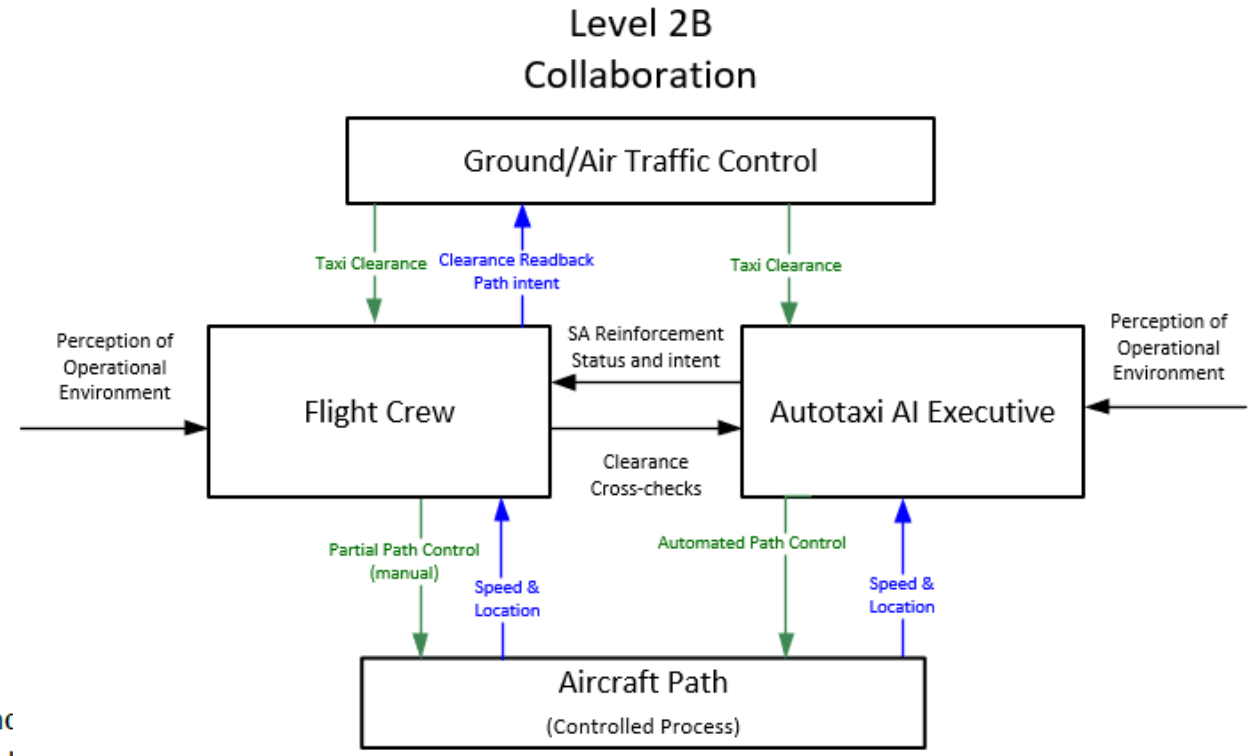
Control Authority Implications

EASA Level 2B Description [1]



Human-AI collaboration (Level 2B AI): collaboration is a process in which the end user and AI-based system work together and jointly to achieve a predefined shared goal and solve a problem through co-constructive approach. Collaboration implies the capability to share situation awareness and to readjust strategies and task allocation in real time. Communication is paramount to share valuable information needed to achieve the goal.

STPA 'Mini' Control Structure



[1] EASA Concept Paper: Guidance for Level 1 & 2 machine learning applications, March 2024

Copyright © 2026 Boeing. All rights reserved.

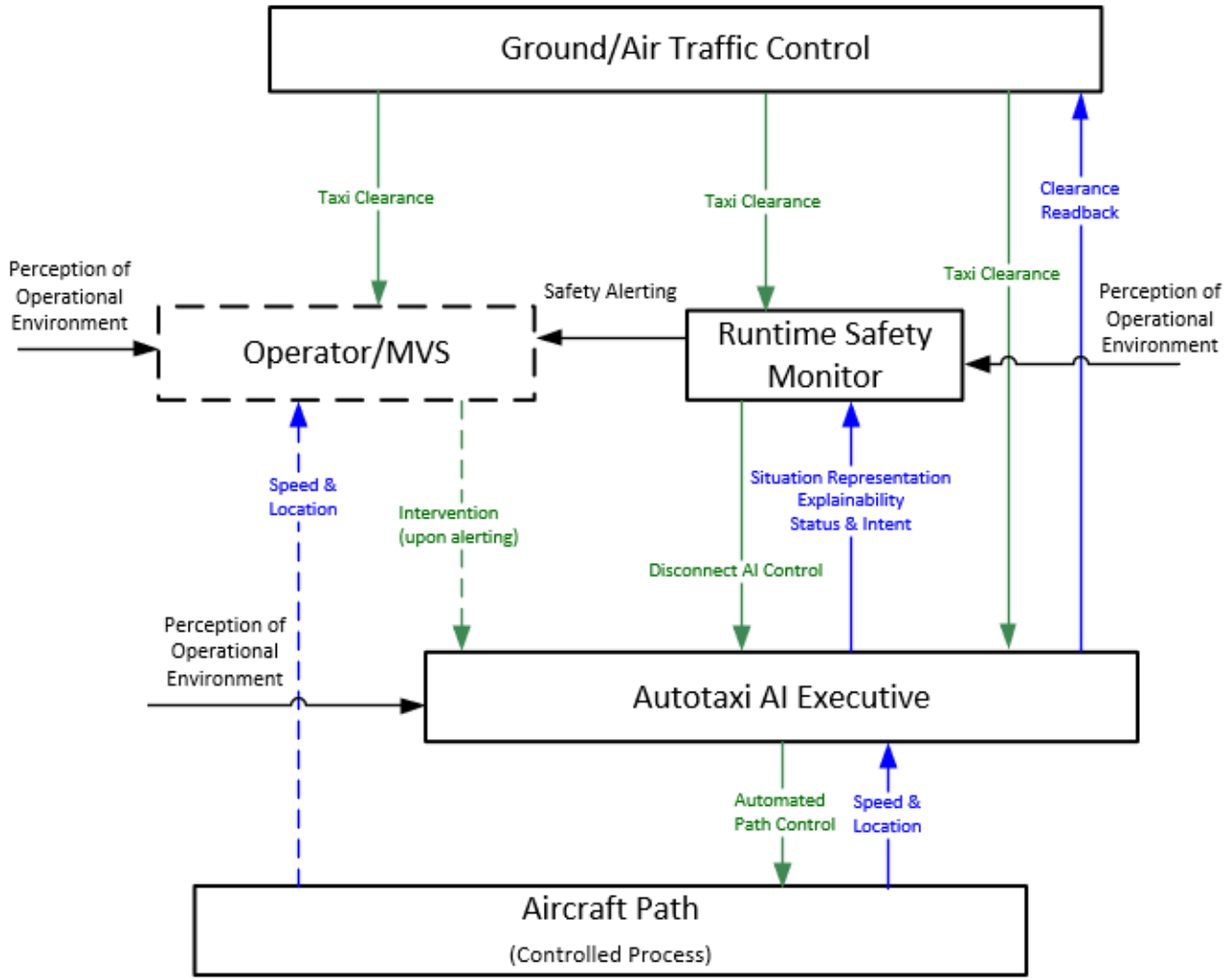
Control Authority Implications

EASA Level 3A Description [1]

AI level	Function allocated to the system to contribute to the high-level task	Authority of the end user
Level 3A Safeguarded advanced automation	Safeguarded automatic decision and action implementation	Limited, upon alerting

The difference between Level 2 and Level 3 AI revolves around the extent of authority given to the AI-based system. At Level 2, the human-AI teaming concept foresees a partial release of authority to the system however under full oversight of the end user, who consistently remains accountable for the operations. On the contrary, at Level 3, the AI-based system is given full authority to make and implement decisions, under remote monitoring of the end user (Level 3A AI) or without end user involvement (Level 3B AI).

STPA 'Mini' Control Structure
Level 3A
Safeguarded Advanced Automation



[1] EASA Concept Paper: Guidance for Level 1 & 2 machine learning applications, March 2024

Copyright © 2026 Boeing. All rights reserved.

Insights for Level 3A Concept

- STPA activity of defining human flight crew responsibilities, mental models, and decision-making highlighted significant and critical human contributions to safety
  - Provided a more holistic baseline for required behaviors of AI-based system
  - Enabled Boeing team to propose new objective and MoC back to EASA for consideration:

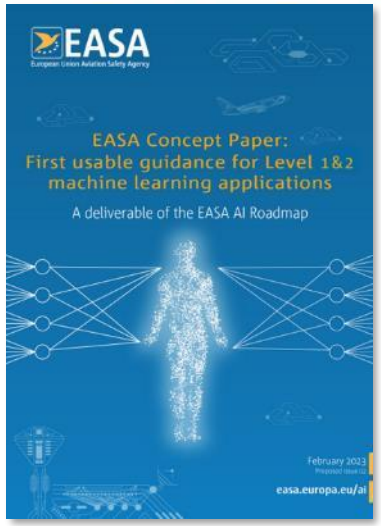
    - **Objective HF-XX:** For AI-based systems that aim to reduce human interaction compared with current or comparable systems, the applicant should design the AI-based system with a detailed understanding and retention (at a minimum) or enhancement (preferable) of all human contributions to operational safety and performance.

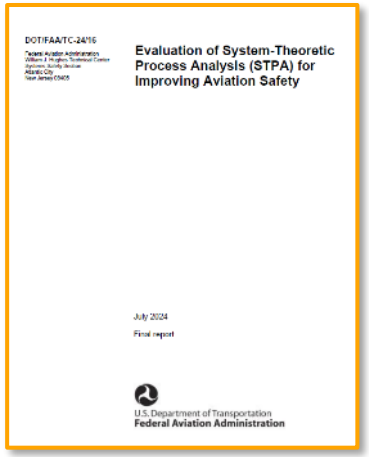
    - **MOC HF-XX:** A detailed task analysis report of all human activities that are being performed within current (comparable) systems, with traceability to the AI-based system design aspects that perform, or eliminate the need for, those activities.

Copyright © 2026 Boeing. All rights reserved.

Regulatory Reception of STPA

- STPA in the IPC with EASA
  - The IPC was EASA's AI team's first chance to see STPA in action
  - EASA AI team stated that STPA helped enhance their understanding of what was important as they moved forward with development of AI regulatory guidance
  - EASA asked Boeing to further explore the use of STPA as a possible means of compliance to Concept Paper objectives





- Project also reinforced previous findings in DOT/FAA/TC-24/16 by SMEs from FAA, EASA, ANAC, ICAO, and NASA:
  - *"STPA provides a capability beyond current practices when analyzing future technologies like increasing autonomy and eVTOL."*
  - *"STPA can satisfy existing regulatory objectives and would be beneficial in regulatory reviews and oversight."*
  - *"SME participants found that STPA provides a way to identify interactions and scenarios relevant to regulatory safety objectives that can be overlooked by current methods."*

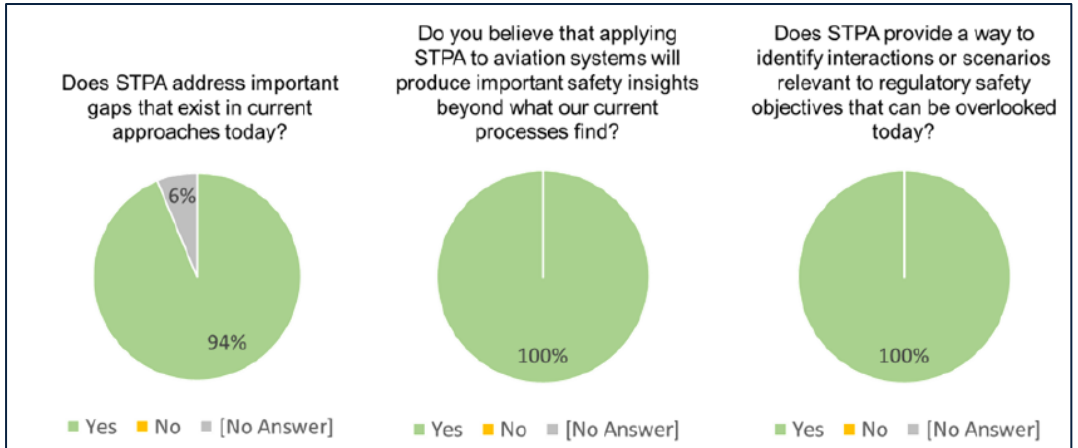


Figure A-1. Findings from FAA, EASA, ANAC, ICAO, and NASA participants related to STPA's ability to produce relevant findings that may be missed today

Copyright © 2026 Boeing. All rights reserved.

STPA as a Means of Compliance

EASA asked Boeing to propose which objectives may be able to be met via the use of STPA

- Reviewed certification objectives in EASA Concept Paper
- Conclusion: STPA can aid system design AND potentially be used to create compliance artifacts

CO-01:
The applicant should **identify the list of end users** that are intended to interact with the AI-based system, together with end-user roles, responsibilities (including indication of the level of teaming with the AI-based system, i.e. none, cooperation, collaboration) and **expected expertise** (including assumptions made on the level of training, qualification and skills).

STPA Rationale:
End Users will be included in the "controllers" that are required to be identified as part of the control structure creation process. The process of building the control structure will help to identify end users, as well as their interaction with the AI-based system, and the **assumptions** around those end users level of expertise, qualification, and skills.

CO-02:
For each end user, the applicant **should identify which goals and associated high-level task**(s) are intended to be performed in interaction with the AI-based system.

The STPA process requires that the responsibilities of each controller (which includes the end user(s) and the AI-based system) be defined, which are equivalent to goals; **STPA control actions represent high-level tasks needed to accomplish those controller goals.**

Copyright © 2026 Boeing. All rights reserved.

Takeaways and Final Thoughts

STPA can be used to:

- **Evaluate potential new concepts for human-automation interaction** to uncover potential unintended consequences and unknown unknowns
- **Evaluate and mature associated concepts of operation** to help ensure automation is being applied to the right problems
- **Ensure that off-nominal situations are well considered**, which are critically important for defining the humans' roles and tasks
- **Demonstrate traceability and satisfaction** as a means of compliance for certain certification objectives
- **Fully account for the human's contribution to safety—**simply replacing the human's behaviors/tasks with automation may not be sufficient and may be detrimental to safety
- **Raise Human Readiness Levels** and derive human-machine interaction requirements early in development

Sample Flight Crew HMI Interaction Requirement

Control Action	Unsafe Control Action	Causal Scenario	Requirements
Modify Route	Flight Crew provides Modify Route command when new route violates current NOTAMs. [H1]	Flight Crew has outdated info on the state of airport NOTAMs.	Design of system must ensure current and complete information, including current state of airport NOTAMs.

Identify Unsafe Control Actions | Identify Loss Scenarios | Define Requirements

Copyright © 2026 Boeing. All rights reserved.



Copyright © 2025 Boeing. All rights reserved.