Empirical Evaluations of STPA in the Aviation Industry

John Thomas

Aeronautics and Astronautics

MIT

Any questions? Email me! JThomas4@mit.edu

Questions from practitioners submitted to MIT STAMP Workshop

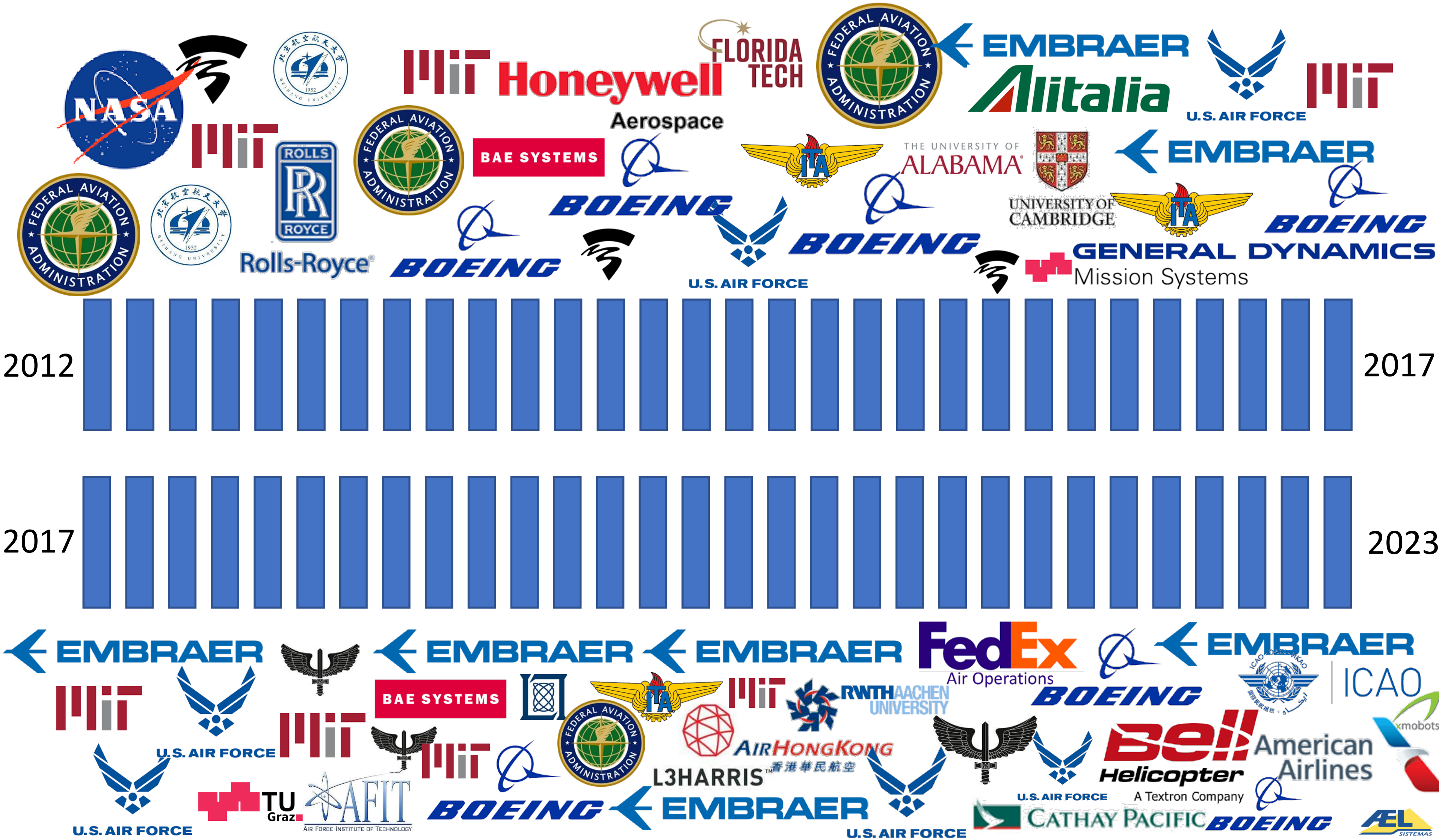
- How does STPA compare to other analysis methods?
- STPA vs. FTA/FMEA?
- How does STPA help with system safety when we are already using the standard methods?
- What is the difference between what STPA can bring and what the other methods offer today?
- What is the additional benefit of STPA over traditional risk assessment methods?
- What is the comparison between STPA and System Safety Assessments?
- What is the benefit of STPA in comparison to deductive and inductive methodologies?
- What is the relationship between STPA and ARP4761?
- Is there an empirical study contrasting STPA with traditional methods?
- What value does STPA have for aeronautics?
- What are the benefits of STPA?
- **Is there any comparison of STPA and the classic FHA/SSA methods in aircraft certification?**
- **Is there any proof that STPA has advantages over traditional methods?**
- **What is the reason to use STPA? We already use the standard methods.**
- How effective is STPA compared to what is done today?
- What are the pros of implementing STPA and the negatives of implementing current methods? [My org] still believes current methods are robust enough for new complex systems. Specifically, illustrate that current methods are not robust enough and how STPA is better.
- What is the motivation to overcome the use of outdated methods and invest resources in STPA?
- Why should we do STPA when we have established FHA, FMEA, FTA, etc. analysis methods?
- Is STPA being adopted by others? What did they find?
- What is the advantage over old methodologies? Need a strong argument just to have a look and consider a new approach.
- Does STPA produce the same results as traditional approaches?
- We need lots of explanations and persuasion to adopt STPA as people don't see the immediate benefit, unless an accident or hazard happens
- The biggest problem for adoption is finding exact and accurate information about case study from companies or officials.
- How can STPA/STAMP be used to enhance safety analysis previously conducted to quantify a net change in results?
- **Need publicly available success stories.**
- How measure the real effectiveness of STPA against other methods?
- STPA remains a new and risky proposition for those who see nothing wrong with the status quo, or see the problems but do not have the will or mandate to instigate change.
- Need more information and examples of how STPA is different than the ARP docs
- How can we compare STAMP vs. the traditional safety assessment process such as ARP 4761?
- How STAMP methods can be implemented in industrial context? What are the advantages from other solutions?
- How STPA is better than pre-existing analysis approaches
- Please provide as many examples as you can from aviation sector as safety plays a major role in aviation.
- Need to establish effectiveness of STPA and comparison to other methods
- How is STPA helpful in Aviation Safety?
- What value does STPA add that traditional methods don't?
- How to demonstrate value vs established methods
- Are there are some practical samples of STAMP applied on practical that we may refer to?
- How does STPA help ensure the requirements completeness?
- How effective is the new method?
- How much better can we expect STPA analyses to be, compared with our existing
- For SOTIF, there is high demand for quantitative evaluation but STPA does not support this aspect and FTA does.
- Do you have good examples of the effectiveness or improvement from STPA?
- **Concerning safety scenarios driven by failures only—do we get at least the same results with STPA as traditional approaches ?**

Are there any Empirical Evaluations of STPA in Aviation?

STPA Publications (as of May 2023)

- 1,640 publications on STPA used to analyze aircraft systems (~10 year period)
    - How does it compare?
      E.g., FHA on Aircraft: 6,380 publications over ~**30 years**
- 4,270 publications on STPA in safety management (~10 year period)
- However, this metric may be biased.
- What about practitioners?

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops

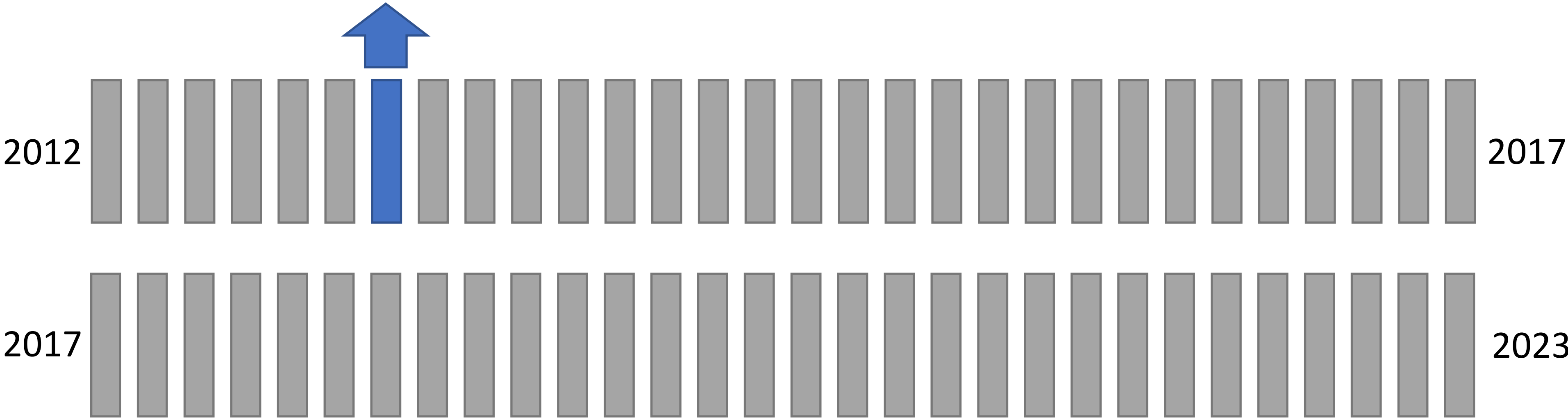


Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops

Rolls-Royce

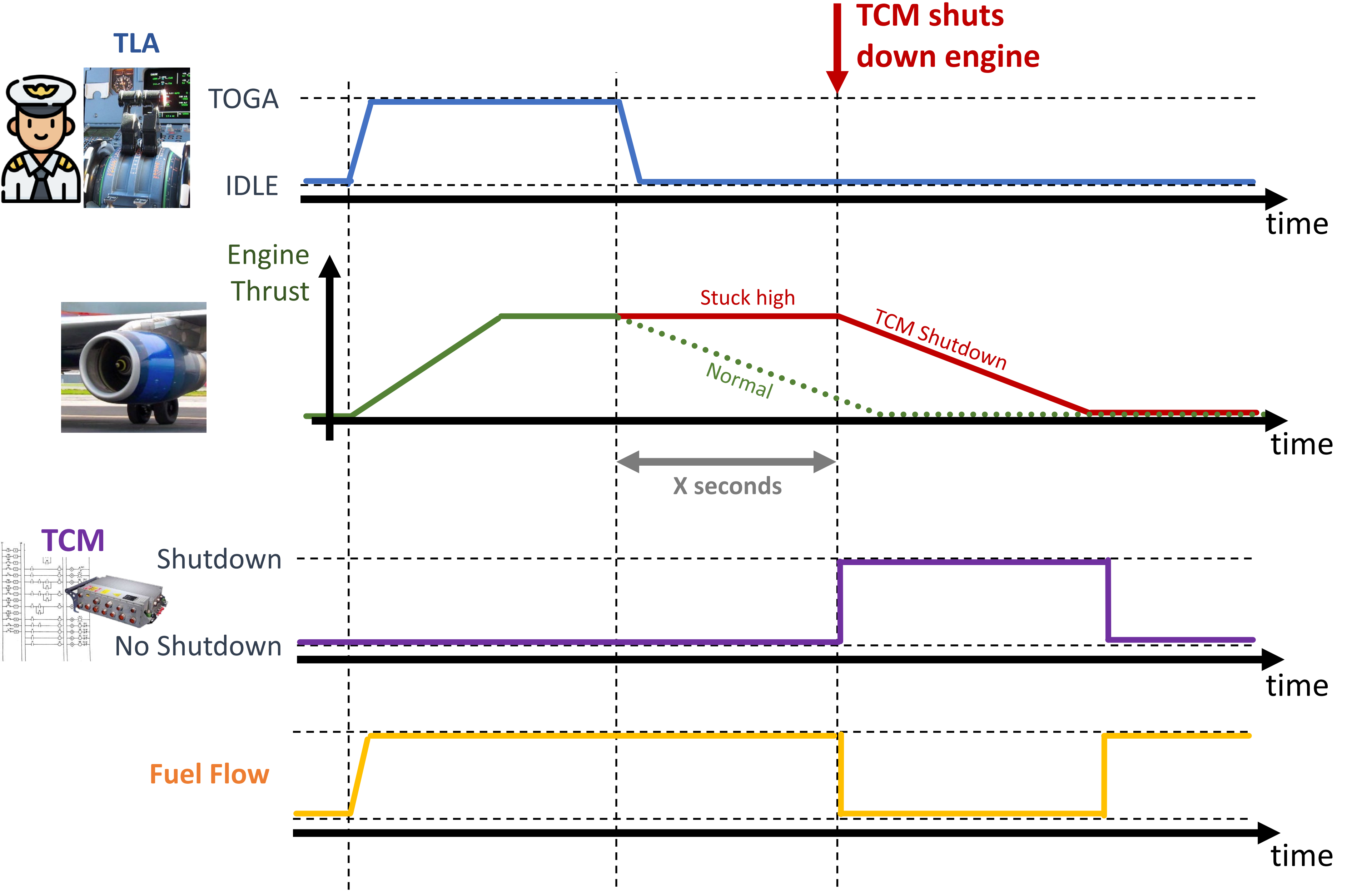
STPA was applied to a commercial aircraft engine control system to mitigate UHT (Uncommanded High Thrust) scenarios

- STPA applied after control system had already been designed.
- Standard development and safety assessment processes for certification already completed.
- Two years of flight testing already completed.



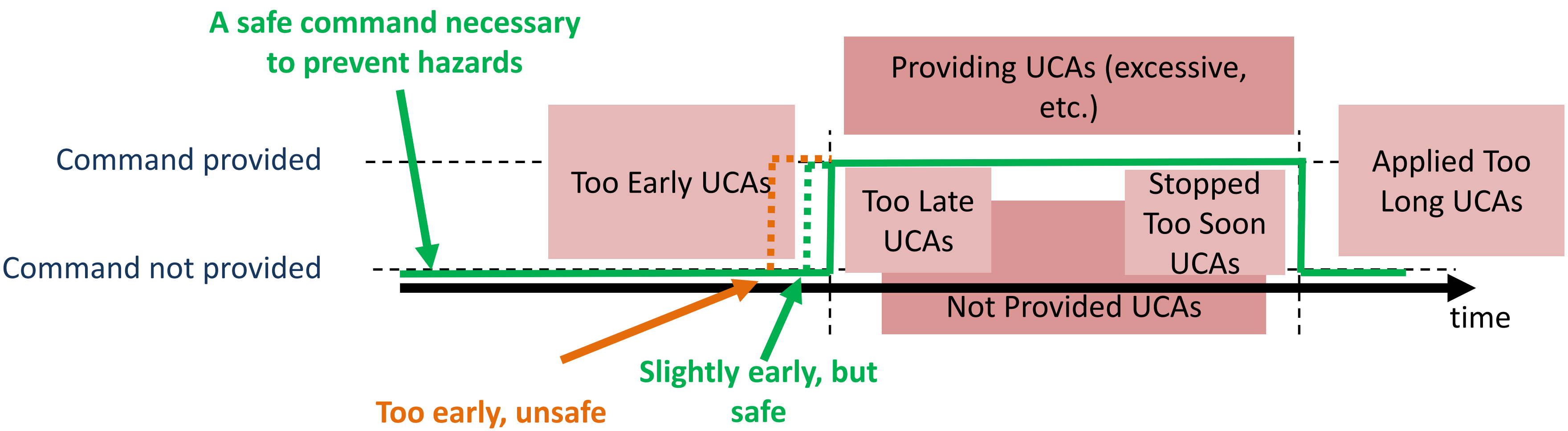
W. Fletcher, Application of System Theoretic Process analysis to requirements and algorithms for a thrust control malfunction protection system, 2014, 3rd STAMP/STPA Workshop

Thrust Control Malfunction (TCM)



This is an oversimplified example only!

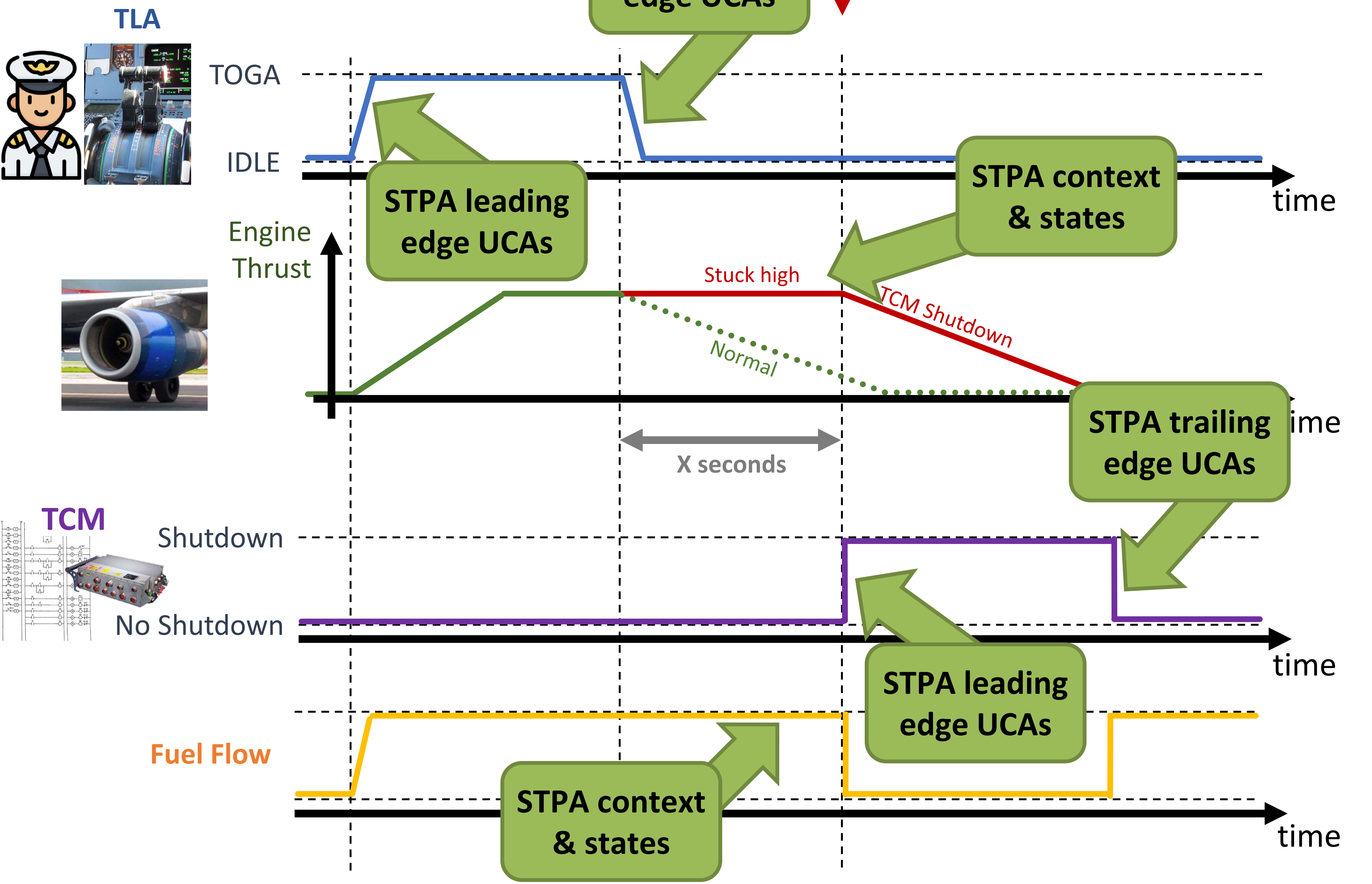
STPA UCA Bounding



Control Actions:	Not providing causes hazard	**Providing causes hazard** *[in wrong situation, excessive, insufficient, repetitive, wrong direction, etc.]*	Too early, too late, Order	Stopped Too Soon / Applied too long
Throttle	?	?	?	?
Engine Shutdown				

The complete set of UCAs will fully bound the necessary safe behavior

TCM concept



STPA trailing edge UCAs

TCM shuts down engine

STPA leading edge UCAs

STPA context & states

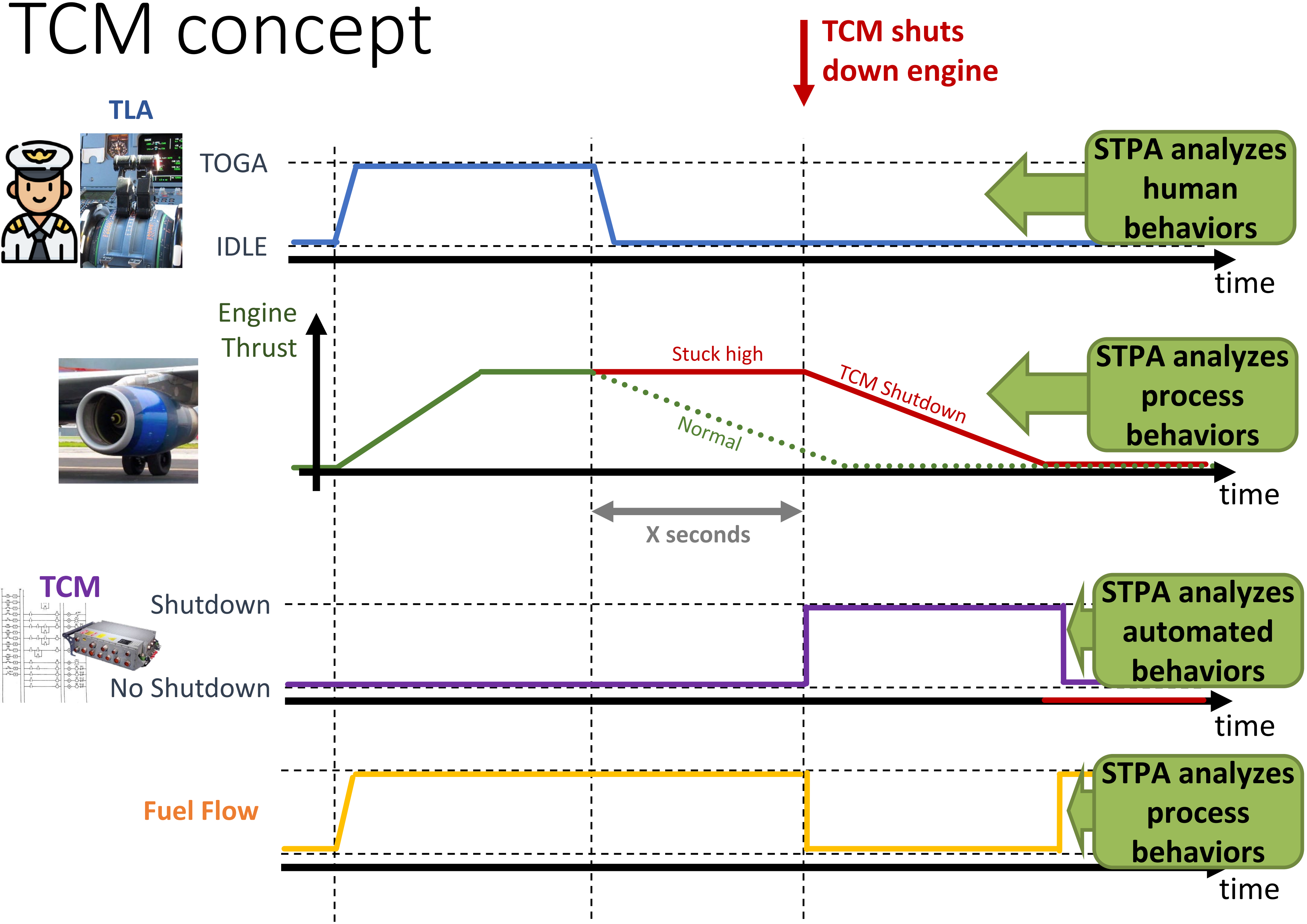
STPA trailing edge UCAs

STPA leading edge UCAs

STPA context & states

This is an oversimplified example only!

TCM concept



TCM shuts down engine

STPA analyzes human behaviors

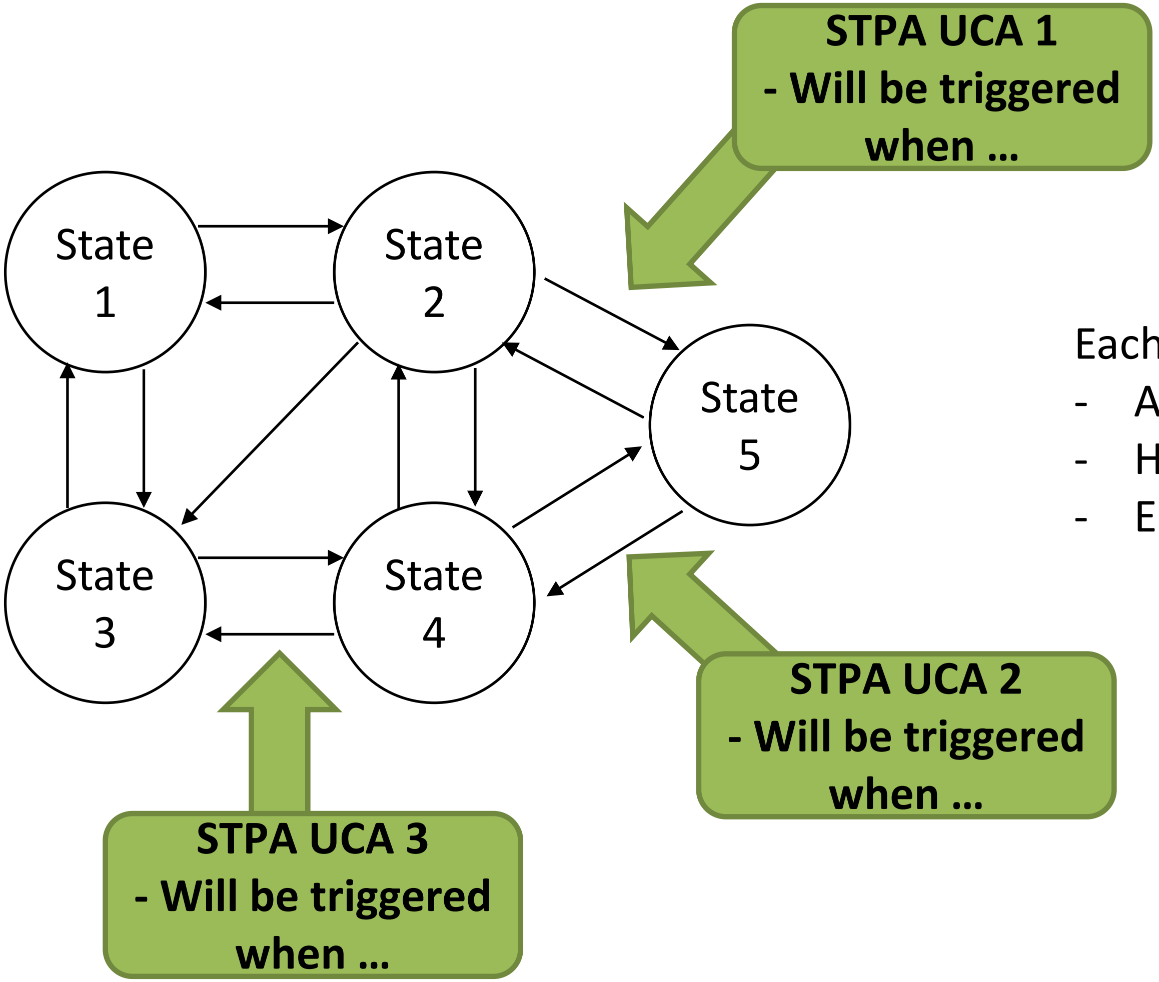
STPA analyzes process behaviors

STPA analyzes automated behaviors

STPA analyzes process behaviors

This is an oversimplified example only!

STPA analyzes hazardous state transitions triggered by both intended functions and unintended behaviors


STPA UCA 1
- Will be triggered when …
State 1
State 2
State 5
State 3
State 4
STPA UCA 2
- Will be triggered when …
STPA UCA 3
- Will be triggered when …

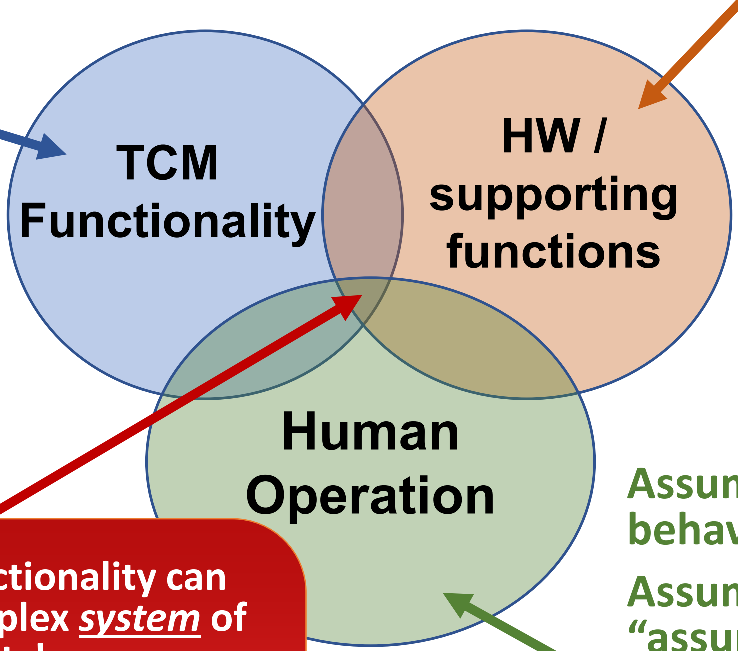
Each state/context includes:

- Automation
- Humans
- Environment

Hard-to-catch issues

You may analyze many failures of intended functions or components.

Reality: TCM can function as designed and still interact in ways that create a hazard.



Analysis of supporting functions may not be informed by specific TCM errors that may exist (analyzed separately or generically).

Single-point failures may be identified & assessed while assuming that the complex, intended TCM functions are correct and complete (analyzed separately).

Single-point HW failures may appear to be mitigated!

Reality: A single-point failure is actually catastrophic given certain indirect TCM and human interactions.

Assumptions made about human behaviors and operating envelope.

Assumptions may not be considered "assumptions" until after a concern is raised.

Reality: Specific unforeseen but normal human behaviors can indirectly create unexpected TCM and HW interactions! (e.g., quick throttle movement)

New, unplanned functionality can emerge from the complex ***system*** of components!

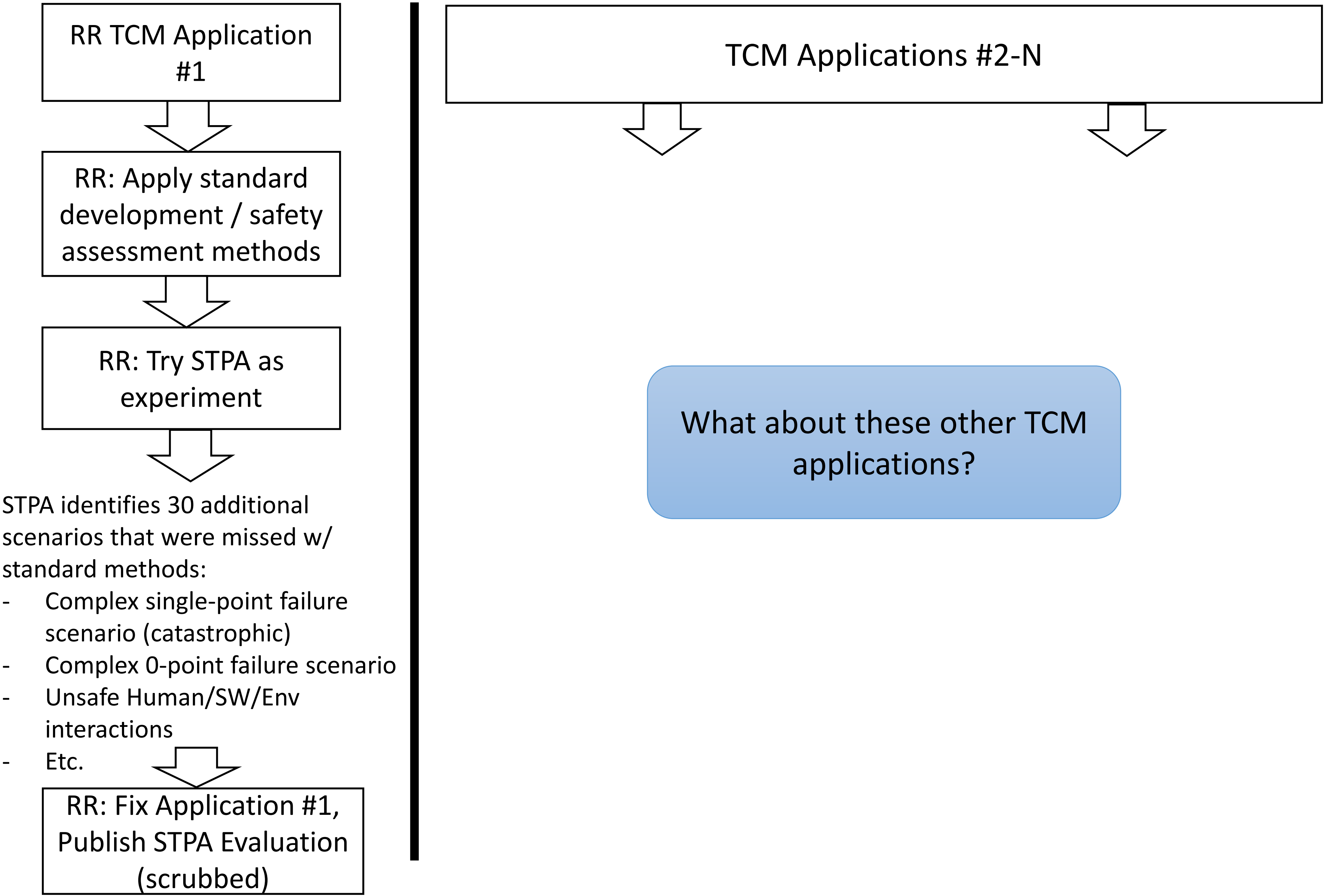
STPA finding: A "No Safety Effect" single point HW failure is actually catastrophic in a particular (normal) environment with a particular (normal) human action!

It can be easy to overlook holistic system problems by looking at individual failures & errors

Summary

- Role of air/ground switch failure states was not fully recognized during the original design process
  - Inputs protecting against inadvertent activation had a common mode failure case
- Changed environment during flight at altitude allows Thrust Control Malfunction (TCM) detection
- STPA analysis identified
  - The inadequate operation of the air-ground switch
  - The TCM protection process output contributing the unsafe control action of inadvertent engine shutdown
  - Relative to the original design work STPA identified approximately 30 additional items that required review including several design changes
- Although a “novel” approach (STPA) applied techniques slightly different from the examples, the ability to explain the approach and understand the results drove consensus for the solutions
- Improved software now in customer’s flight tests with no TCM functional issues. Aircraft level approval for both engines in 2014.

Many Aircraft Add TCM Functionality



RR TCM Application #1

RR: Apply standard development / safety assessment methods

RR: Try STPA as experiment

STPA identifies 30 additional scenarios that were missed w/ standard methods:

- Complex single-point failure scenario (catastrophic)
- Complex 0-point failure scenario
- Unsafe Human/SW/Env interactions
- Etc.

RR: Fix Application #1, Publish STPA Evaluation (scrubbed)

TCM Applications #2-N

What about these other TCM applications?

TCM in Other Aircraft

- Many aircraft add similar/identical TCM functionality.
    - Airbus Model A318-100, A340-500, A340-600 airplanes; Embraer EMB-135BJ, EMB-145XR, ERJ 170-100, ERJ 170-200, ERJ 190-100, ERJ 190-200 airplanes; Boeing 717, 737, 747, 757, 767, 777, 787, DC-9, MD-90, MD-88, MD-11 airplanes; and Gulfstream GIV-X, 0280, GV, GV-SP, and GVI airplanes
- STPA is not used.
- Standard development/safety processes are followed.
- FAA evaluates and approves TCM for other aircraft (without STPA):
    - TCMA "logic that identifies and safely accommodates any sustained, substantial discrepancy […] has been implemented"
    - … "will not adversely affect safety"
    - "all practicable actions have been taken to minimize the adverse effects on safety"

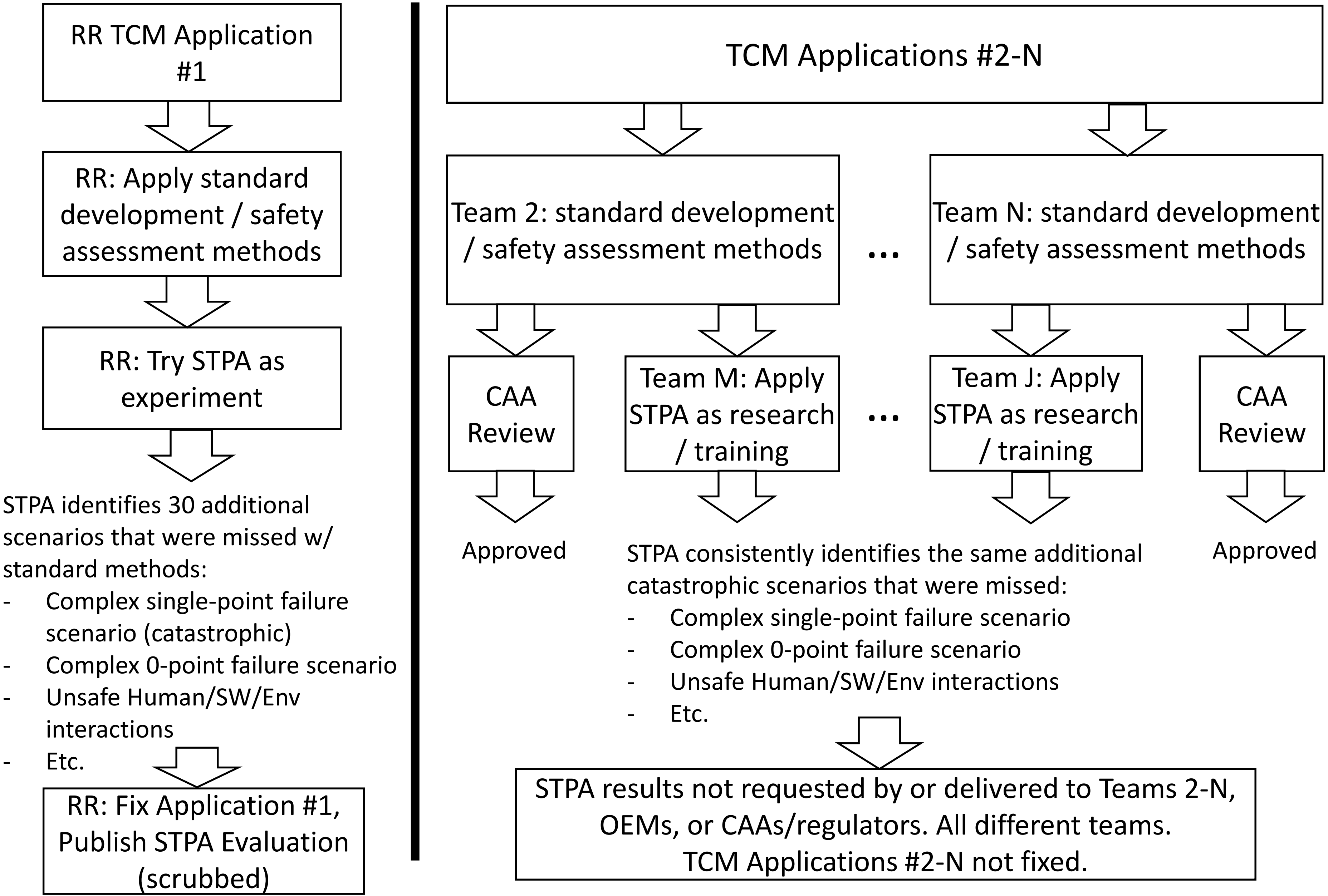
For example, see: Regulatory Docket No. FAA-2016-8059, Grant of Exemption, May 2, 2017

STPA is replicated by other groups

- INTA and other groups independently apply STPA to other engine controls that include TCM functionality
    - STPA applied without knowledge of the original study results
    - Each group identified same TCM flaws using STPA:
        - Example STPA Scenario: [Env. State X] & [Crew action Y] & [Process Z], which are expected conditions in flight, can together cause all redundant TCMs to trigger dual engine shutdown with no engine malfunction.
            - Unsafe interactions between humans, software, physical engines, and environment
        - Identified TCM <u>intended</u> functions that are unsafe
        - Identified catastrophic 2-failure scenarios, 1-failure scenarios, and 0-failure scenarios that were overlooked using standard processes
        - Identified undocumented assumptions about environment (identified with STPA)
        - Identified undocumented assumptions about human actions (identified with STPA)
    - STPA was applied in ~8 hours

- STPA performed on TCM as internal STPA research & education, not a certification project
    - These STPA results are not delivered to regulators or OEMs
    - Regulators and OEMs do not request STPA for TCM
    - <u>STPA is not used for TCM certification</u>

Many Aircraft Add TCM Functionality



RR TCM Application #1

RR: Apply standard development / safety assessment methods

RR: Try STPA as experiment

STPA identifies 30 additional scenarios that were missed w/ standard methods:

- Complex single-point failure scenario (catastrophic)
- Complex 0-point failure scenario
- Unsafe Human/SW/Env interactions
- Etc.

RR: Fix Application #1, Publish STPA Evaluation (scrubbed)

TCM Applications #2-N

Team 2: standard development / safety assessment methods

…

Team N: standard development / safety assessment methods

CAA Review

Team M: Apply STPA as research / training

…

Team J: Apply STPA as research / training

CAA Review

Approved

Approved

STPA consistently identifies the same additional catastrophic scenarios that were missed:

- Complex single-point failure scenario
- Complex 0-point failure scenario
- Unsafe Human/SW/Env interactions
- Etc.

STPA results not requested by or delivered to Teams 2-N, OEMs, or CAAs/regulators. All different teams.
TCM Applications #2-N not fixed.

Dual Engine Flameouts

- Many aircraft add TCM software without STPA

- 2016: TCM causes dual engine flameouts on aircraft certified without STPA
  - Fortunately, no accident—only causes delays
  - Not widely known or publicized
  - The TCM flaws exactly match the STPA findings by other teams years earlier, but nobody realizes this
  - No corrective actions implemented

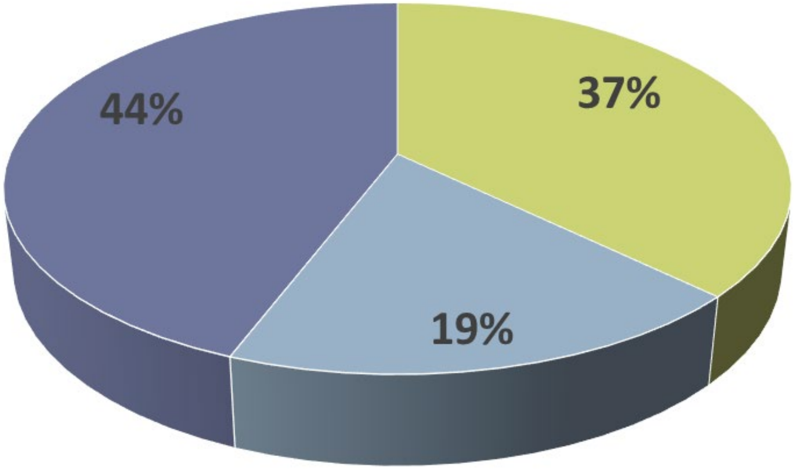
Dual Engine Flameouts (again)

- Many aircraft add TCM software without STPA

- 2018: TCM causes dual engine flameouts on aircraft certified without STPA (again!)
  - Fortunately, no accident
  - Aircraft landed and is stuck on runway, crew cannot restart engines
  - Maintenance cannot locate problem—no components have failed
  - Eventually, investigation uncovers the TCM flaws
    - The TCM flaws exactly match the STPA findings from 4 years prior
    - The flaws had been missed (again) without STPA
  - Corrective actions are implemented
    - All corrective actions exactly match the STPA-generated requirements from 4 years prior

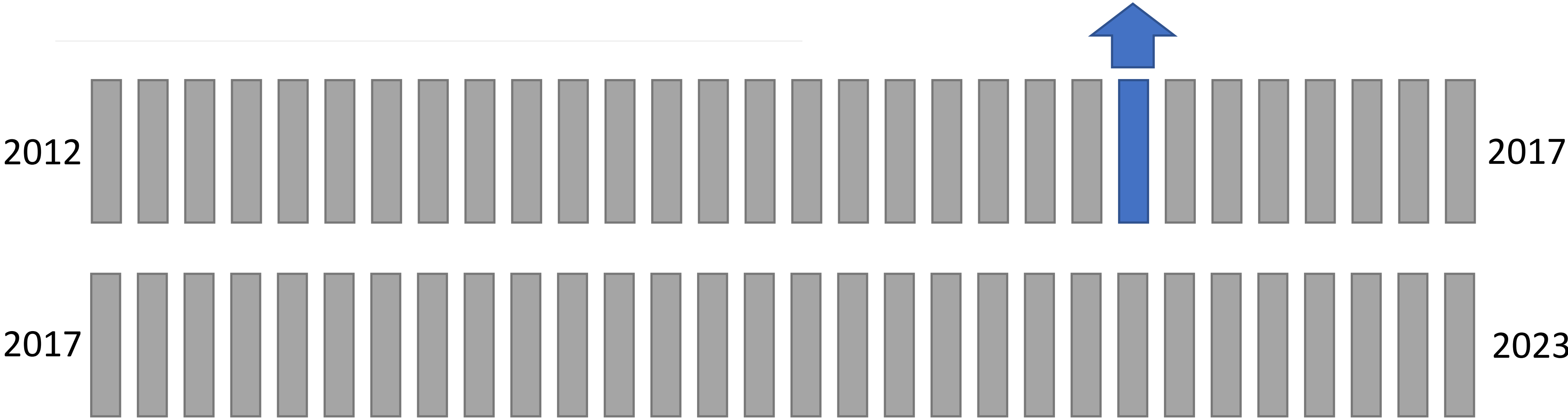
Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops

STPA Results



EMBRAER

- 🟦 Captured with existing standard processes
- ▨ Captured only in advanced stages, STPA found earlier
- 🟩 Captured only with STPA



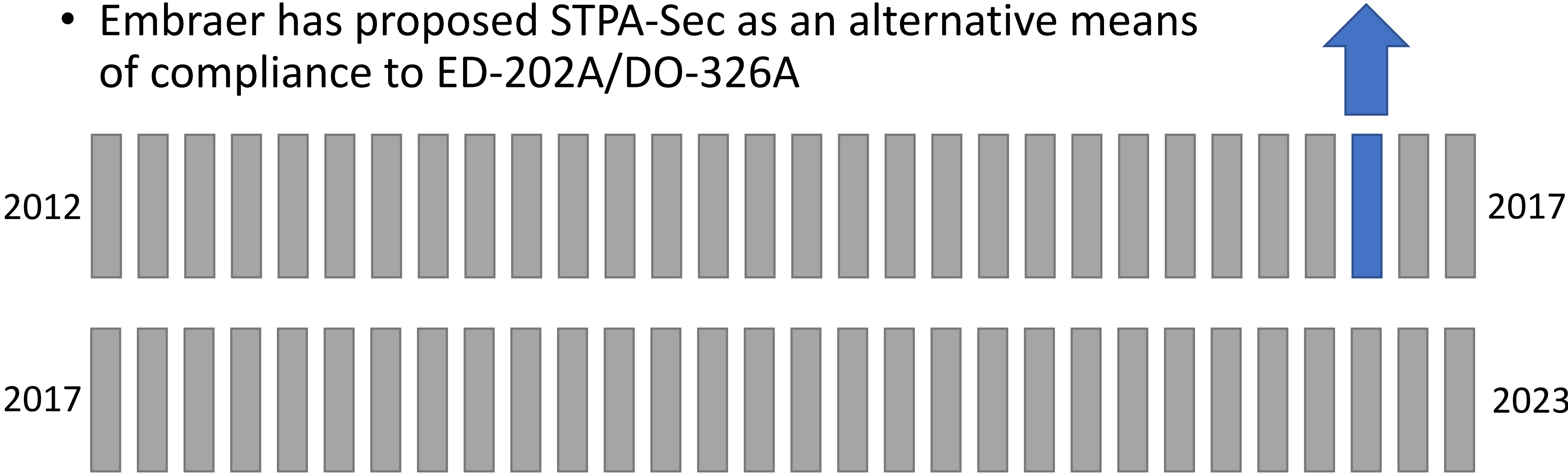
D. Ribeiro, A Systems Approach to the Development of an Aircraft Smoke Control System, 2016, 5th STAMP/STPA Workshop

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops

EMBRAER

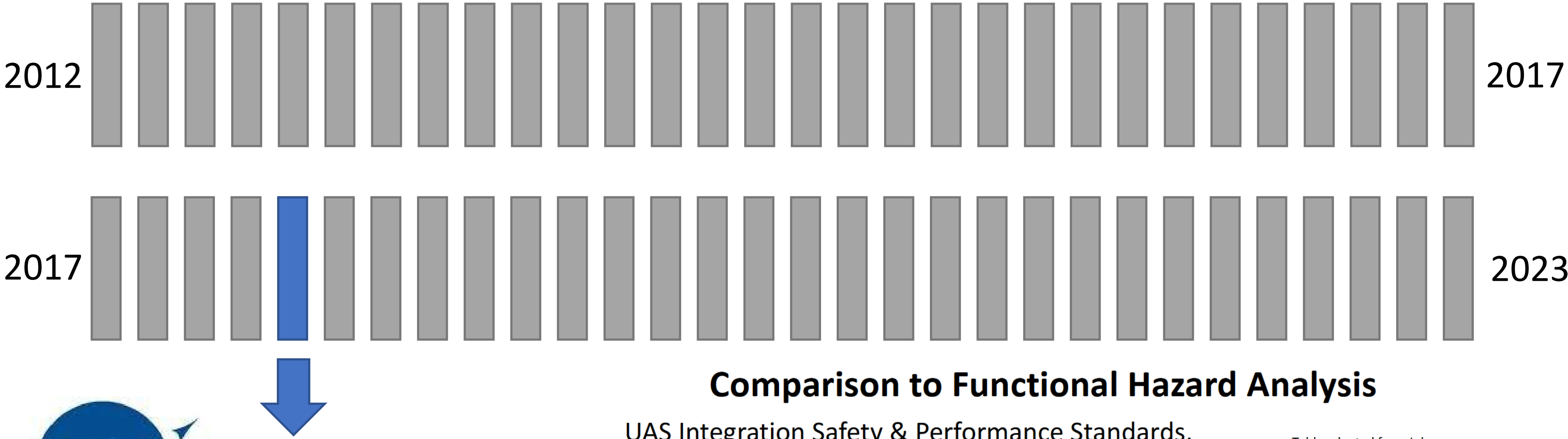
Conclusions:

- STPA shows to be an alternative method to current ED-203/DO-356 implementation
- STPA control structure development identifies the security environment and security perimeter
- Security Risk Assessment activity is covered during STPA
- Embraer has proposed STPA-Sec as an alternative means of compliance to ED-202A/DO-326A



D. Pereira, C. Hirata, R. Pagliares, F. de Lemos, STPA-Sec for Security of Flight Management System, 2017, 6th STAMP/STPA Workshop

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops



MIT AEROASTRO

U.S. AIR FORCE

Comparison to Functional Hazard Analysis

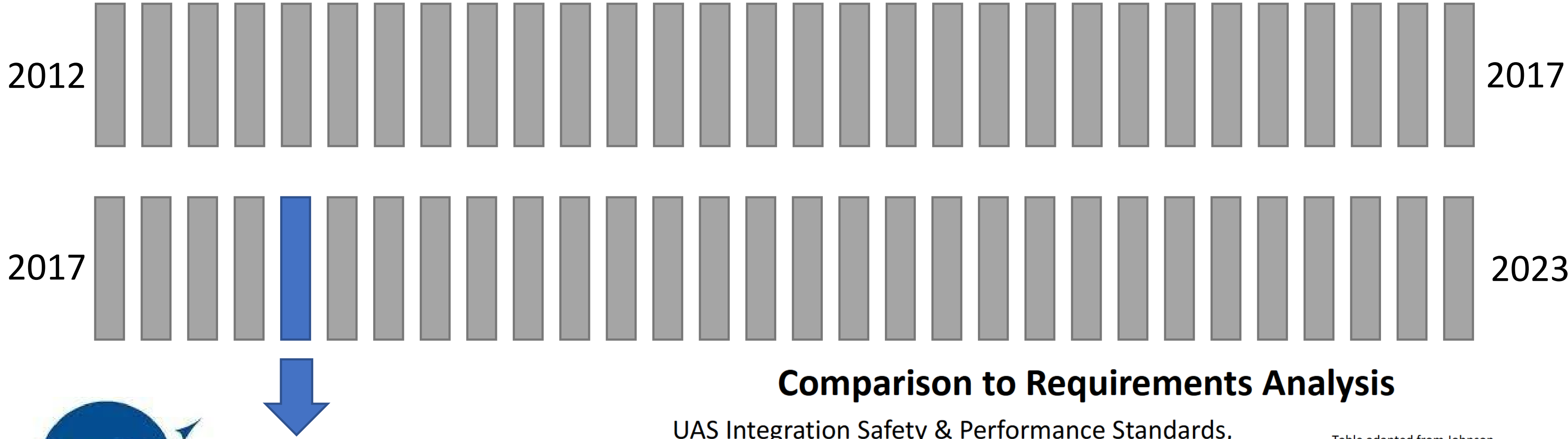
UAS Integration Safety & Performance Standards, DO-344 (RTCA SC-203, 2013)

Table adapted from Johnson 2017, p. 132. © by MIT.

Coordination Elements	Hazardous Coordination Scenarios	
	DO-344 / FHA	STPA-Coordination
1. Coordination Goals	0	3
2. Coordination Strategy	0	46
3. Decision Systems	0	3
4. Communications	1	16
5. Group Decision-Making	0	12
6. Observation of Common Objects	7	18
7. Authority, Responsibility, Accountability	0	23
8. Common Understanding	30	46
9. Predictability	10	27
Total Hazardous Coordination Scenarios	**48**	**194**

K. Johnson, Extending Systems-Theoretic Safety Analyses for Coordination, 2017, 6th STAMP/STPA Workshop

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops



MIT AEROASTRO

U.S. AIR FORCE

Comparison to Requirements Analysis

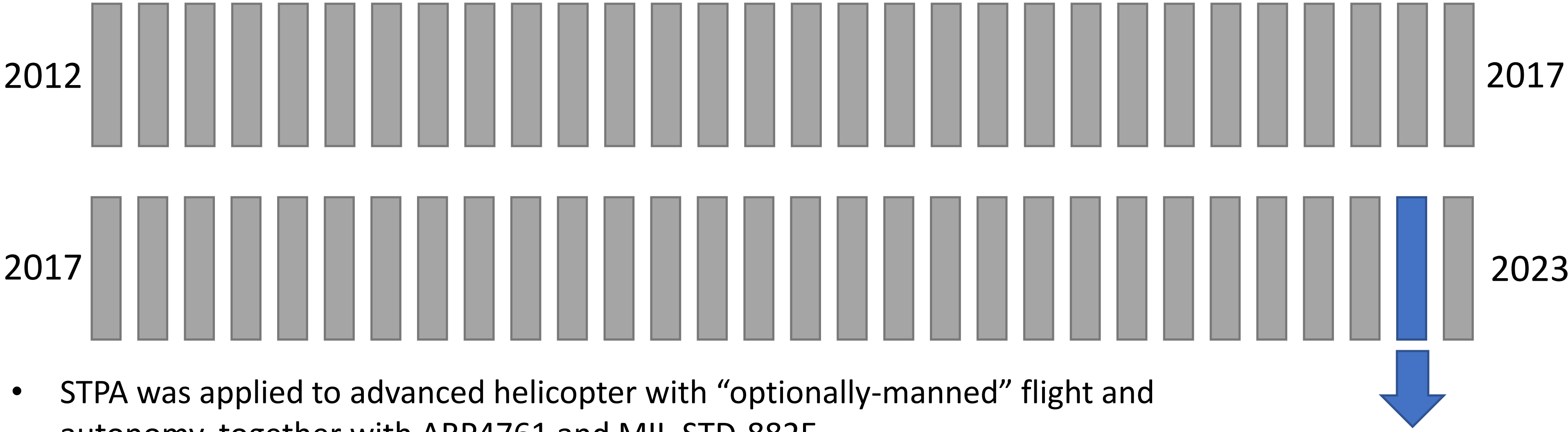
UAS Integration Safety & Performance Standards, DO-344 (RTCA SC-203, 2013)

Table adapted from Johnson 2017, p. 136. © by MIT.

Coordination Elements	Coordination Recommendations	
	DO-344 / Req.	STPA-Coordination
1. Coordination Goals	0	2
2. Coordination Strategy	4	53
3. Decision Systems	0	2
4. Communications	2	22
5. Group Decision-Making	0	13
6. Observation of Common Objects	4	25
7. Authority, Responsibility, Accountability	0	33
8. Common Understanding	19	37
9. Predictability	3	29
Total Coordination Recommendations	**32**	**216**

K. Johnson, Extending Systems-Theoretic Safety Analyses for Coordination, 2017, 6th STAMP/STPA Workshop

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops

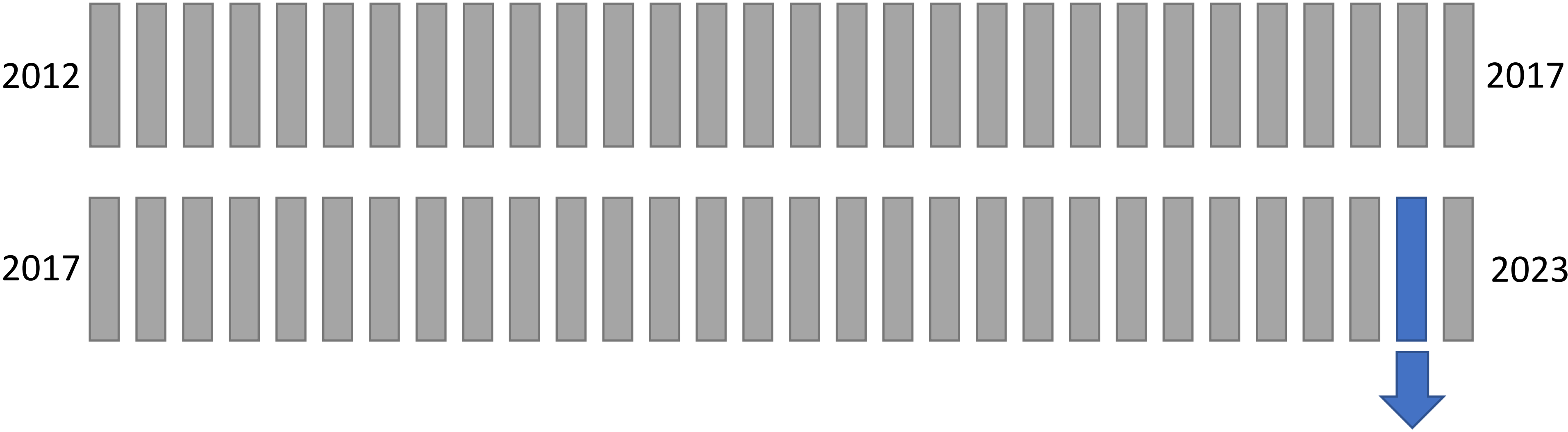


- STPA was applied to advanced helicopter with “optionally-manned” flight and autonomy, together with ARP4761 and MIL-STD-882E
- Conclusions:
    - STPA was effective in extending the standard system safety framework to strengthen human factors considerations.
    - STPA applied at aircraft level and system level.
    - Key benefits: Improved hazard identification, risk assessment, risk mitigation, requirements identification, safety verification, and identification of critical test cases.
    - STPA both extends and integrates with system safety activities.
    - STPA was found to be most powerful where traditional practices were weakened by context (e.g., lack of established design maturity, complexity of interactions).

Bell Helicopter
A Textron Company

L. Mutuel, A Structured and Comprehensive Air Vehicle Risk Assessment, 2022, 11th STAMP/STPA Workshop

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops



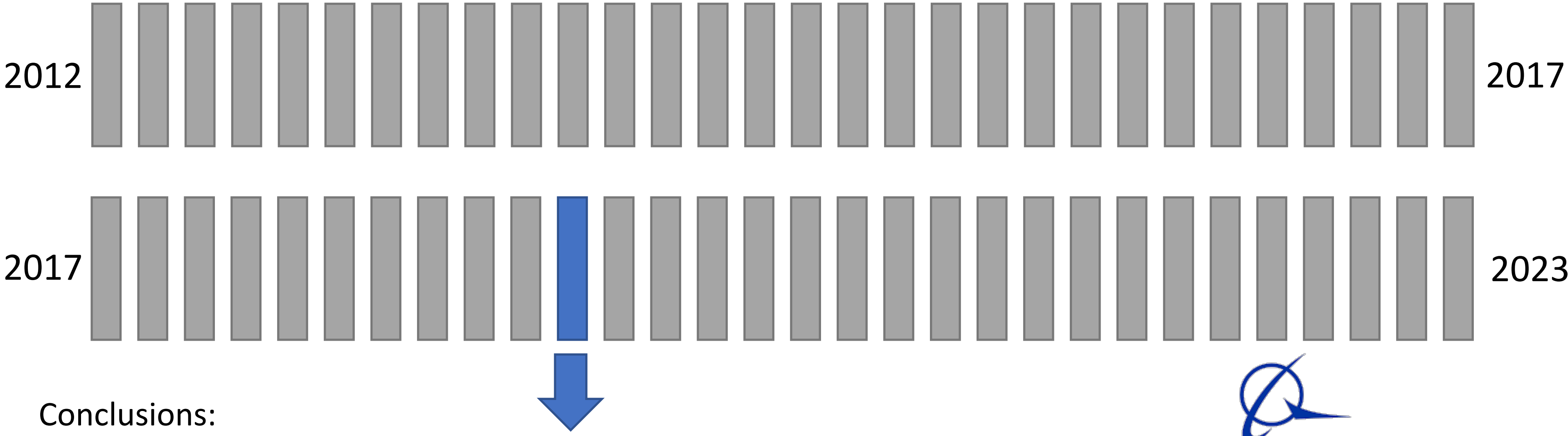
Conclusions:

- Attempted to add STPA results into the existing standard approaches.
- Some complex unsafe behaviors identified by STPA could not be represented by standard processes like FHA, FTA, CMA, etc.

Bell Helicopter
A Textron Company

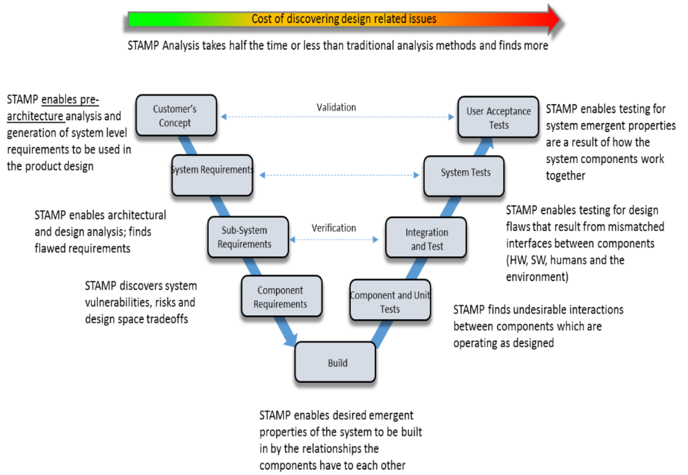
L. Mutuel, A Structured and Comprehensive Air Vehicle Risk Assessment, 2022, 11th STAMP/STPA Workshop

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops



Conclusions:

- STPA identified additional potential design flaws including:
  - 54 Pilot/Flight Management
  - 84 Avionics System
  - 23 Flight Control Computing system (FCCS) unsafe actions
  - 34 Flight Control Actuation
- Greatest STPA benefits: complex systems with hardware, software and human interaction
- STPA provides different perspective than industry standard tools, e.g., failure modes & effects analysis
- Relatively simple & straightforward to use



STAMP Analysis takes half the time or less than traditional analysis methods and finds more

STAMP enables pre-architecture analysis and generation of system level requirements to be used in the product design

STAMP enables architectural and design analysis; finds flawed requirements

STAMP discovers system vulnerabilities, risks and design space tradeoffs

STAMP enables testing for system emergent properties are a result of how the system components work together

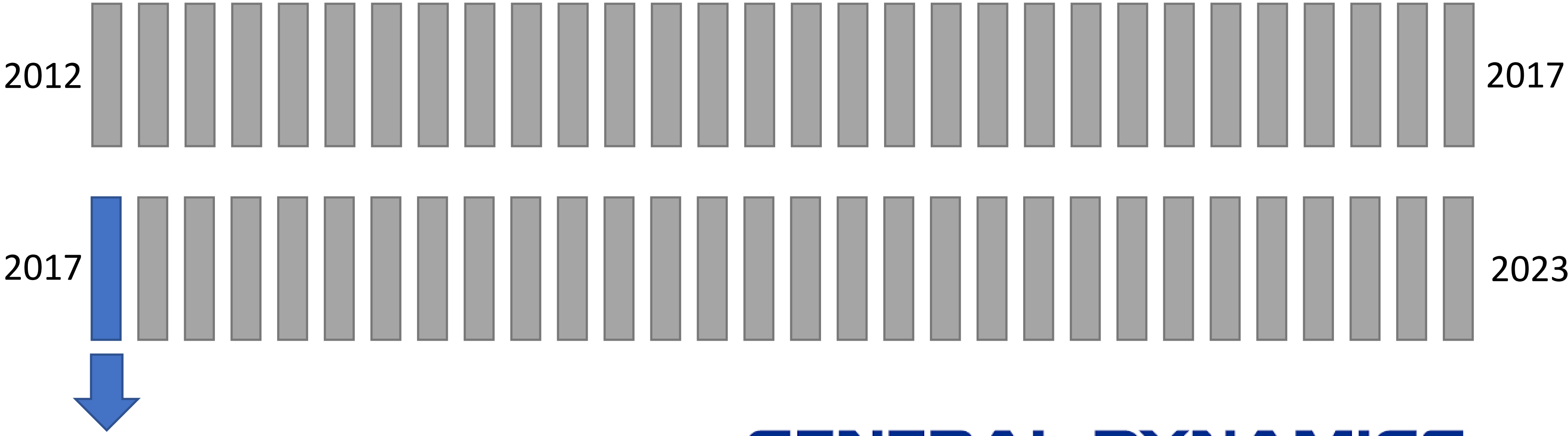
STAMP enables testing for design flaws that result from mismatched interfaces between components (HW, SW, humans and the environment)

STAMP finds undesirable interactions between components which are operating as designed

STAMP enables desired emergent properties of the system to be built in by the relationships the components have to each other

M. Nance, Overview of STAMP and STPA for Product and Production Systems Engineering, 2019, 8th STAMP/STPA Workshop

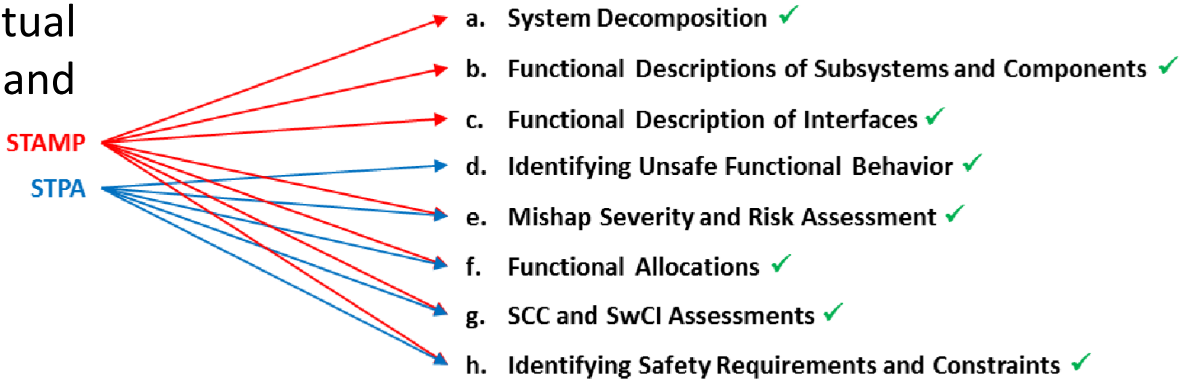
Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops



GENERAL DYNAMICS
Mission Systems

Conclusions:

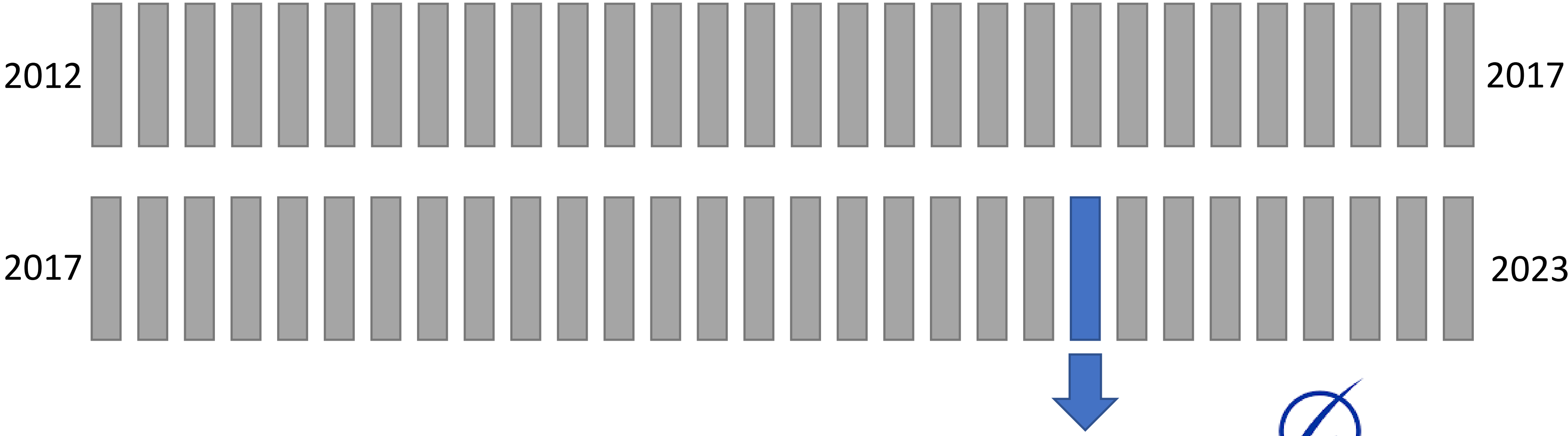
- STPA provides the needed conceptual rigidity and contextual flexibility to perform accurate and complete Functional Hazard Analysis (FHA) consistently



a. System Decomposition ✓
b. Functional Descriptions of Subsystems and Components ✓
c. Functional Description of Interfaces ✓
d. Identifying Unsafe Functional Behavior ✓
e. Mishap Severity and Risk Assessment ✓
f. Functional Allocations ✓
g. SCC and SwCI Assessments ✓
h. Identifying Safety Requirements and Constraints ✓

N. Malloy, Integrating STAMP-based Hazard Analysis with MIL-STD-882E Functional Hazard Analysis, 2017, 6th STAMP/STPA Workshop

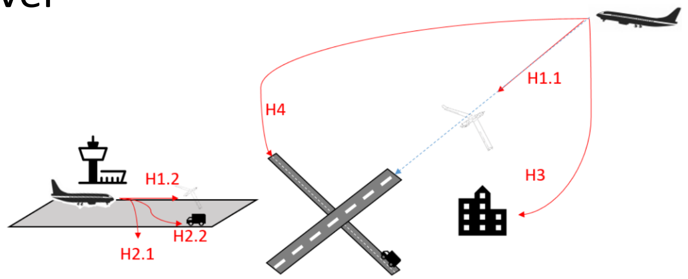
Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops



STPA applied to small Uncrewed Aircraft Systems in terminal airspace

Conclusions:

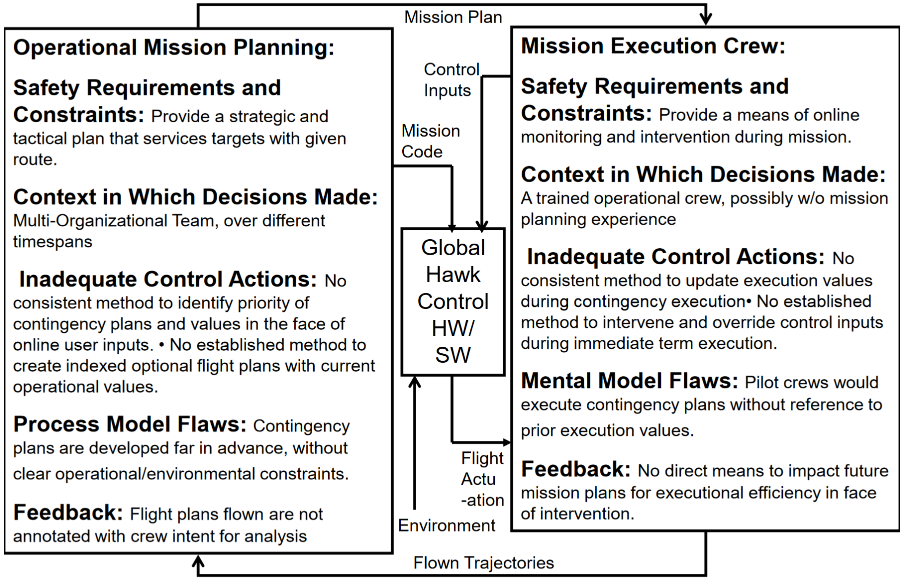
- STPA proved to be an effective analysis tool for this study
- Complex interactions managed through relatively high level of abstraction
  - Allowed analysis of interactions without necessarily understanding internal details of each element
  - Hardware, software, and human elements



P. Stanley, V. Barraquero, STPA Evaluation of Potential Conflicts between Large Commercial Air Traffic and Small Uncrewed Aircraft Systems in the Terminal Airspace, 2021, 10th STAMP/STPA Workshop

Sample of STPA Evaluations in Aviation Presented at Past MIT Workshops

STPA was applied to safety of new unmanned aircraft. Control structure includes software, hardware, crew, operational planning, and contingency planning and execution



Operational Mission Planning:

Safety Requirements and Constraints: Provide a strategic and tactical plan that services targets with given route.

Context in Which Decisions Made: Multi-Organizational Team, over different timespans

Inadequate Control Actions: No consistent method to identify priority of contingency plans and values in the face of online user inputs. • No established method to create indexed optional flight plans with current operational values.

Process Model Flaws: Contingency plans are developed far in advance, without clear operational/environmental constraints.

Feedback: Flight plans flown are not annotated with crew intent for analysis

Mission Execution Crew:

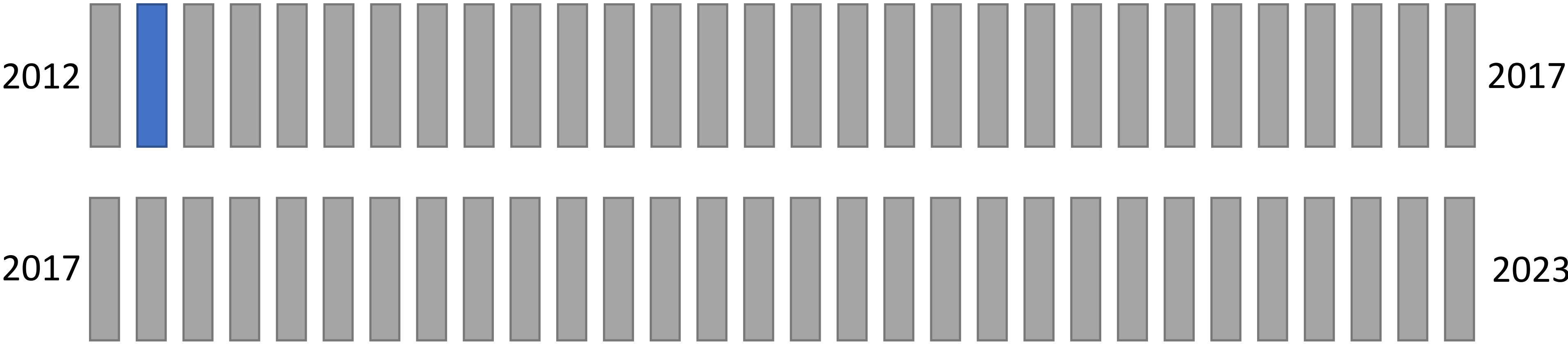
Safety Requirements and Constraints: Provide a means of online monitoring and intervention during mission.

Context in Which Decisions Made: A trained operational crew, possibly w/o mission planning experience

Inadequate Control Actions: No consistent method to update execution values during contingency execution• No established method to intervene and override control inputs during immediate term execution.

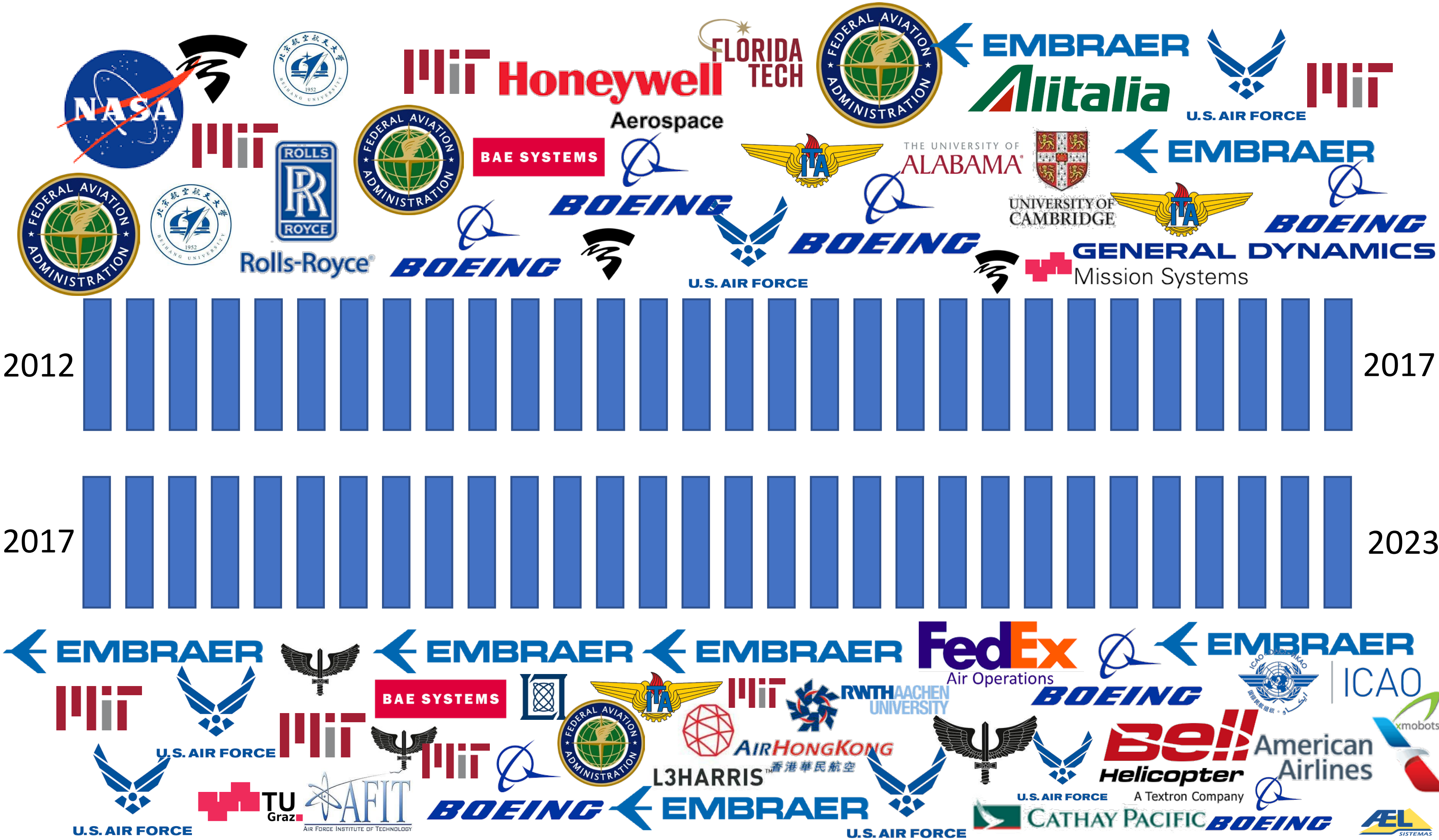
Mental Model Flaws: Pilot crews would execute contingency plans without reference to prior execution values.

Feedback: No direct means to impact future mission plans for executional efficiency in face of intervention.



N. Neogi, Integrating Uninhabited Aerial Systems into the NAS, 2012, 1st STAMP/STPA Workshop

Industry evaluations available at mit.edu/psas


NASA
MIT
Rolls-Royce
Federal Aviation Administration
BAE SYSTEMS
Honeywell Aerospace
Florida Tech
Boeing
ITA
U.S. Air Force
Embraer
Alitalia
The University of Alabama
University of Cambridge
General Dynamics Mission Systems
FedEx Air Operations
ICAO
RWTH Aachen University
Air Hong Kong 香港華民航空
L3Harris
Bell Helicopter A Textron Company
American Airlines
Cathay Pacific
TU Graz
AFIT Air Force Institute of Technology
AEL Sistemas
xmobots