# Product Assurance in the Model-Based System Engineering Ecosystem: Performing STPA during Preliminary Design

Timothy Russell
Jennifer Schlotter
Kyle Ryan

September 2026

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

## Timothy Russell



Associate Technical Fellow,
System Safety Engineering,
Boeing Global Services

Tim joined Boeing in 2013 and is currently an Associate Technical Fellow in System Safety Engineering for Boeing Global Services. He previously held System Safety and Reliability/Maintainability roles on multiple platforms in Boeing Defense, Space, & Security's Vertical Lift division.

Before joining Boeing, Tim worked in System Safety/Reliability at United Technologies from 2004-13 and earned a bachelor of science in Mechanical Engineering & History minor from the University of Connecticut in 2005.

Tim presently resides in Delaware with his dogs (Odin, Zora (pictured), Oakley) and cat (Loki). Outside of work, he enjoys travel, weightlifting, video games, and nature.

TABRussell@gmail.com

## Jennifer Schlotter



Boeing Designated Expert,
System Safety Engineering,
Boeing Defense, Space & Security

Jen has been with Boeing for almost 30 years and is currently a Boeing Designated Expert in System Safety for Boeing Defense and Space. She has focused on System Safety support to Boeing's human spaceflight programs such as NASA's Space Launch System and Boeing's Commercial Crew vehicle, the Starliner CST-100.

Jen has supported programs such as the Joint Multi-Role (JMR) Tech Demonstrator Program, V-22 Osprey, and Boeing NeXt's Cargo Air Vehicle which provided flying X-Wing drones for entertainment in Disney World.

Jen grew up in Philadelphia, PA and holds a B.S in Mechanical Engineering from Drexel University. She is currently pursuing a Master of Space Operations from Embry-Riddle.

## Kyle Ryan






Associate Technical Fellow,
Socio-Technical Systems Engineering,
Boeing Defense, Space & Security

Kyle joined Boeing in 2007 and is currently an Associate Technical Fellow in Socio-technical Systems Engineering for Boeing. His primary role involves supporting STAMP-related projects and initiatives across the enterprise to enable engineering teams to apply systems thinking to better understand how social, human, and technical factors intersect in complex systems. He is an active member of the SAE G-48 STPA Task Force and S-18 Safety Committee developing industry guidance on STPA.

Kyle has BS in Aero/Astro Engineering from Purdue University and a Masters in Systems and Industrial Engineering from University of Washington. He currently resides in TN where most of his time is spent with his wife renovating their home and keeping up with their 7 kids.

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Agenda

- Introduction
- Control Structure & Requirements
- Findings & Impact
- Future Considerations
- Conclusion

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

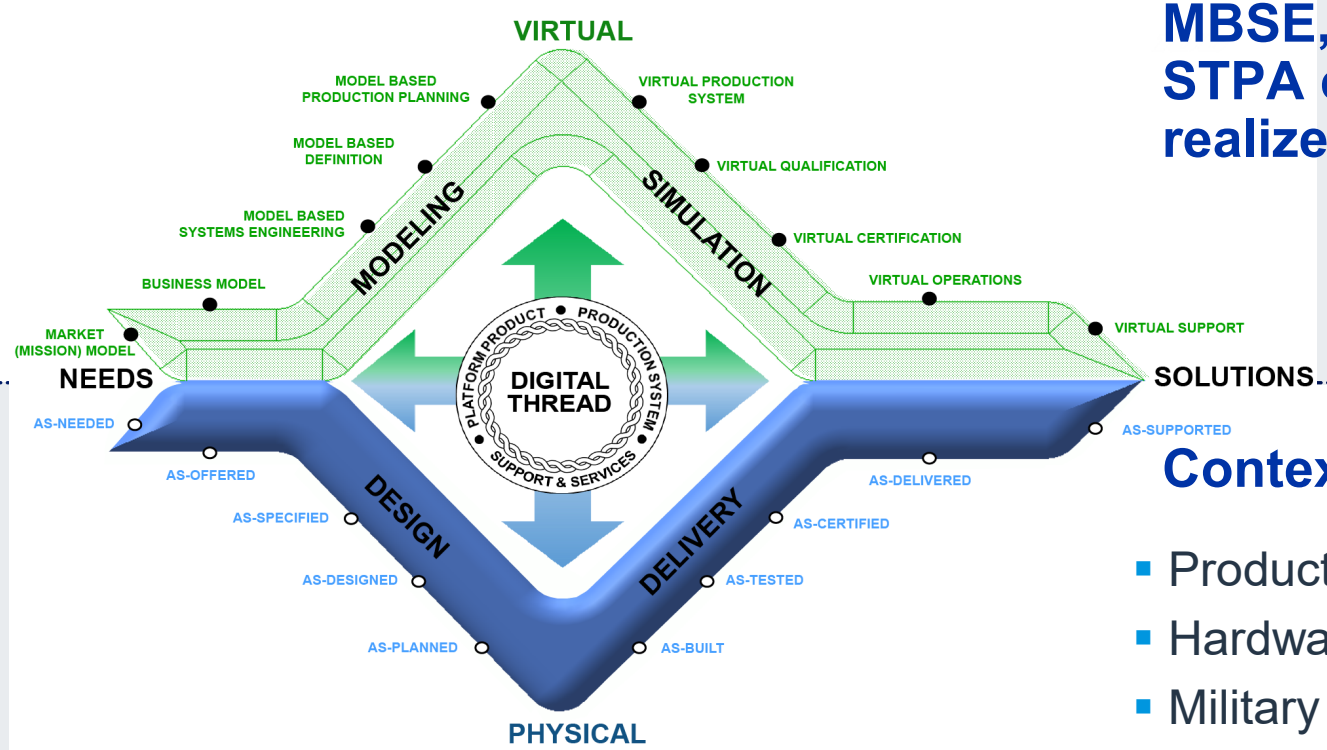
# Introduction

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

**Boeing is reimagining how we design, build, test, and support our products/services across the full lifecycle.**

**Integral to this is a unified, comprehensive digital ecosystem in MBSE, an environment STPA can uniquely realize benefits within.**

## Evolution of System Engineering (SE) to Model Based Engineering (MBE)




## Product Assurance

- System Safety (SS)
- Mission Assurance (MA)
- Product Support (PS)
- Reliability/Availability/Maintainability (RAM)

## Contexts

- Products and Services
- Hardware and Software
- Military and Civilian
- Full Lifecycle (Development to Disposal)

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Presentation Objective

- Discuss STPA in MBSE
  - Military Rotorcraft Platform (MRP) Early Lifecycle
  - Initial model completed for System Functional Review (SFR) program milestone
  - Imported into DESE-CAMEO for MBSE integration and government customer delivery

- Observations
  - STPA identified **~50%** more specific, measurable requirements to prevent erroneous behavior
  - STPA's discovery of lower-level requirements earlier than traditional analyses
  - Integration opportunities from performing STPA in MBSE
  - Late lifecycle use cases and other future considerations

**STPA is a Force Multiplier to Enhance Product Safety**

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Control Structure & Requirements

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Military Rotor Platform Effort

- STPA was conducted for engine controls
  - Explicitly called out by customer in program contract

- Impact - STPA enhances confidence in the safety analysis
  - STPA identified ~25% additional causes for a functional hazard analysis
  - FHA focus on loss or erroneous "FUNCTION" while STPA can more specifically identify the cause of erroneous behaviors not identified elsewhere
  - Example - "Command to STOP sent too late causing X"
    - FHA did not identify "Command to STOP ended too early/ intermittent/ causing X"



**STPA Identifies more CAUSES of Erroneous Functional Failure**

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

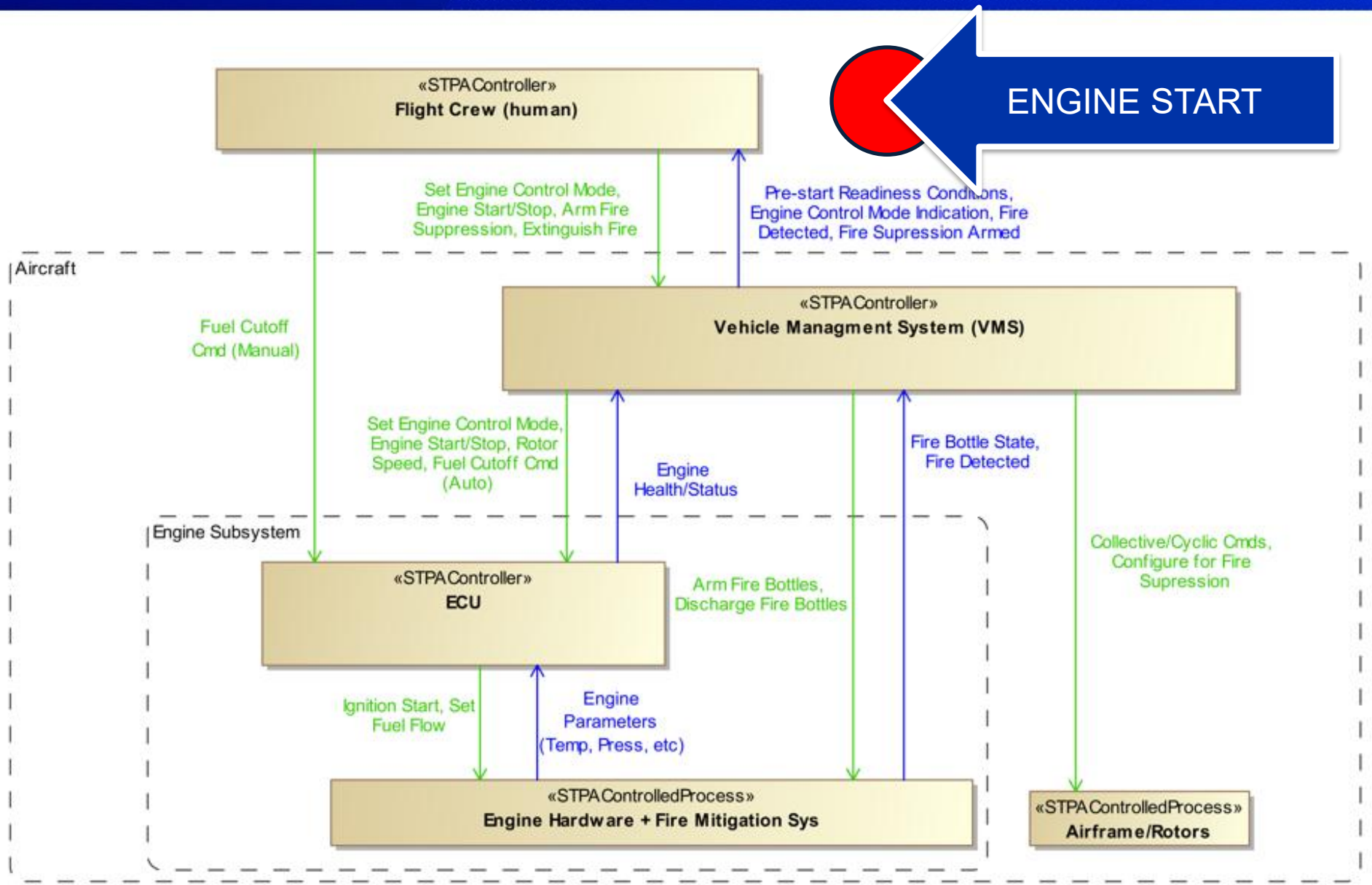
# The Story

- Example Function – Engine Start
  - Did STPA identify new Hazards or New Causes?
    - Comparison of SFHAs to the UCAs and Hazards of STPA
  - How did STPA driven requirements compare to traditionally derived requirements?
    - Comparison of FHA derived requirements to STPA derived requirements
- Hypothesis - STPA enhances confidence in the safety analysis
  - ***Did STPA Enhance the Safety Analysis?***
    - Of course it did.  Let's look at what we found

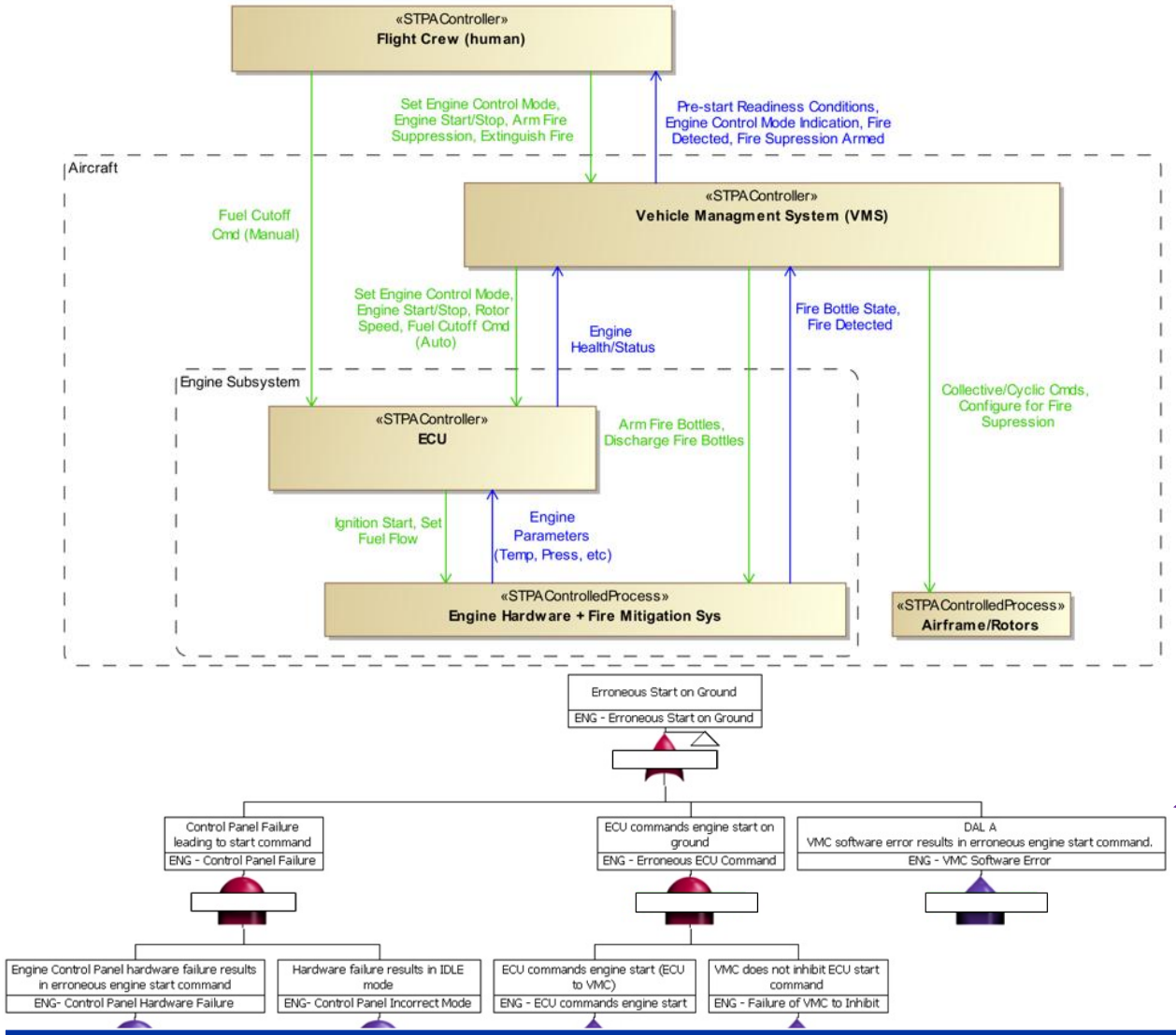


**Did STPA Enhance the Safety Analysis?**

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130).  Copyright © 2026 Boeing.  All rights reserved.




Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.




# FHA vs STPA

- Typically, an event is added to fault tree to provide initial DAL recommendation based on hazard severity

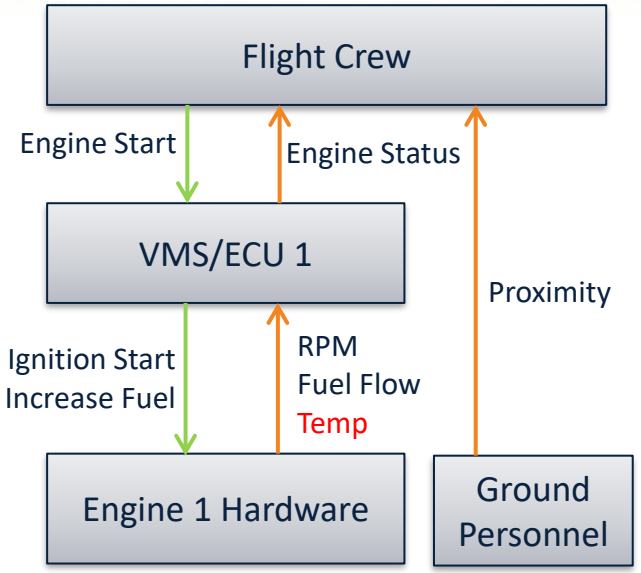
- STPA analysis with focus on interactions, better characterizes desired aircraft behavior to feed into aircraft software requirements

**STPA Identifies more CAUSES of Erroneous Functional Failure**

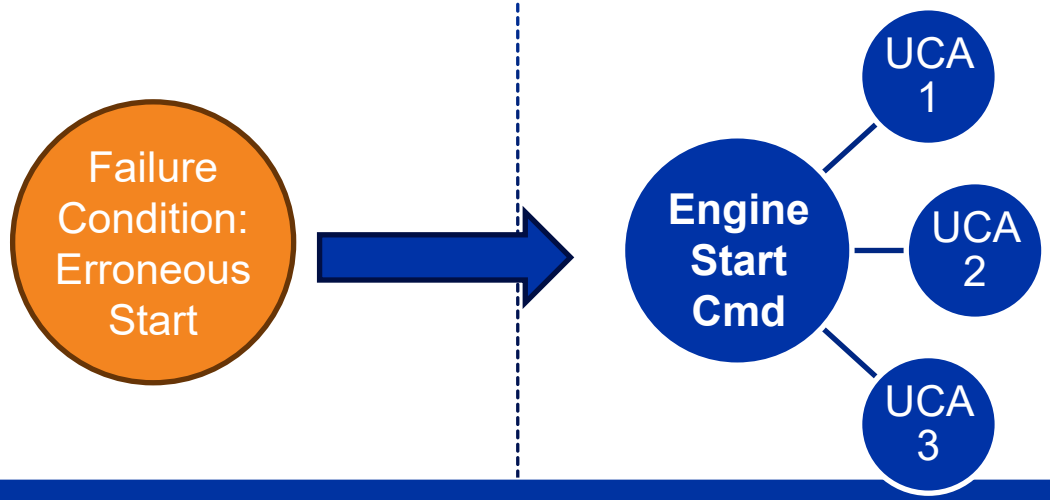
Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

## FHA Hazard

- Erroneous start command
  - *HOW is it ERRONEOUS?*
    - FHA does not specify what makes it erroneous
    - Relies on valid data/health monitoring
    - No timing consideration




Engine Control Abstracted Example




## STPA UCAs

- **UCA-1:** Flight Crew provides engine start command too soon after engine shut down, before engine has cooled down [H-1, H-8]
- **UCA-2:** Flight Crew provides engine start command for too long, and VMC doesn't inhibit command, and FADEC doesn't disengage starter [H-6, H-8]
- **UCA-3:** VMS provides engine start command too soon after aborted start, before fuel has drained, creating risk of engine fire [H-1]

**More Specific Unsafe Behavior = Better Requirements to Prevent Hazards**

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

## Traditional Safety

- Focus on failures
- Written to support the severity and can be probabilistic software safety requirements
- Extensive time to verify/validate PRA of software
- Rely on development assurance level of rigor pedigree as adequate safety/behavior of software

## STPA Safety

- STPA requirements unique to 37% of FHA IDs - traditional analysis miss
- 100% of STPA requirements were improvements upon the FHA derived requirements
- **100% were more specific and measurable software behavior requirements** to directly support system safety, to avoid undesirable outcomes

Failure Focus



~ 50% STPA requirements identified **not** likely to have been identified in traditional process

Behavioral requirement

**STPA is a Force Multiplier to Enhance Product Safety**

# Findings & Impact

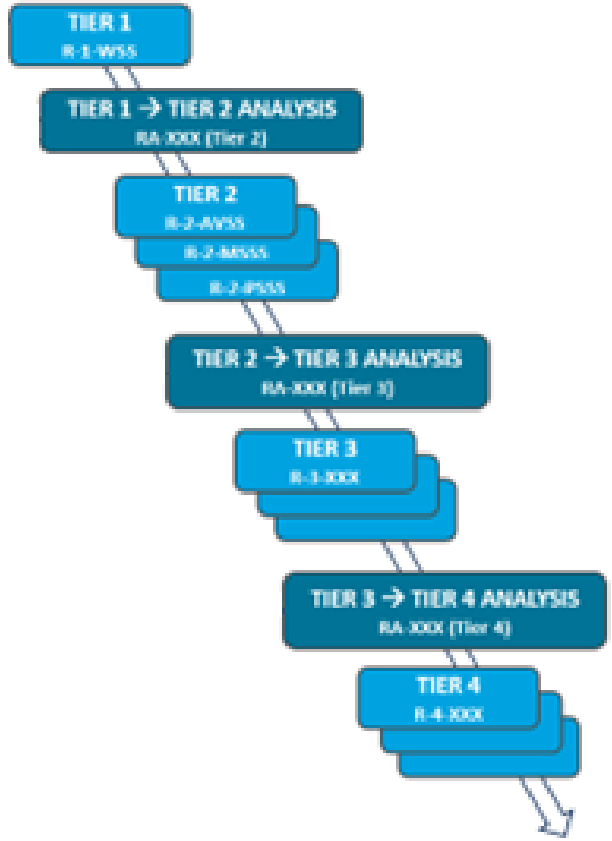
Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Requirements

- STPA effort undertaken while the program in general was focusing on tier 1 system & tier 2 segment requirements
  - Informed functional baseline
  - Drove updates to tier 1 & tier 2 requirements

- Lower-level requirements identified years earlier than expected
  - 44 tier 3 subsystem requirements identified 1-2 years earlier
  - 153 tier 4 or lower (component, etc.) requirements identified 1-4 years earlier
  - Years ahead of milestones like design reviews and flight tests where requirements baselines are planned to be very firm

- **STPA effectively supplemented traditional safety approaches by facilitating discovery of lower-level safety requirements earlier than they otherwise may have been identified**

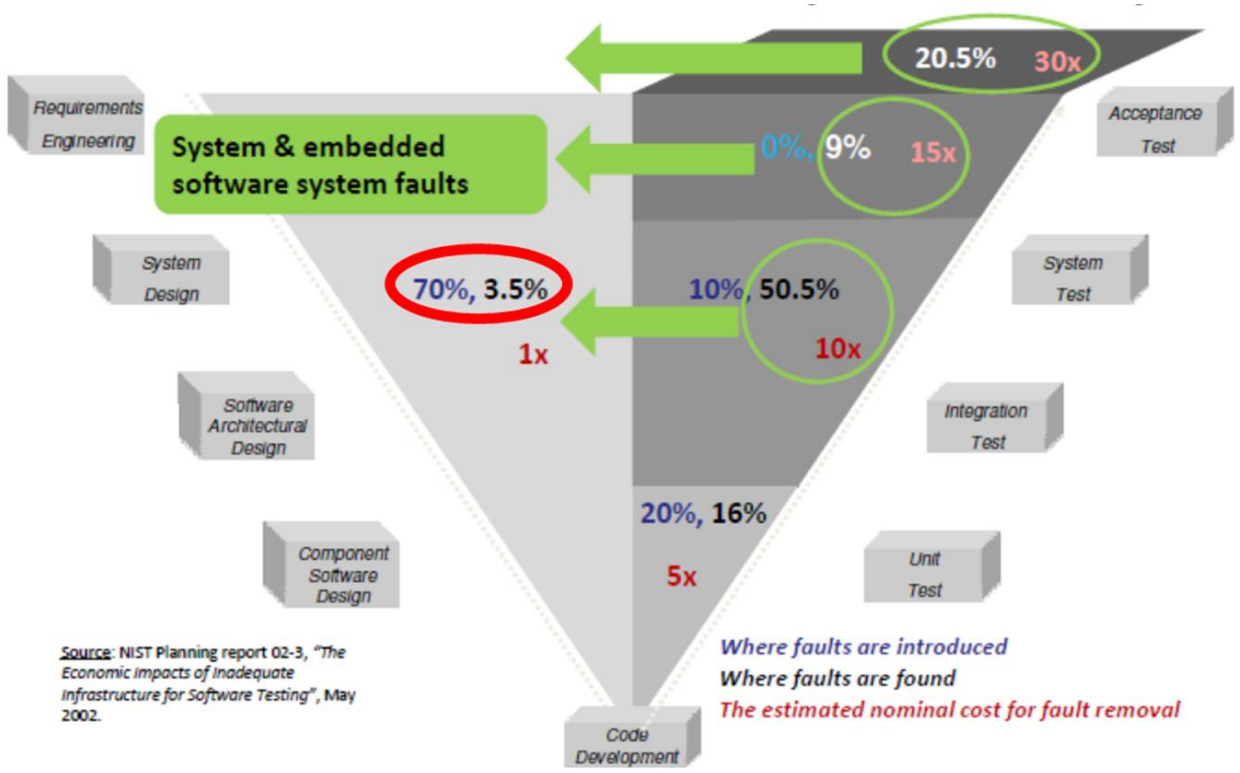



Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Cost Savings

- STPA was small percentage of safety program (6-digit personnel cost through initial analysis delivery)

- Cost avoidance
  - 44 tier 3 & 153 tier 4+ requirements identified
  - ~50% found to cause erroneous behavior => ~100 requirements
  - Distribution on left at $10k-100k baseline cost per requirement yield 7-8 digits in avoidance
  - Does not include cascading downstream effects from avoiding production/delivery delays and in-service impacts




- **STPA avoided cost, protected schedule, & reduced risk.**

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# What lessons were learned?

- Trained facilitator/analysts are essential
  - Handbook, training, and community of practice have evolved over the years
  - SAE documents (J3307, J3187's, etc.)

- Perform to appropriate level of abstraction
  - Going too low creates assumptions and rework while potentially losing signal in noise
  - Staying too high limits what the analysis can reveal

- Scope and constrain analysis
  - Focused control structure that considered architecture maturity
  - Hazards and losses narrowly defined for safety context

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# What went well?

- Leaning into early/proactive requirement identification
  - Focus on erroneous functionality
  - More hazards/causes => better requirements => stronger safety case

- Hybrid approach
  - Fusion of analog/in-person and digital/remote working
  - Build as much as possible first before importing into DESE-CAMEO

- Fruitful & insightful engagement
  - Boeing Design, Systems, & Cybersecurity learned STPA by doing it
  - Engine Supplier discovered opportunities for design improvement
  - Customer dialogue was greatly aided by DESE-CAMEO integration

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Future Considerations

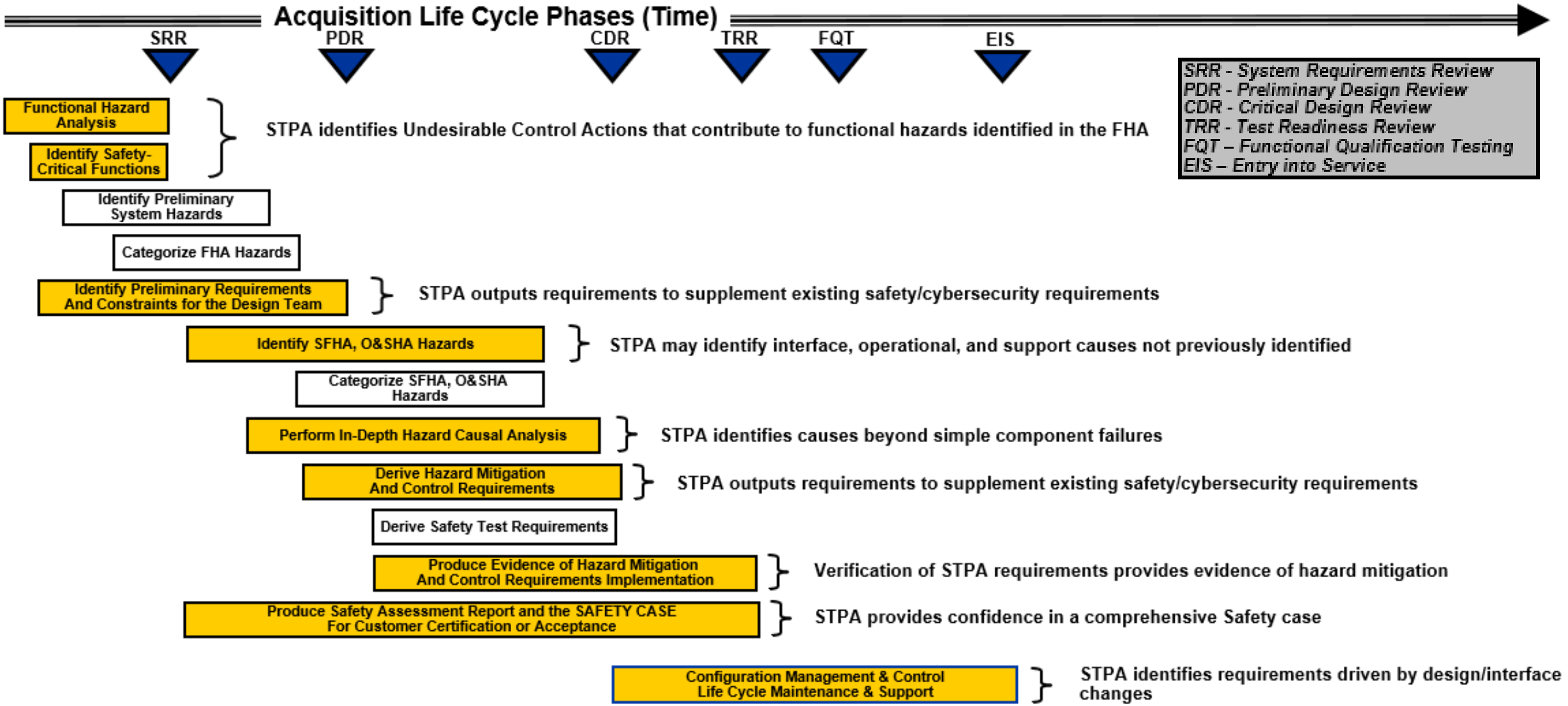
Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Integration Opportunities

- STPA potential future applications
  - Lower-Level Engine Controls
  - Modular Open Systems Approach (MOSA) or similar concept
  - Embedded Training
  - Manned-Unmanned Teaming
  - Cybersecurity

- MBSE-STPA integration
  - Performing STPA directly in CAMEO allows UCAs to be linked to applicable requirements, hazards, functions, and elements (functional/logical, hardware/software).
  - STPA applicability and impact across the product/service lifecycle (see next slide)

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.



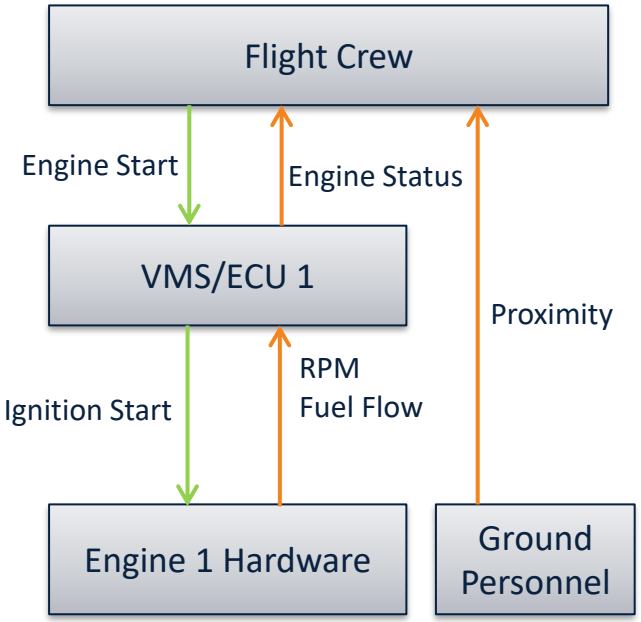

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Conclusion

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Recap

- Continued the MBSE for PA Series with a focus on early lifecycle MRP STPA
  - Demonstrated how MBSE & related tools enabled powerful linkages for System Safety
  - Discussed lessons learned & what worked well
  - Highlighted future considerations for analytical integration & expansion
  - Connected MBSE and PA to Boeing's ongoing digital transformation via MBSE/PA solution kits
- Showcased key STPA learnings
  - STPA's discovery of lower-level requirements earlier than traditional analyses
  - Focus on erroneous functionality yielded new hazards and new causes for hazards
  - Importance of trained facilitators and proper scoping, bounding, & abstraction
  - Hybrid approach with fruitful internal & external engagement
- Demonstrated STPA impact on program and enterprise
  - More hazards/causes => better requirements => stronger safety case
  - Cost avoidance, schedule protection, risk reduction
  - Integration opportunities from performing STPA in MBSE
  - Late lifecycle use cases



Engine Control Abstracted Example

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Thank you


- Our families as we worked on the MRP
- Our teammates and colleagues working on the MRP with us
- Greg Benn for contributions to this presentation
- Kayla King for independent review of this presentation
- MIT STAMP Workshop for hosting us
- You for your attention


Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Back-Up

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Acronyms

- ABL: Allocated Baseline
- ABSM: Allocated Baseline System Model
- AFHA: Aircraft Functional Hazard Assessment
- AFTA/SFTA: Aircraft & System Fault Tree Analysis
- CDR: Critical Design Review
- CRP: Civilian Rotorcraft Platform
- CSI: Critical Safety Item
- DAL: Development Assurance Level
- DD: Detailed Design
- EASA: European Union Aviation Safety Agency
- FAA: Federal Aviation Administration
- FBL: Functional Baseline
- FBSM: Functional Baseline System Model
- FDAL: Function Development Assurance Level
- FH: Flight Hour
- FMECA: Failure Modes Effects & Criticality Analysis
- FTA: Fault Tree Analysis
- HMMP/R: Hazardous Material Management Program Plan/Report
- IDCR: Initial Design Concept Review
- IDFR: Initial Design Functional Review
- IDRR: Initial Design Requirements Review
- IPT: Integrated Product Team
- MBE: Model-Based Engineering
- MBSE: Model-Based Systems Engineering
- MOSA: Modular Open Systems Approach
- MRP: Military Rotorcraft Platform
- O&SHA: Operating & Support Hazard Analysis
- OMB: Operational Model Baseline
- PA: Product Assurance
- PBL: Product Baseline
- PD: Preliminary Design
- PDR: Preliminary Design Review
- PS: Product Support
- PSSA: Preliminary System Safety Assessment
- PSSCFA: Preliminary Software Safety Critical Functional Analysis
- RAC: Risk Assessment Code
- RAM: Reliability/Availability/Maintainability
- RWB: Reliability Workbench
- SE: Systems Engineering
- SFHA: System Functional Hazard Assessment
- SFR: System Functional Review
- SHA/SSHA: System/Subsystem Hazard Analysis
- SMS: Safety Management System
- SRHA: System Requirements Hazard Analysis
- SRR: System Requirements Review
- SS: System Safety
- SSPP: System Safety Program Plan
- STPA: System-Theoretic Process Analysis
- UCA: Undesirable Control Action
- WRR: Windchill Risk & Reliability

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Abstract (1/3)

The objective of this presentation is to share observations and experiences from performing System-Theoretic Process Analysis (STPA) during Preliminary Design (PD) on a military rotorcraft platform in a Model-Based System Engineering (MBSE) ecosystem.

The general program structure for the military rotorcraft is described, followed by a brief introduction to STPA (note that this presentation is not intended to teach STPA). The presentation then explores how STPA was performed using DESE-CAMEO, including an overview of the control structure, example safety hazards and Undesired Control Actions (UCAs), and representative derived safety requirements. Observations, experiences, and future considerations are then discussed and the three main points are summarized below.

First, the results presented show STPA's effectiveness at identifying detailed lower-level safety requirements earlier than traditional safety processes normally might – if these requirements would be identified at all. As the STPA method focuses on these complex interactions between systems, including the human – system interactions, it can also help identify interface requirements. Dozens of tier-3 requirements at the element level and dozens more lower-level requirements were derived while the program in general was focusing on tier-1 and tier-2 requirements at the system and segment levels. STPA was particularly effective at facilitating requirements discussions between the rotorcraft manufacturer and the engine supplier, as the engine supplier was engaged early to help build the control structure, define UCAs, and identify and refine derived safety requirements.

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Abstract (2/3)

Second, the use of a MBSE tool to provide a single central repository of SE data created opportunities that would not have been previously feasible in traditional SE ecosystems. In the realm of SS, hazards from Aircraft/System Functional Hazard Assessments (AFHA/SFHA) and UCAs from STPA are represented as elements in the MBSE ecosystem. These elements can then be linked within the MBSE tool to the other elements of the MBSE ecosystem, including requirement elements, function elements, logical elements, and physical elements, allowing an analyst to quickly see all of the related elements in a single central repository, more easily understand the connections between them, and analyze for change impact.

Third, even though this presentation mainly focuses on performing STPA in MBSE early in the acquisition lifecycle during Preliminary Design, use cases for STPA later in the acquisition lifecycle are also explored here. During Design, STPA identifies UCAs that contribute to hazards and/or new hazards; outputs requirements to supplement or refine existing requirements; discovers interface, operational, and support causes not previously found; and identifies hazard causes beyond component failures. During Validation/Verification, STPA aids in validation of other requirements while the verification of STPA-generated requirements provides evidence of hazard mitigation, both of which bolster confidence that the program has a comprehensive safety case. During Development and Service, STPA identifies requirements stemming from design/interface changes.

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Abstract (3/3)

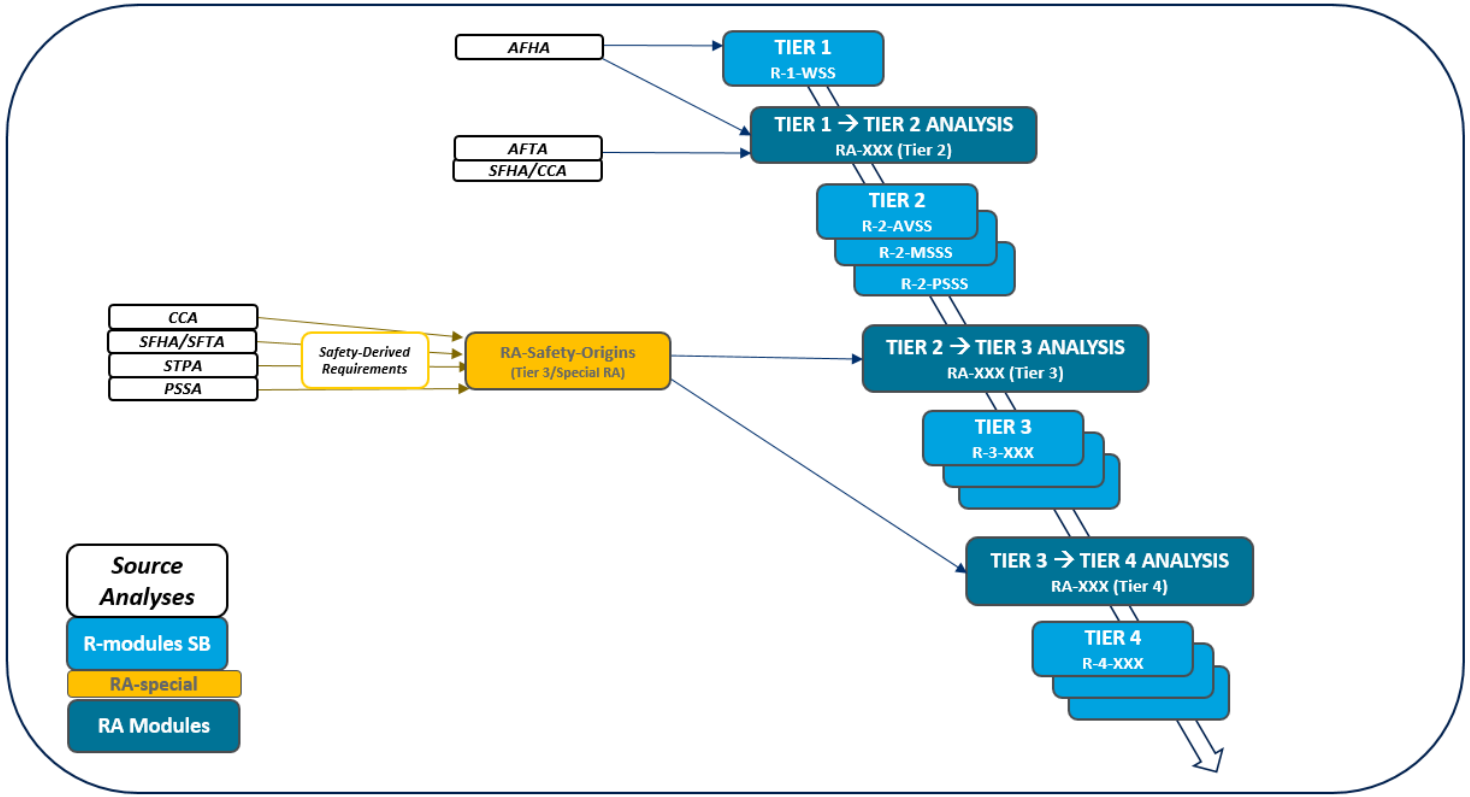
Finally, the presentation closes with a collection of other relevant lessons beyond what was discussed above and a conclusion to summarize everything that was presented.

Note: This presentation is also part of a broader series exploring what could be learned from the application of MBSE for Product Assurance (PA) on platforms at various stages of their respective lifecycles. The scope of this research series includes hardware and software contexts on both civilian and military product/service platforms and spans the lifecycle from initial conceptual development to retirement/disposal. For this series, PA is centered mainly on Reliability/Availability/Maintainability (RAM), Product Support (PS), and System Safety (SS) (collectively RAMPSSS).

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

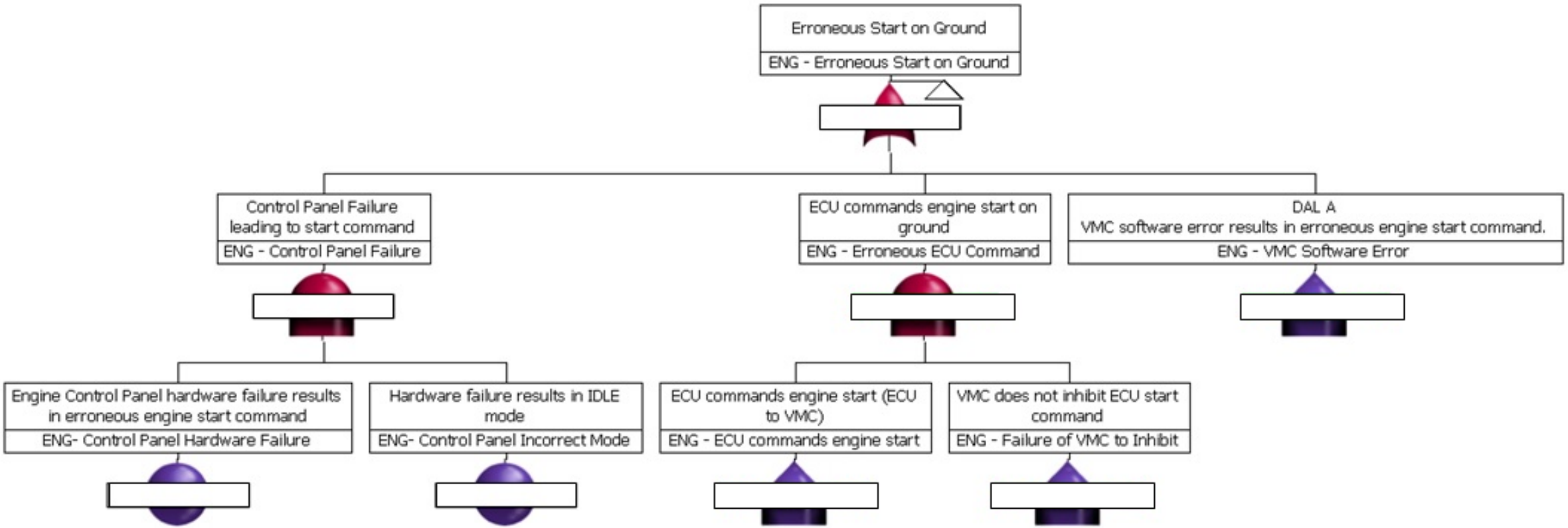
# Safety Context

- Initial Tier 1 system & Tier 2 segment requirements derived from traditional safety process
- STPA conducted in parallel with requirement, functional, physical, & logical baselining
- STPA delivered directly in DESE-CAMEO model
- STPA also informed Tier 3 subsystem, Tier 4 component, & lower requirements
- **STPA derives requirements at any tier based on control structure depth/detail**



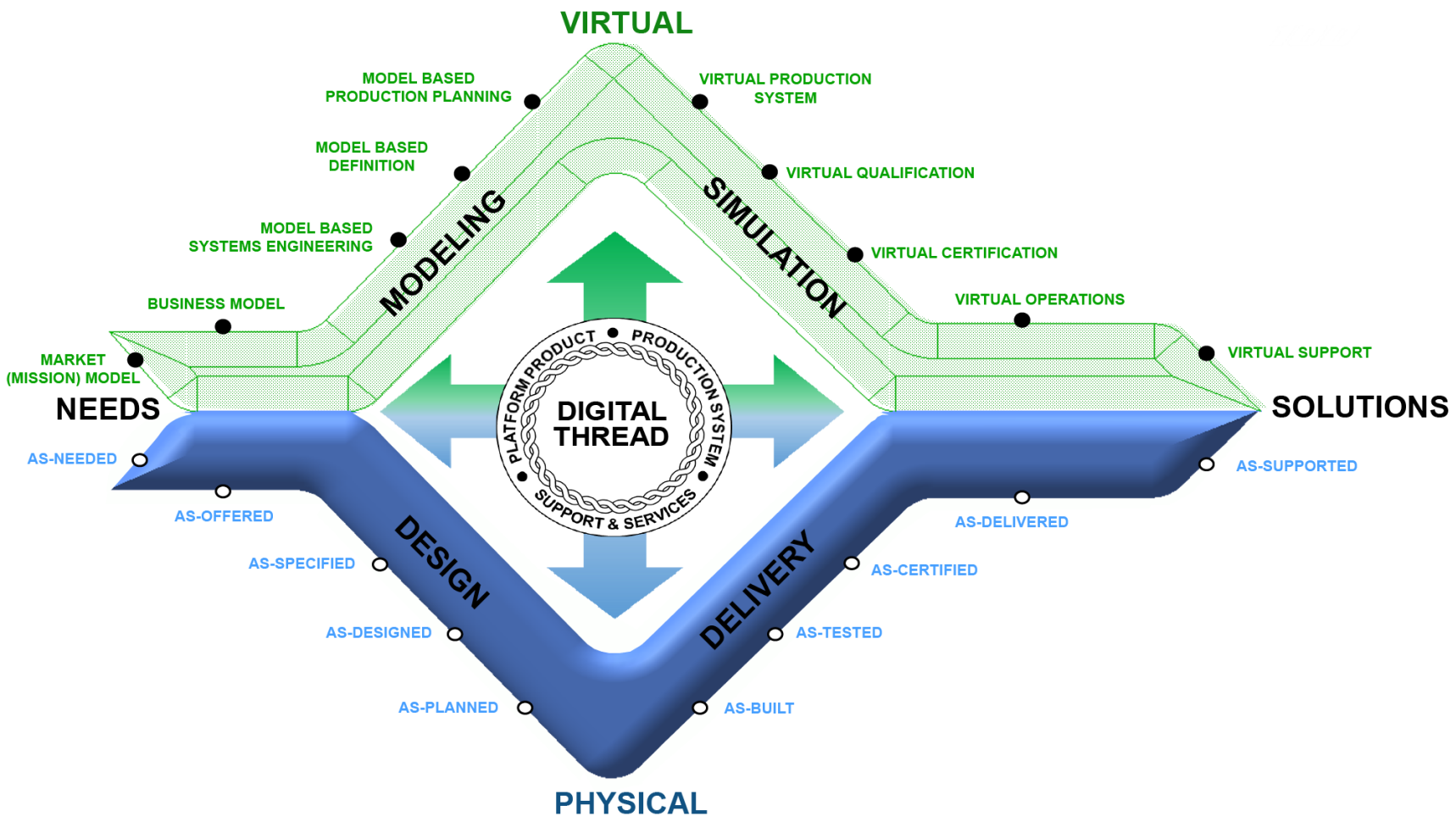

Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

| # | AFHA ID | Name | Function | Functional Failure | Functional Failure Breakdown | Phase | Environment | Detectability | Effect Of Failure | Accident | Severity |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1.1.1.c | 80.01a | Provide engine start capability | Erroneous Engine Start Capability | Start sequence erroneously initiated on the ground | G1 | ALL | Undetected | Erroneous activation of engine start sequence on the ground can results in loss of personnel and/or damage to aircraft or external objects due to rotating component contact or exhaust gasses. | Death or Permanent Total Disability | Catastrophic (1) |




Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.

# Evolution of System Engineering (SE) to Model Based Engineering (MBE)




Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.




Not subject to U.S. Export Administration Regulations (EAR), (15 C.F.R. Parts 730-774) or U.S. International Traffic in Arms Regulations (ITAR), (22 C.F.R. Parts 120-130). Copyright © 2026 Boeing. All rights reserved.