Towards Functional Hazard Assessment (CFHA): A Gap Analysis and Concept for Emerging Aviation Systems

Seydou Mbaye, Ph.D., Daniel Hulse, Ph.D., Lukman Irshad, Ph.D., **Hannah Walsh, Ph.D.,** and Sequoia Andrade

NASA – Ames Research Center

2025 AIAA SCITECH, 6-10 January 2025

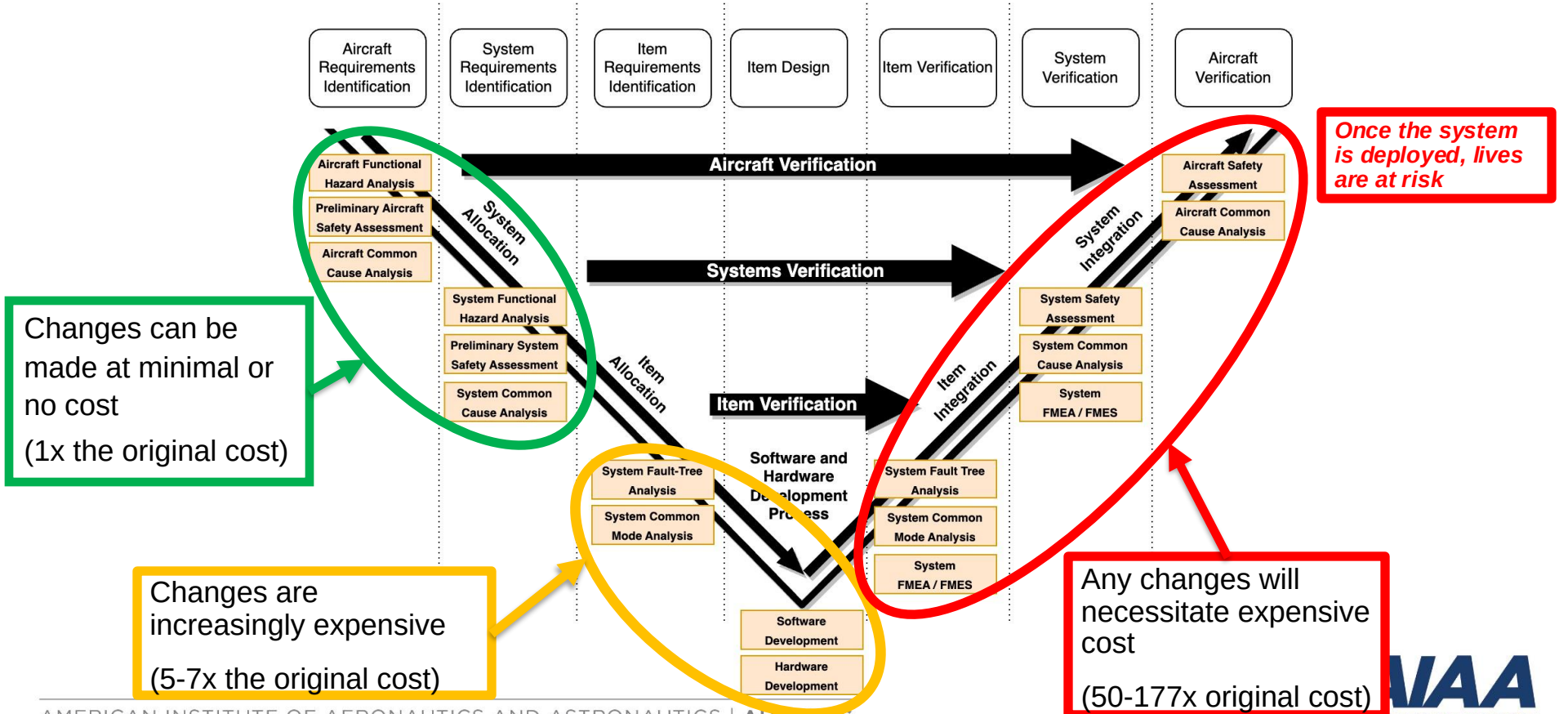
Thin Haul Commuter

Advanced General Aviation

Urban Vertical Take Off & Landing Air-Taxi

Small Unmanned Aircraft

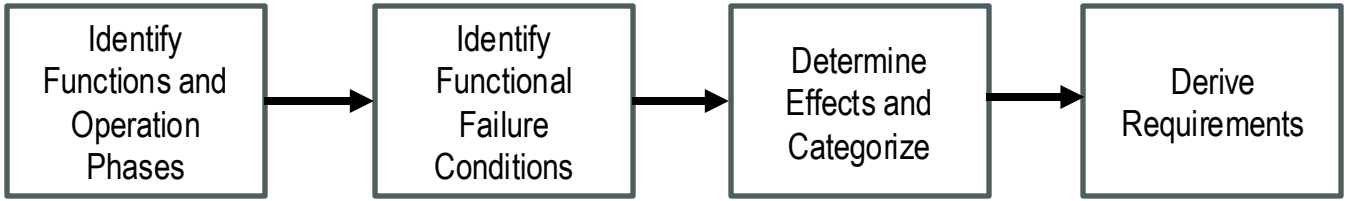
Aerospace Recommended Practices (ARP) 4761A

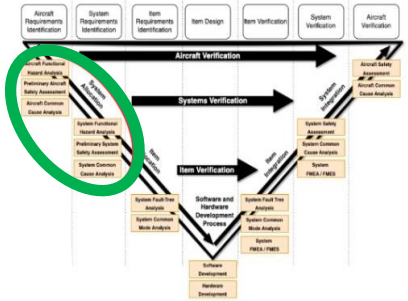


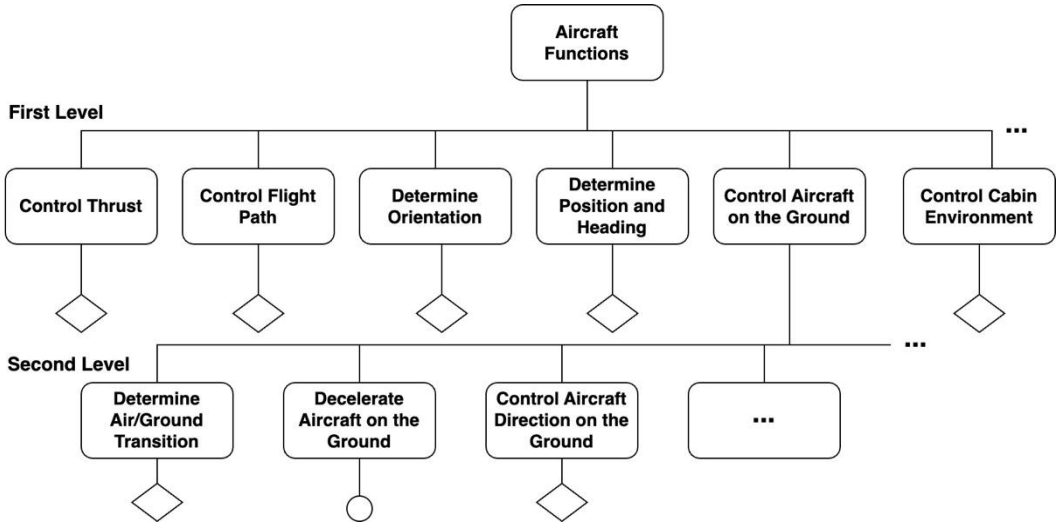
Aim & Objectives

- Identify challenges in FHA for novel, increasingly autonomous aviation concepts
- Identify opportunities for new and improved approaches
- Propose Computational Functional Hazard Assessment (CFHA) to address gaps in analysis capabilities for emerging aviation concepts

Functional Hazard Analysis (FHA)







Function	Failure Condition	Effect	Classification
Decelerate Aircraft on the Ground	Loss of Deceleration Capability		
	a. Unannunciated loss of deceleration capability	Inability to decelerate aircraft, resulting in high-speed overrun	Catastrophic

Adapted from *ARP4761A: GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT*

FHA for Novel Aviation Concepts: Barriers and Considerations

- Conventional FHA may be insufficient to capture:
  - Large, complex hazard space
    - Due to autonomy, human-system interaction, system-of-systems, etc.
    - What if the design (or, software) changes?
    - What if our assumptions were wrong?
  - Time-based behaviors and interactions needed to represent systems resilience
  - New, more complex mission profiles
    - What if we wanted to integrate new entrants carrying out new operations?
  - Meaningful classification of effects in emerging operational environments
  - Systems for which existing safety expertise is limited

Literature Review

Models and Formalisms for FHA

- Energy-Materials-Signals Based Models
- Socio-Technical Models

Model-Based Engineering for Traceability in FHA

- Model as a single point of truth
  - Improved communication and collaboration
  - Efficiency of hazard analysis

Computational Support for Analyzing Hazardous Scenarios

- Modeling and simulation in FHA – e.g., Functional Failure Identification and Propagation (FFIP)
- Learning from incident and accident reports

Opportunities for the Next Generation FHA

Using computation to support hazard assessments

- Managing large, complex hazard space
- Enabling rapid re-analysis and adaption
- Enabling identification and assessment of resilience
- Enabling assessment of severity of failure effects

Standardizing model capture and representation

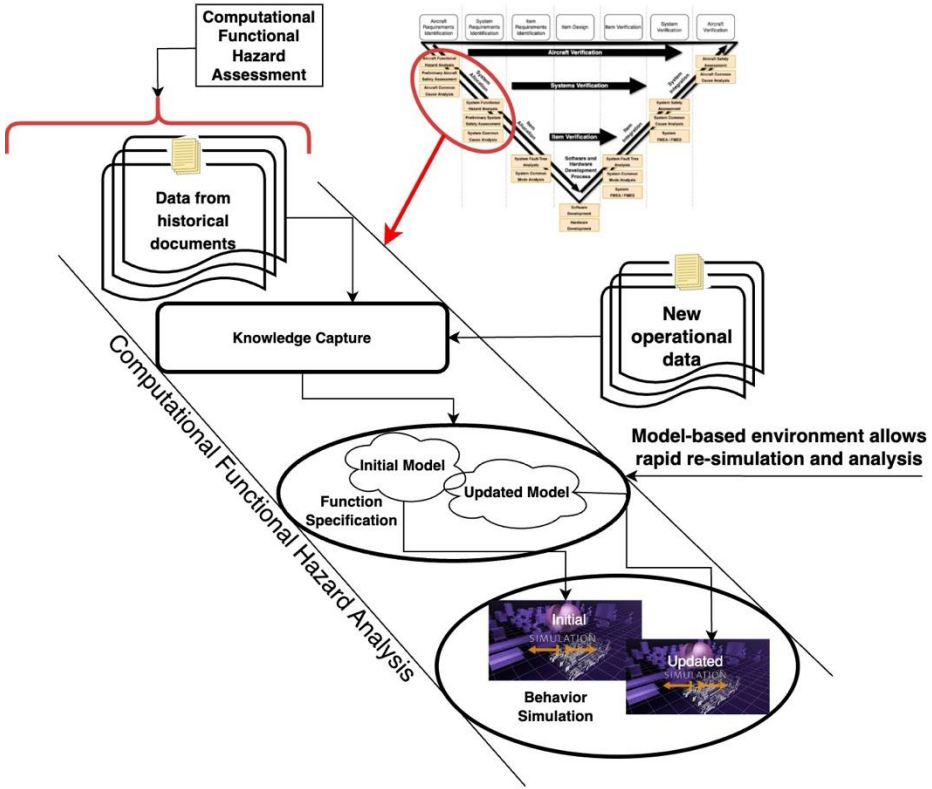
- Incorporating human and operational hazards
- Deriving and decomposing system functions
- Enabling traceability through Model-Based Engineering

Incorporating existing knowledge and data

- Improving completeness of knowledge capture by incorporating broad and analogous data sources

Towards Computational Functional Hazard Assessment

- Knowledge Capture
  - Leverage historical data
  - Monitor system during operations
- Specification of functions in a model-based environment
  - Enable updates
  - Better understanding of failure propagation
- Simulation of behaviors in scenarios
  - Assess system behavior over a wide variety of scenarios



Conclusion

- This study examined the current state of existing FHA approaches and identified existing gaps
- Opportunities identified from the gap analysis realized through the proposed framework:
  - Computational Functional Hazard Analysis
- Future work will integrate existing tools with capabilities addressing individual elements of CFHA
  - Additional tool maturation required

Thank you!

seydou.mbaye@nasa.gov

daniel.e.hulse@nasa.gov

lukman.irshad@nasa.gov

hannah.s.walsh@nasa.gov

sequoia.r.andrade@nasa.gov