

# Standardizing and Streamlining the Certification of Complex Machine-Human Applications

Dr. Andrew Zeitlin

703-983-6858 • [azeitlin@mitre.org](mailto:azeitlin@mitre.org)

FAA MOIE

The logo consists of a stylized graphic of stacked, colorful blocks (yellow, orange, and blue) on the left, followed by the text "MITRE Technology Program" in a bold, sans-serif font. The background of the slide features a pattern of these same colorful blocks.

**MITRE**  
Technology  
Program

**MITRE**

© 2004, The MITRE Corporation

# Problem

- **Current certification guidance gives no insight in crediting the human in the loop in a safety analysis.**
- **If operator judgment and problem-solving aren't considered, the criticality of the box becomes higher – and costlier – than necessary.**

# Background

## Old Guidance ...

**Advisory Circular**

Subject: GUIDELINES FOR THE DEVELOPMENT, APPROVED BY THE FAA, OF OPERATIONAL PROCEDURES FOR EQUIPMENT, SYSTEMS, AND INSTALLATIONS

Issue: 03/18/06 AC No. 135-76A

1. PURPOSE. The new High Intensity Terrain (HIT) and Airport Certification Service (ACS) systems are critical to the safety of flight. The FAA is issuing this advisory circular to provide guidance to operators, manufacturers, and the Department of Defense (DoD) on the development, testing, and approval of these systems. The FAA is also providing guidance on the development, testing, and approval of these systems. The FAA is also providing guidance on the development, testing, and approval of these systems.

2. SCOPE. This advisory circular applies to all operators, manufacturers, and the Department of Defense (DoD) who are developing, testing, and approving these systems.

3. REFERENCES. The following references apply to this advisory circular:

- (1) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.
- (2) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.
- (3) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.
- (4) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.

Hazard Class	Safety Objectives			
	Probable	Remote	Extremely Remote	Extremely Improbable
1	Unacceptable	Unacceptable	Unacceptable	Unacceptable
2	Unacceptable	Unacceptable	Unacceptable	Unacceptable
3	Unacceptable	Unacceptable	Unacceptable	Unacceptable
4	Unacceptable	Unacceptable	Unacceptable	Unacceptable
5	Unacceptable	Unacceptable	Unacceptable	Unacceptable

**Risk Acceptance Cases**

Unacceptable	Minimum Safety Objective	Acceptable
Minimum Safety Objective - Unacceptable with Single Point Failures and Common-Cause Failures		

4	Slight reduction in safety margins or aircraft functional capabilities.	5 (least severe)	No effect on operational capabilities or safety.
Physical discomfort, including	Physical discomfort.	Incovenience.	
Slight increase in workload.	Slight increase in workload.	No effect on flight crew.	
Slight reduction in separation or reduction in air traffic control capability.	Slight reduction in separation or reduction in air traffic control capability.	Slight increase in air traffic controller workload.	
control for a significant period of time.	control for a significant period of time.	in air traffic control capability.	

**Advisory Circular**

Subject: AIRCRAFT OPERATIONS, AND THE FAA'S OPERATIONAL PROCEDURES FOR EQUIPMENT, SYSTEMS, AND INSTALLATIONS

Issue: 03/18/06 AC No. 135-76A

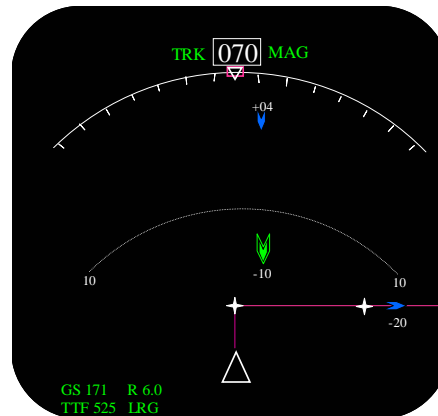
1. PURPOSE. The FAA is issuing this advisory circular to provide guidance to operators, manufacturers, and the Department of Defense (DoD) on the development, testing, and approval of these systems. The FAA is also providing guidance on the development, testing, and approval of these systems.

2. SCOPE. This advisory circular applies to all operators, manufacturers, and the Department of Defense (DoD) who are developing, testing, and approving these systems.

3. REFERENCES. The following references apply to this advisory circular:

- (1) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.
- (2) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.
- (3) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.
- (4) The occurrence of any other failure condition which would reduce the capability of the system to perform its intended function.

## ... New Systems



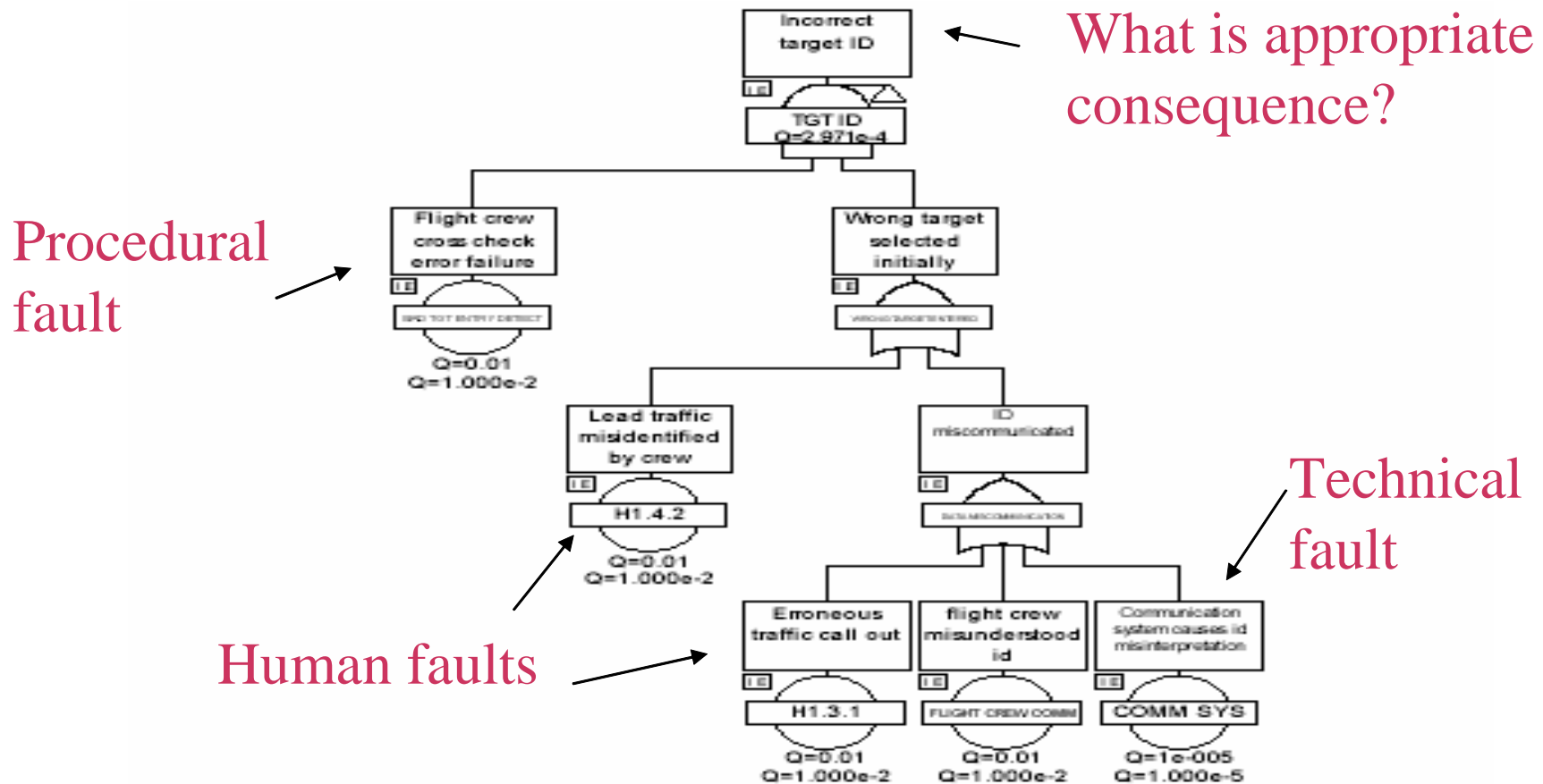
# Objective

- **Develop methods appropriate for analyzing complex machine-human systems**
- **Help FAA produce guidance material for applicants**
- **Make new systems less costly to certify and help them be fielded sooner to realize their benefits**

# Activities

- **Selected a lead example application: IMC Approach Spacing using ADS-B/CDTI**
- **Conducting safety analysis with a variety of methods:**
  - Traditional Fault Tree and Event Tree
  - Cognitive Modeling of Flight Crew Tasks
  - Dynamic Simulation of Hazard Exposure Time
- **Determine effectiveness of methods**
- **Illustrate hazards and mitigations in ATM Lab**

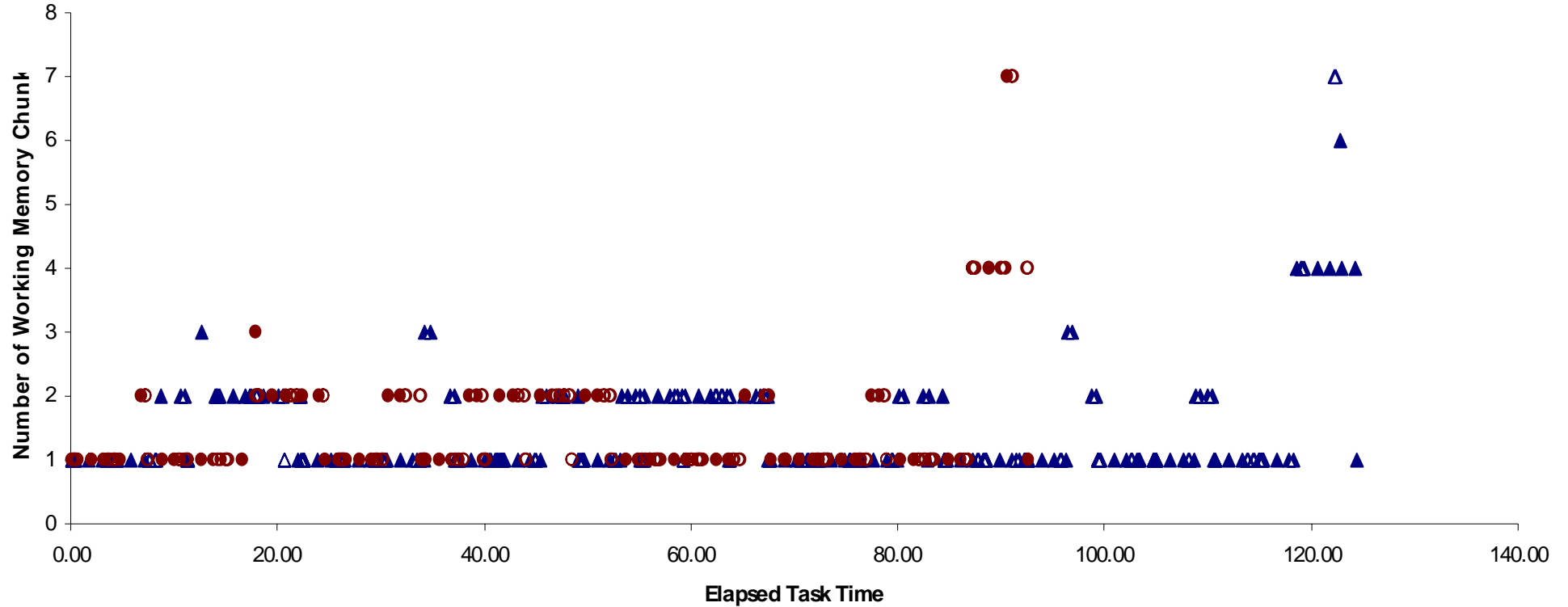
# Highlight



Example Hazard Fault Tree from CDTI Application

# Highlight

Cognitive Workload as Working Memory Usage over Course of MIT Departure Task



Example Output from a Cognitive Model

# Impacts

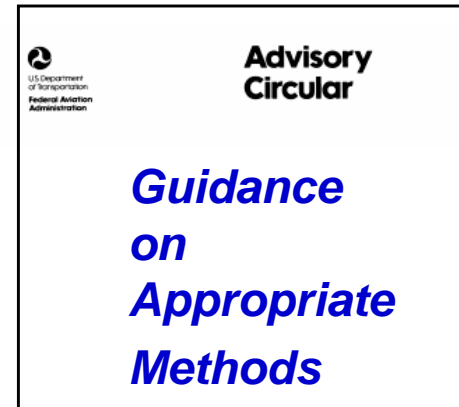
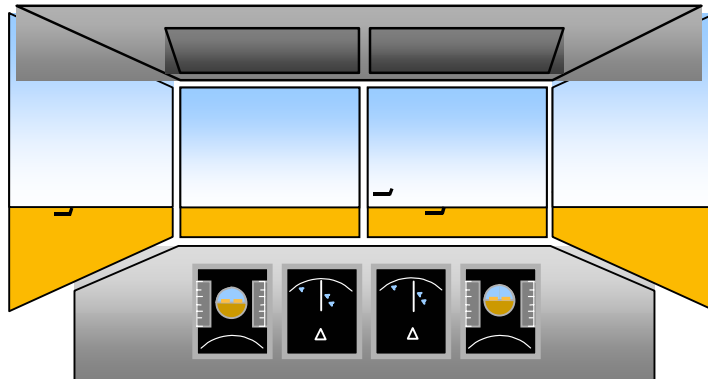
- **Reap operational benefits without delay**
  - **Enable new technologies and applications to be fielded earlier and to be more affordable**
- **Advance and streamline the certification process**
  - **Manufacturers save time and cost, and become more willing to propose innovative products that users can afford**

# Future Plans

## Analyses

Method	Advantages	Disadvantages
Fault Tree	Shows all Events leading to a Hazard of interest. Shows Mitigations.	Difficult to capture the range of human events, to credit human function
Event Tree	Shows Sequences of Actions and Failures, and their consequence	Difficult to translate to a likelihood of top hazard
Cognitive Modeling	Predicts Cognitive Workload and helps Predict Error Susceptibility	Results will need validation and consensus
Dynamic Simulation	Shows interaction of several asynchronous machine & human processes	Modeling human functions needs validation

ATM Lab Demo +  
Stakeholder  
Consensus



Migrate  
to Other  
Projects