Thoughts on Aviation Safety R&D

Andy Lacher

6 September 2017

Some Drivers

- **Unmanned Aircraft**
- **Urban Air Mobility**
- **General Aviation Safety**
- **Commercial Aviation**
  - Continued Safety Improvements
  - Automation Complexity
  - Cost reductions
  - Pilot Shortages

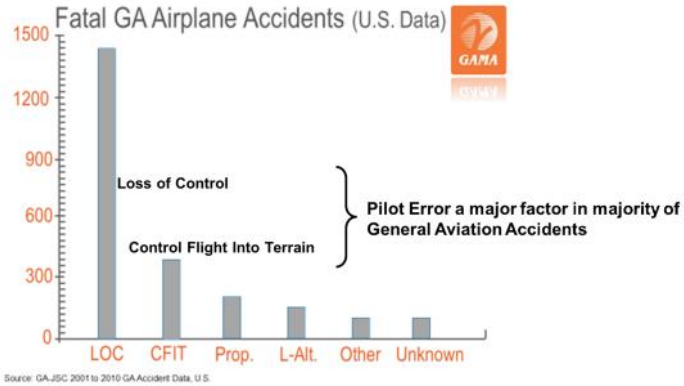

Aurora Flight Sciences


Creative Commons - Dkroetsch


UBS

Q-Series

Flying solo – how far are we down the path towards pilotless planes?




Creative Commons

MITRE

Concepts

- **Unmanned Aircraft**
- **Urban Air Mobility**
- **General Aviation Safety**
- **Commercial Aviation**
  - Continued Safety Improvements
  - Automation Complexity
  - Cost reductions
  - Pilot Shortages

Accessible Aviation

Simplified Operational Interface

"Easy Button"

Automated Parcel Delivery

Pilotless Flight

Refuse to Crash Technology

Automation as a Safety Net

Reduced Crew Requirements

Single Pilot Ops

MITRE

Technology Implications

More Dependence Upon Software for Safe Operations

- **Human-Machine Teaming**
- **Software Assurance**
- **Cybersecurity**
- **Cyber-Resiliency**

Software is both a key enabler and a barrier to operational implementation

- **Certification**

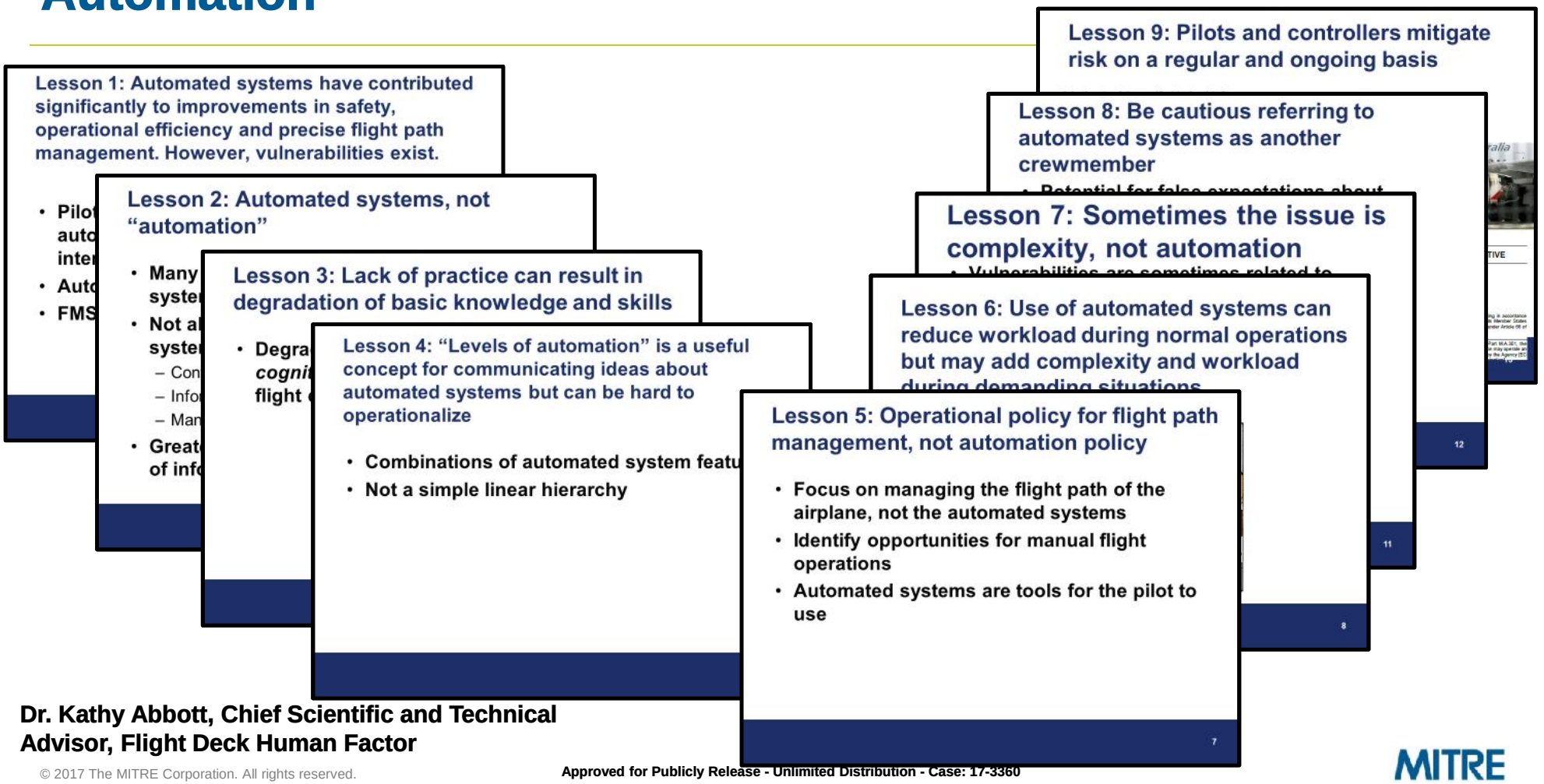
Approved for Publicly Release - Unlimited Distribution - Case: 17-3360

MITRE

Automated Actions vs. Cognitive Assistance

- **Task Automation under human control**
  - Autopilot; Autoland
- **Human operation with automation assistance (safety net, watch dog, cognitive aid)**
  - Auto-GCAS
  - Digital Co-pilot
- **Pilot-less Flight – Automation is the pilot**

Human-Machine Interface Challenges Associated with Automation



Dr. Kathy Abbott, Chief Scientific and Technical Advisor, Flight Deck Human Factor

Approved for Publicly Release - Unlimited Distribution - Case: 17-3360

MITRE

Auto-GCAS: Automatic Safety Net
(Ground Collision Avoidance System)

CFIT & GLOC accidents

Six systems on the F-16 → CFIT rate unchanged

- **Introduced in 2014 – Block 40/50**
- **Maneuver – Roll-to-upright and 5G pull**

Auto-GCAS Keys to Success

- **Design started with the pilot requirements**
  - Nuisance Budget
  - Maximum acceptable maneuver
  - Interface
- **Run-time Assurance Architecture Approach**

CFIT: Controlled Flight Into Terrain
GLOC: G-Force induced Loss of Consciousness
Auto-GCAS: Auto-Ground Collision Avoidance System

MITRE

Digital Co-Pilot – Cognitive Assistance

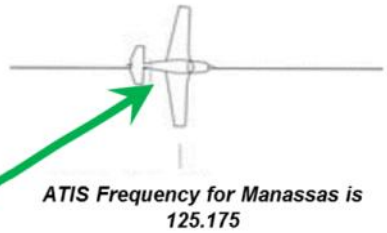
Solo flight is riskier than flight with a crew*

- **Accident rate: ~3x**
- **Fatal Accident Rate: ~13x**

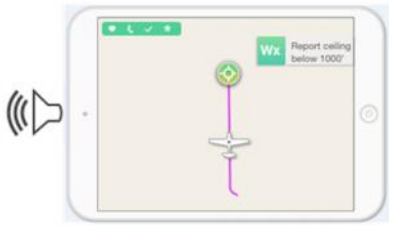
*** Solo pilots also tend to have less training, less experience, and are operating single engine aircraft**

Better Info + Improved Workload + Extra Cognition ➡ Better Decisions ➡ Safer Operations

Right Information



Right Time



Right Format

Pilot Workshops

Lab Studies

Flight Tests

Analytic Modeling

MITRE

Technology Implications

More Dependence Upon Software for Safe Operations

- **Human-Machine Teaming**
- **Software Assurance**
- **Cybersecurity**
- **Cyber-Resiliency**

Software is both a key enabler and a barrier to operational implementation

- **Certification**

Approved for Publicly Release - Unlimited Distribution - Case: 17-3360

MITRE

Old Wine in New Bottles

- **Mature Research Space**
  - **People building systems don't read the research**
  - **People doing research don't understand how to apply it within systems engineering**

Researchers

Developers

Valley of Death

Approved for Publicly Release - Unlimited Distribution - Case: 17-3360

MITRE

Human-Machine Teaming – Themes from the Research

Design Content			Design Process
Transparency	**Augmenting Cognition**	**Coordination**	**Design Specifics**
• ***Observability*** Transparency into what an automation partner is doing relative to task progress • ***Predictability*** Future intentions and activities are observable & understandable	• ***Directing Attention*** Orient attention to critical problem features and cues • ***Exploring the Solution Space*** Leverage multiple views, knowledge, and solutions to jointly understand • ***Adaptability*** Recognize and adapt fluidly to unexpected situations	• ***Directability*** Humans can direct and redirect an automation partner's resources, activities, and priorities • ***Calibrated Trust*** Understand when and how much to trust automation partner • ***Common Ground*** Pertinent beliefs, assumptions, intentions are shared	• ***Design Process*** Guidance on the systems engineering processes for HMT • ***Information Presentation*** Format information to support understandability & simplicity

Quenching the Thirst for Human-Machine Teaming Guidance: Helping Military Systems Acquisition Leverage Cognitive Engineering Research - Patricia L. McDermott (MITRE), Katherine E. Walker (MITRE), Cynthia O. Dominguez (MITRE), Alex Nelson (AFRL), and Nicholas Kasdaglis (MITRE).

MITRE

Technology Implications

More Dependence Upon Software for Safe Operations

- **Human-Machine Teaming**
- **Software Assurance**
- **Cybersecurity**
- **Cyber-Resiliency**

Software is both a key enabler and a barrier to operational implementation

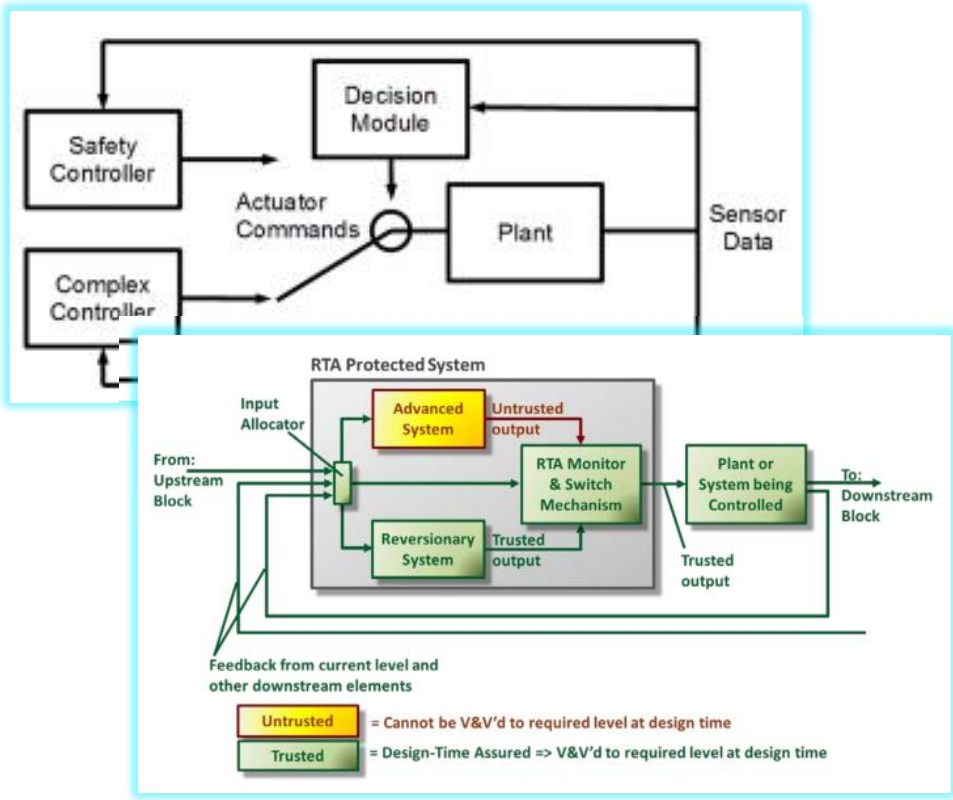
- **Certification**

MITRE

Run-Time Assurance

- **Monitors system behavior during run-time**
- **When specific thresholds are reached triggers bounding behaviors**
- **Variants**
  - Monitor system state
  - Monitor autonomous processes
    - Data outputs
    - Inferred behaviors

From U. of Illinois Study

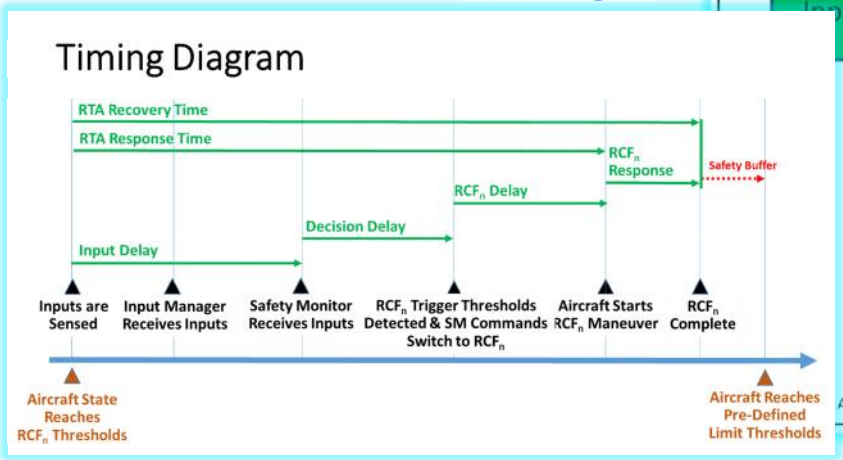


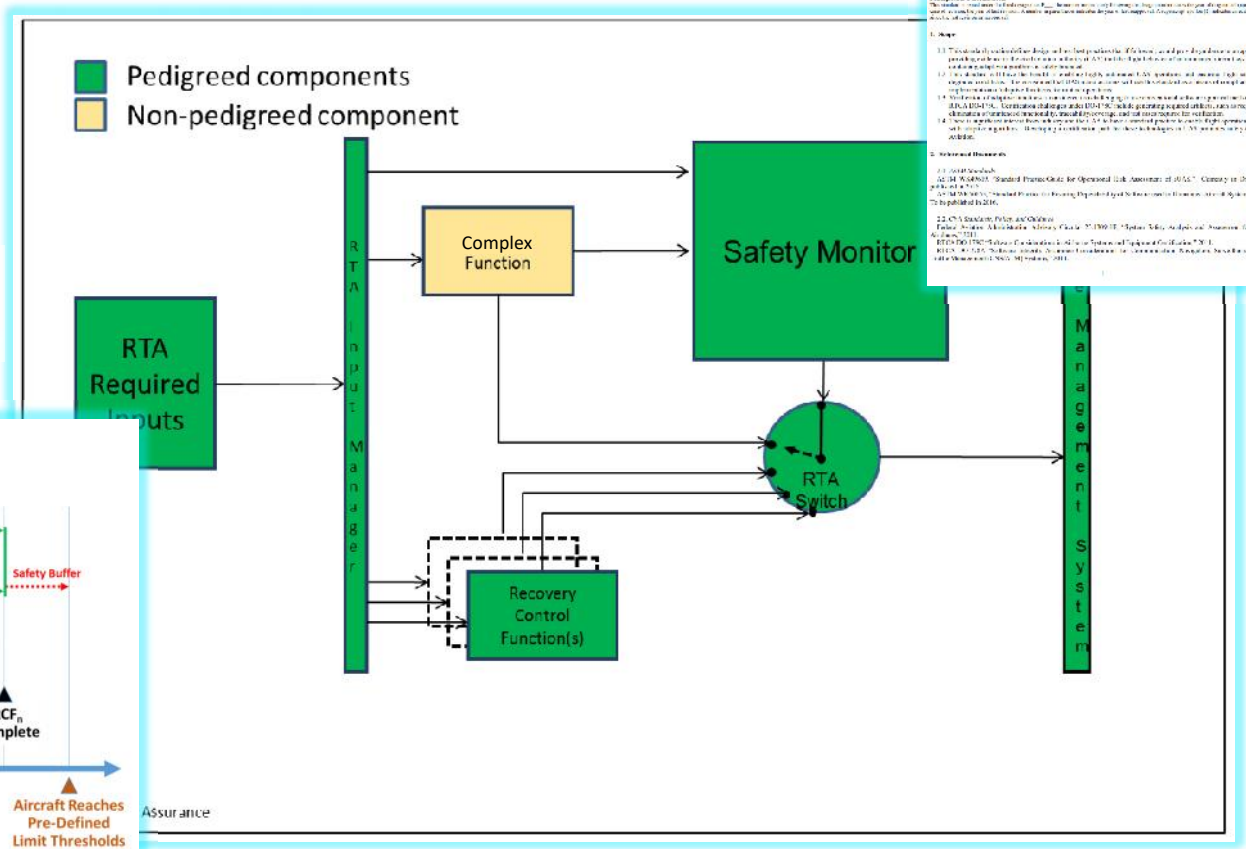
From AFRL Study

MITRE

Draft Standard – System State Monitor

- **Guidance on a run-time assurance architecture**
- **Enables applicant to determine implementation**





From Draft ASTM Standard

Technology Implications

More Dependence Upon Software for Safe Operations

- **Human-Machine Teaming**
- **Software Assurance**
- **Cybersecurity**
- **Cyber-Resiliency**

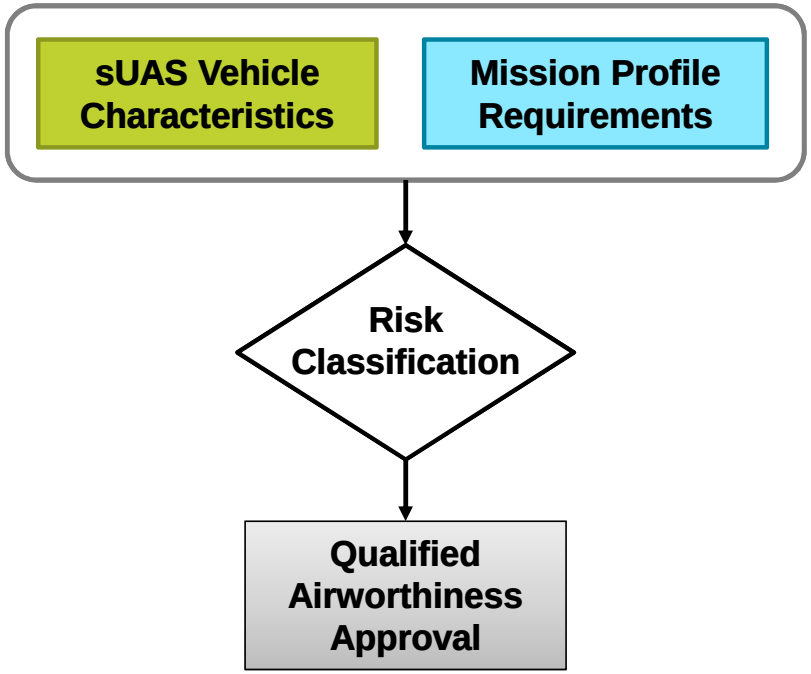
Software is both a key enabler and a barrier to operational implementation

- **Certification**

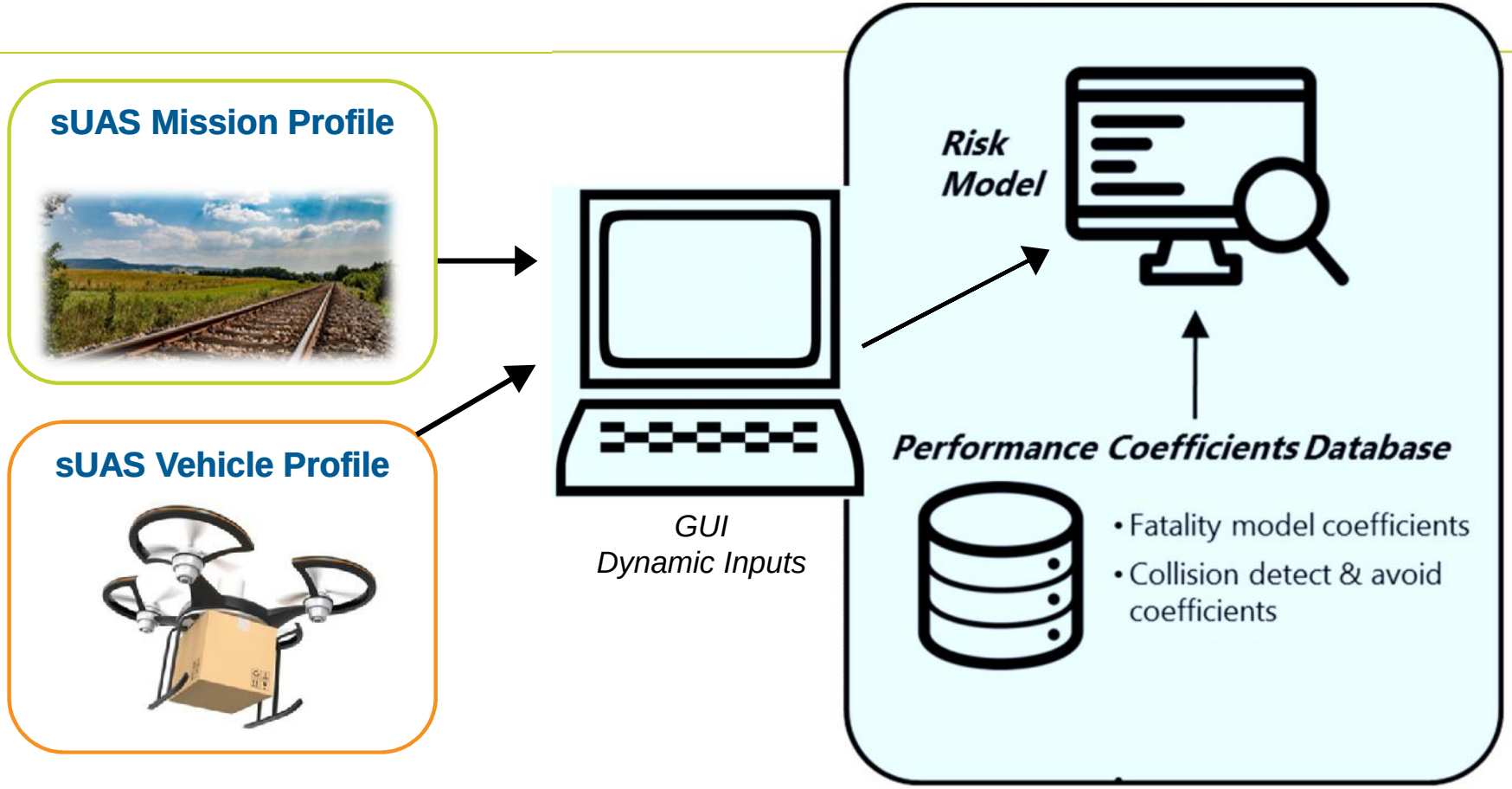
MITRE

Risk Based Approach for sUAS Operational Approval

A Risk-Based Approach for sUAS operational approval combines the vehicle and mission characteristics to ensure an acceptable level of safety



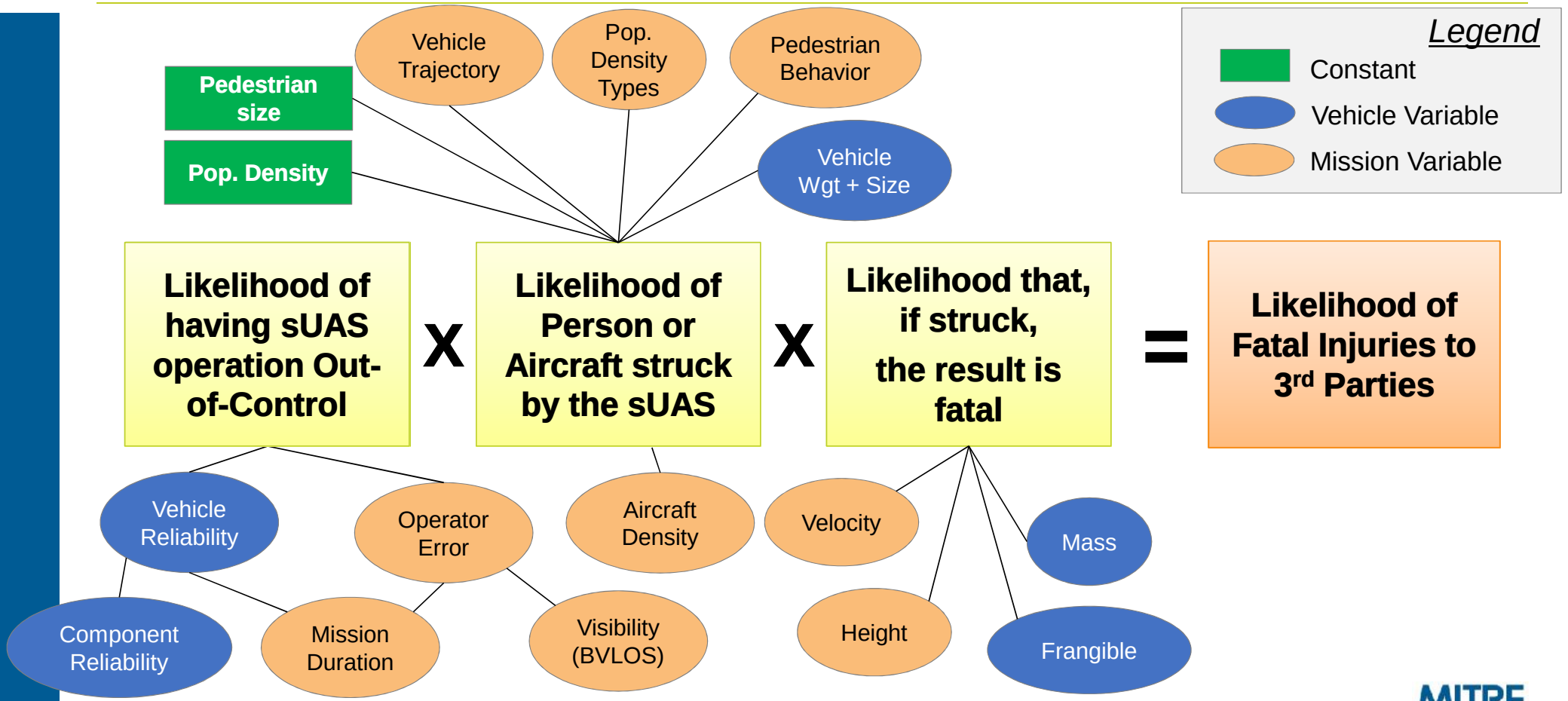
sUAS Risk Model System



MITRE

sUAS Risk Model Overview

Modeling Each Node



MITRE

Standard Mission Profiles

Each of the Mission profiles have different types of operational risks.

The risk is based on the combination of:

- **Mission profile**
- **Vehicle profile**
- **Operational factors**
- **Environmental factors (such as buildings and obstacles)**

Sparse Operations: Agriculture, Wildlife, Disaster Assessment, etc.

Contained Area Operations: Static Infrastructure Inspection, Real Estate Photography, Temporary Hotspots

Linear Area Operations: Linear Infrastructure, Waterfront Advertising, Traffic, etc.

Public Event Operations: Parades, Sporting Events, Concerts, Static News Coverage, etc.

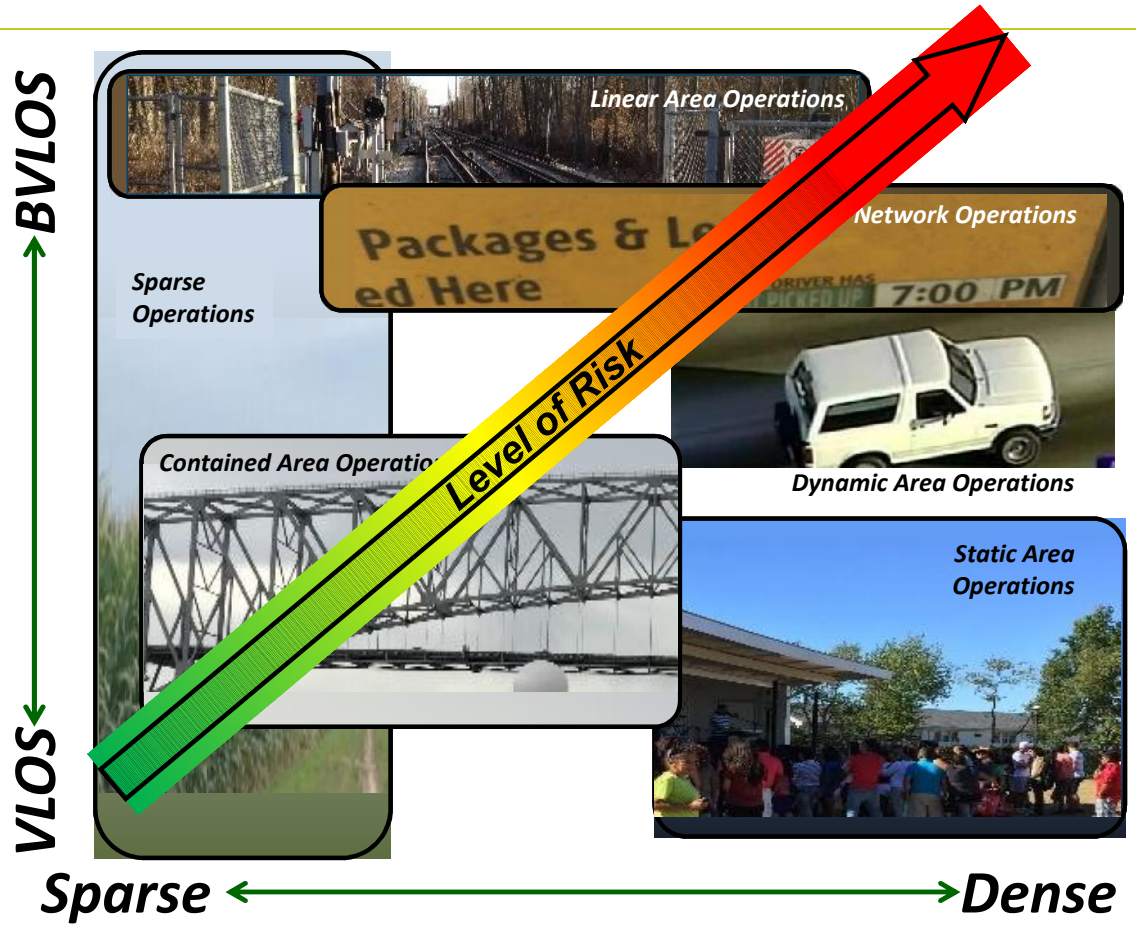
Network Operations: Small Cargo Delivery, emergency response, etc.

Dynamic Area Operations: Fire and Rescue, search and rescue, police chases, media coverage

MITRE

Mapping Mission Profile to Key Risk Variables

- **Sparse Operations** are characterized by low populated areas, but may be near or far from sUAS operator
- **Contained Area Operations** are characterized by operations near structures typically near the operator with controlled population access.
- **Linear Area Operations** are characterized by long distance operations typically over sparse or controlled population areas**.**
- **Public Event Operations** are characterized by operations near the operator over densely packed populations.
- **Network Operations** are characterized by operations traversing wide area networks near or far from populations**.**
- **Dynamic Area Operations:** Fire and Rescue, search and rescue, police chases, media coverage



MITRE

Technology Implications

More Dependence Upon Software for Safe Operations

- **Human-Machine Teaming –** ***Automation as a safety net and cognitive assistant***
- **Software Assurance –** ***New architectures – Software watching software***
- **Cybersecurity –** ***New attack surfaces – vulnerabilities at the interfaces***
- **Cyber-Resiliency -** ***Must continue to function safely***
  - ***Despite***
    - **Design defects**
    - **Unanticipated situations**
    - **Missing/corrupt/spoofed/unexpected data**
    - **Deliberate attacks**

Software is both a key enabler and a barrier to operational implementation

- **Certification –** ***Consider operational and system risk together***

Approved for Publicly Release - Unlimited Distribution - Case: 17-3360

MITRE