Workshop: Risk Mitigation in UAS Operations
Risk Mitigation in UAS Operations

Wes Ryan, FAA
Maggie Geraghty, FAA
Tracy Lamb, AUVSI
Lorenzo Murzilli, Swiss FOCA

#UAS2018
Starting Principles

• Safety: Our Mission
  – Focus: Protection of people/property on ground and in the air through performance based process
  – Shared challenge: Actively manage new risks UAS present

• Be Performance-Based Instead of Prescriptive
  – Requirements: Address risk, apply FAA resources appropriately, while also managing industry demands
  – Safety management concepts & risk-based decision making: Tools meet safety intent for UAS integration
Safety Risk Management Policy

  - Non-punitive Assessment of Risk & Effectivity of Mitigations
- US FAA State Safety Program
  - FAA Order 8000.369B - Safety Management System
  - FAA Order 8040.4B - Safety Risk Management Policy
  - FAA Order JO 1000.37B – ATO SMS Policy
- Specific Tools to be Discussed Today
  - JARUS SORA
  - SRMP Process

#UAS2018
Key Goals of SMS - Event Mitigation

• Actively Managing Risk
  – Proactively evaluate/mitigate risk – design and operational
  – Help FAA and Industry understand system/integration

• Avoid Regulating by “accident”
  – Fixes case-by-case, informal, temporary, & inconsistent
  – Often solved locally w/o standardization
  – Resident with local expert
  – Not timely/permanent - Policy, Reg., etc.

• Existing manned aircraft risk assessment/targets may not work for all UAS use cases/sizes
Risk Analysis for UAS Integration

- Risk Assessment Defines Risks, Mitigations, and When Risk Controls Need FAA Validation for Integrity & Safety
- Aircraft, Airmen, and Operational Requirements Change with Use Case, Concept of Operation – Risk Analysis Must Address All
UAS Risk Analysis Process

- Risk to People on Ground and In Air
- Determines If Design, Airworthiness, & Risk Mitigations Need Direct FAA Involvement
- FAA SRMP and JARUS SORA Good Examples
- Above a Certain Risk Score, Need TC/PC
Risk-Based FAA Direct Involvement

Operator Compliance

Small UAS:
- Low risk
- Low involvement from Aviation Authority
- Limitations: <55 lb.
- Visual line of sight, <400 ft. altitude, distance from airports and no ops over people
- CFR Part 107

Industry Compliance

Specific Use Cases:
- Increased risk
- Operation by Waiver, Certificate of Authorization, Airworthiness
- Specific requirements on drone, personnel, equipment based on safety assessment and using industry standards
- Waivers/Exemptions/Future Part 21 Changes

FAA Compliance

Fully Certified
- High Risk
- Fully Integrated Operations
- Risk-based Regulatory Structure similar to manned aviation
- FAA Design and Production Certificates
- Typical Level of Certification
Resilience Engineering

- Resilient Design for System/Human Interaction
  - Is the system stable? Can it handle changes and still be safe? Can it maintain or regain stability & continue operations after a major mishap and/or problem

Anticipate  Monitor  React

What to Expect?  What to look for?  What to do?  What Happened?

Learn
Safety Risk Management
Maggie Geraghty, Safety Management Group Manager, Federal Aviation Administration FAA
SRM Process: DIAAT

DIAAT: The formalized approach used by a panel of experts and affected stakeholders to identify issues, evaluate their criticality, and determine a means to minimize or eliminate their impact.
Describe the System

1. Describe the System
2. Identify the Hazards
3. Analyze Risk
4. Assess Risk
5. Treat Risk
5M Model

The 5M Model is a tool used to describe the system, operation, or procedures being added or changed. It includes:

- **MISSION**: The clearly defined and detailed purpose of the NAS change or system/operation being assessed
- **(hu)MAN/PERSON**: Operators, maintainers, and affected stakeholders
- **MACHINE**: Equipment used in the system
- **MANAGEMENT**: Procedures and policies that govern the system’s behavior
- **MEDIA/ENVIRONMENT**: The environment in which the system is operated and maintained
Identify Hazards

Describe the System → Identify the Hazards → Analyze Risk → Assess Risk → Treat Risk

#UAS2018
What is a Hazard Analysis Worksheet (HAW)?

- An analysis tool used to document the risk assessment of the system or change
- Inputs are developed from a Preliminary Hazard List (or other hazard identification tool)

Why complete a HAW?

- Required as part of the SRM process
- Links identified hazards to controls and risk mitigation activities
- Documents risks, hazards, system states, and safety requirements
Describe the System
Identify the Hazards
Analyze Risk
Assess Risk
Treat Risk
“Credible effect” refers to the reasonable expectation that the assumed combination of conditions that define the system state will occur within the operational lifetime of a typical air traffic control system.

Hazard assessments consider all credible effects (outcomes).

Less severe effects may pose a higher risk than the worst credible effect.
What Is Risk?

- The composite of predicted **severity** and **likelihood** of the potential effect of a hazard, before any of the proposed mitigations are implemented.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Likelihood</th>
</tr>
</thead>
</table>
| - The consequence or impact of a hazard’s effect (outcome) in terms of degree of loss or harm (less severe to more severe)  
- While assessed first, determination of severity is independent of likelihood | - The estimated (predicted) probability or frequency, in quantitative or qualitative terms, of a hazard’s effect (outcome)  
- Definitions are tailored to ATC Operations, Flight Procedures, and Systems Engineering |

#UAS2018
What Are Risk Levels?

- **High: Unacceptable Risk**
  - Must be mitigated to a Medium or Low risk prior to implementation

- **Medium: Acceptable Risk**
  - May be implemented but safety requirements are recommended to increase the safety margin

- **Low: Acceptable Risk**
  - May be implemented (but safety requirements are recommended)
  - Must have at least one safety performance target

### Severity / Likelihood Table

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Minimal 5</th>
<th>Minor 4</th>
<th>Major 3</th>
<th>Hazardous 2</th>
<th>Catastrophic 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent A</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Probable B</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Remote C</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Extremely Remote D</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High*</td>
</tr>
<tr>
<td>Extremely Improbable E</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium*</td>
</tr>
</tbody>
</table>

*Risk is high when there is a single-point or common cause failure.
Identify the Hazards → Analyze Risk → Assess Risk → Treat Risk

#UAS2018
How Do We Treat Risk?

- Identify feasible risk management options
- Determine predicted residual risk
- Define safety performance targets
- Develop a monitoring plan:
  - Define monitoring activities and methods used to verify predicted residual risk
  - Implement and verify these plans
Safety Performance Targets

• Measurable goals used to verify the predicted residual risk of a hazard
• Appropriate metrics must be determined
• Consider controls and safety requirements
• Pre-SRM panel data analysis serves as the basis for comparison against the post-implementation metrics
Monitoring Plans

- Documents all hazards
- Documents a plan to implement safety requirements for all risk levels identified in the final HAW
- Records monitoring activities:
  - Who is responsible?
  - How will we monitor and how often?
  - How will we track the hazards?
  - What are we measuring against?
  - How will we measure progress?

Document and Verify Low-Risk Hazards at Least Once
Document Review and Approval

- Documents are reviewed for:
  - SRM Consistency
  - Accuracy

- Document Approval:
  - Does NOT equate to the approval of an operation
  - The approval represents the approval of the safety assessment

- Monitoring:
  - Begins after implementation
  - Is monitored until the predicted residual risk verified.