Building your Operational Risk Assessment

Jarrett Larrow
Aerospace Engineer, AFS-410(c)
Building Your ORA

- Nicholas Flom, Executive Director, Northern Plains UAS Test Site
- Mark Blanks, Director, Virginia Tech Mid-Atlantic Aviation Partnership (MAAP)
- Alexandra Florin, Drones Project Manager – Executive Directorate, EASA
- Andy Thurling, Chief Technology Officer, Northeast UAS Airspace Integration Research (NUAIR)
- Jeremy Grogan, Aviation Safety Inspector, FAA – Part 107 Waiver Team Lead
What is an ORA and when do I need one?

Waiver

Exemption

Type Certification
References for ORAs
What’s in an ORA?

<table>
<thead>
<tr>
<th>Hazard Category</th>
<th>Hazard Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Issue with UAS</td>
<td>Propulsion System Failure</td>
</tr>
<tr>
<td></td>
<td>FCS Failure</td>
</tr>
<tr>
<td></td>
<td>Loss of C2 Link</td>
</tr>
<tr>
<td></td>
<td>GPS receiver fails</td>
</tr>
<tr>
<td></td>
<td>GCS Failure</td>
</tr>
<tr>
<td>Deterioration of external systems</td>
<td>Loss of ground radar</td>
</tr>
<tr>
<td></td>
<td>RangeVue failure</td>
</tr>
<tr>
<td></td>
<td>Ops van power failure</td>
</tr>
<tr>
<td></td>
<td>Wide Area Network (WAN) failure</td>
</tr>
<tr>
<td></td>
<td>Crew communication failure</td>
</tr>
<tr>
<td></td>
<td>GPS service fails</td>
</tr>
<tr>
<td>Human Error</td>
<td>Preflight planning errors</td>
</tr>
<tr>
<td></td>
<td>Maintenance errors</td>
</tr>
<tr>
<td></td>
<td>Crew fatigue</td>
</tr>
<tr>
<td></td>
<td>Improper communication RPIC/RPIC or RPIC/EO</td>
</tr>
<tr>
<td>Adverse Operating Conditions</td>
<td>Flight into conditions beyond aircraft limitations</td>
</tr>
<tr>
<td>Unable to See and Avoid</td>
<td>DAA system does not detect intruder</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Extremely Improbable (1)</td>
</tr>
<tr>
<td>Catastrophic (5)</td>
<td>5</td>
</tr>
<tr>
<td>Hazardous (4)</td>
<td>4</td>
</tr>
<tr>
<td>Major (3)</td>
<td>3</td>
</tr>
<tr>
<td>Minor (2)</td>
<td>2</td>
</tr>
<tr>
<td>Negligible (1)</td>
<td>1</td>
</tr>
</tbody>
</table>

Risk Analysis

Mitigation

Risk Identification
Risk-Based Safety Case Development

1. **Operational Context Definition**
   - Concept of Operations
     - Mission objectives
     - Operational description
     - Requirements definition
   - Risk Assessment
     - Hazard identification
     - Risk mitigation development
     - Identify supporting data needed
   - Repeat until risks are mitigated to acceptable level

2. **Data Collection**
   - Test Planning
     - Test/data requirements
     - Scope and method of test
     - Schedule and resources
   - Testing & Demos
     - Quantitative data collected
     - Verify sufficient data to support mitigations
     - Data validates mitigations
   - Update ConOps and ORA if mitigations cannot be validated

3. **Safety Case**
   - Safety Case Compilation
     - Final analysis of safety
     - Compilation of all data
     - Completed application package
   - Safety case complete when all mitigations are validated with data

4. **FAA Approval**
   - Approval Granted If:
     - All hazards are addressed
     - Acceptable level of safety
     - Data verifies mitigations are effective
   - Novel approvals inform new policies, standards, and regulations

Increasing FAA Involvement
Defining the Operational Context

1. Operational Context Definition
   - Concept of Operations
     - Mission objectives
     - Operational description
     - Requirements definition
   - Risk Assessment
     - Hazard identification
     - Risk mitigation development
     - Identify supporting data needed
   Repeat until risks are mitigated to acceptable level

2. Data Collection
   - Test Planning
     - Test/data requirements
     - Scope and method of test
     - Schedule and resources
   - Testing & Demos
     - Quantitative data collected
     - Verify sufficient data to support mitigations
     - Data validates mitigations

3. Safety Case
   - Safety Case Compilation
     - Final analysis of safety
     - Compilation of all data
     - Completed application package
   Safety case complete when all mitigations are validated with data

4. FAA Approval
   - Approval Granted If:
     - All hazards are addressed
     - Acceptable level of safety
     - Data verifies mitigations are effective
   Novel approvals inform new policies, standards, and regulations

Increasing FAA Involvement
### A Familiar Risk Matrix

#### Virginia Tech UAS Operational Risk Matrix

<table>
<thead>
<tr>
<th>Severity Likelihood</th>
<th>Minimal</th>
<th>Minor</th>
<th>Major</th>
<th>Hazardous</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>5</td>
<td>10a</td>
<td>15a</td>
<td>20a</td>
<td>25</td>
</tr>
<tr>
<td>Probable</td>
<td>4a</td>
<td>8a</td>
<td>12a</td>
<td>16</td>
<td>20b</td>
</tr>
<tr>
<td>Remote</td>
<td>3a</td>
<td>6a</td>
<td>9</td>
<td>12b</td>
<td>15b</td>
</tr>
<tr>
<td>Ext Remote</td>
<td>2a</td>
<td>4b</td>
<td>6b</td>
<td>8b</td>
<td>14 *</td>
</tr>
<tr>
<td>Improbable</td>
<td>1</td>
<td>2b</td>
<td>3b</td>
<td>4c</td>
<td>8c</td>
</tr>
</tbody>
</table>

#### Risk Levels:

- **High Risk**: 13.1-25.0
- **Medium Risk**: 7.1-13.0
- **Low Risk**: 1.0-7.0

*Single Point or Common Cause Failures = Red / 14*

- Based on FAA’s risk matrix in SRM Policy 8040.4B
- Shared by DOD, DHS
- X axis (Severity)
- Y axis (Likelihood)
- Numbering added for easy cross reference and tracking
## Mitigating Risks – Casualty Example

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Hazard ID</th>
<th>Hazard Description</th>
<th>Hazard Assessment</th>
<th>Hazard Assessment Description</th>
<th>Mitigation ID</th>
<th>STAAR</th>
<th>Mitigation Action</th>
<th>Post Mitigation Assessment</th>
<th>Data to Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Casualty Risk</td>
<td>C</td>
<td>sUAS loss of propulsion leads to collision with person</td>
<td>9</td>
<td>Loss of propulsion due to battery power or loss of power train leads to uncontrolled descent into a person. Loss of power train may be caused by operator error with regard to preflight, battery monitoring or flight into an object that causes damage to propulsion system</td>
<td>C3</td>
<td>Reduces Severity</td>
<td>Limit altitude ceiling to acceptable level as determined in AIS Injury Testing. Reduces descent range to prohibit unacceptable injury risk.</td>
<td>6b</td>
<td>Acceptable injury thresholds and methods to evaluate injury risk of a specific UAS have been discussed in numerous papers and rulemaking committees and research conducted at Virginia Tech. At this time, the FAA has not accepted a standard for injury threshold or test method. However, based on two existing Part 107.39 waivers, there does appear to be acceptance that very small aircraft such as the PhotoKitePro (620 g. 1.37 lbs.) and Prox Dynamics PD-100 (18 g. 0.04 lb.) are safe for operations over people (OOP). Evaluating risk of AIS 2 and 3+ injury to the head, neck, and thorax through a series of controlled laboratory vehicle impact tests into an instrumented Hybrid III dummy.</td>
</tr>
</tbody>
</table>

Overall Category Risk: Low / 6
Example: Selecting an Aircraft

- Able to perform the mission
- Needed risk reducing features:
  - Proven reliability
  - Low injury risk
  - Optimized flight behavior/logic
- Reputable manufacturer
- Readily available
Best Practices: Operational Context Definition

1. **Bound the operation**
   - “Dream” operations versus “Minimum Viable Product”
   - Prevents implementing limitations/mitigations that eliminate the business case

2. **Narrow the context**
   - Start broad and iterate to specific
   - Ensures potential risk mitigations and technology are not overlooked

3. **Prioritize risk mitigations**
   - Some risk mitigations improve safety, but are not “critical path”
   - The amount of supporting data (i.e. “robustness”) likely depends on criticality
Traditional vs holistic approach

• Traditionally, manned aviation requests certification of the aircraft, approval of the operator and license of the pilot.
• Certification/approval/license provide a high level of assurance / confidence that an aircraft operation can be conducted with an acceptable level of risk.
• What is an acceptable level of risk?
  – In manned aviation, a Target Level of Safety (TLS) is the general term which designates the minimum safety objectives to be achieved expressed in terms of probability of potential fatalities on the ground or in the air.
Traditional vs holistic approach

• Unmanned aircraft are expected to meet the same TLS as manned aircraft.
• Does this mean that all UAS need to be certified, operator approved and pilot licensed?
• An holistic approach allows to take credit of operational or design mitigations to demonstrate that an operation can be conducted with an acceptable level of risk, e.g.
  – VLOS vs BVLOS
  – Independent flight termination system
  – Controlled ground area.
Why a (S)ORA?

- An ORA is a way to analyze a proposed ConOps and identify if there are sufficient mitigation means to conduct an operation with an acceptable level of risk.
- The SORA developed by JARUS provides a systematic methodology to identify in an holistic way risks associated to a UAS operation.
- This is the approach used in Europe to develop an operation centric, performance based and risk based drone regulation.
  - 3 categories: open, specific and certified
  - Open (intrinsic low risk): safety is achieved by limitations, competencies of the pilot, technical requirement for the UAS
  - Certified (intrinsic high risk): like for traditional aviation
  - Specific (intrinsic medium risk): risk assessment (SORA as AMC)
“Old School” Functional Hazard Assessments Work Too!
VLOS - Quite a Good Mitigation

• Learning Point – simply adapting a VLOS safety case to a BVLOS CONOP was much harder than I thought
  – When you give up the Mk I eyeball as a feedback mechanism, you lose your:
    • Icing sensor
    • Backup ADI
    • Obstacle detector
    • Aircraft collision detector
    • Wind Sensor
  – Hard to tell you’ve breached containment
  – Datalink Interference – “but I check on the spectrum analyzer”
“Old School” Functional Hazard Assessment

4. Operate

4.1 Avoid Collisions

4.1.2 Avoid Ground and Vertical Structures (while airborne)

4.1.2.1 Detect Ground & Vertical Structures

4.1.2.2 Track Relative Location of Ground & Vertical Structures

4.1.2.3 Provide Relative Location of Ground & Vertical Structures

4.1.2.4 Determine Corrective Action

4.1.2.5 Produce Corrective Action Command

4.1.2.6 Execute Corrective Action Command (accomplished in aviate)

4.1.2.7 Convey Post Corrective Action Status to ATC

4.2 Avoid Adverse Environmental Conditions

4.2.1 Detect Adverse Environmental Conditions

4.2.2 Track Relative Location of Adverse Environmental Conditions

4.2.3 Convey Relative Location of Adverse Environmental Conditions

4.2.4 Determine Corrective Action

4.2.5 Produce Corrective Action Command

4.2.6 Execute Corrective Action Command (accomplished under aviate)

4.2.7 Convey Post Corrective Action Status to ATC
Weather Hazards – Hidden in Plain Sight

- Even VLOS isn’t infallible!
- So, BVLOS requires considerably better information
- Where will you get it?
- Even if you had perfect information, do you know how your drone will really respond?

Real World Safety Incident

- Lack of wind measurements aloft
- Situation: VLOS – Loss of Control at 100 Feet AGI
- Followed the standard - hand held anemometer, TAF, METAR
- Result: Crash due to invisible threat lurking above
- Real Data Versus Inference - great deal of inference requiring knowledge of how the atmosphere works
“Land As Soon As Possible”

- Scenario – Single engine Helicopter
- Engine quits – Where are you going to land?
- You probably have about 5 seconds to decide before you lose link
- “That soccer field looked good on Google Earth, officer”
- So, all your contingencies become much harder to manage
Part 107 safety baseline

- Part 107 safety is based on Visual Line of Sight Flight as a primary risk mitigation.

- When performing operations Beyond Visual Line of Sight, many other rule compliance issues may arise. Some examples are:
  - 107.37-Operations near aircraft, right-of-way rules
  - 107.39-Operations over human beings
  - 107.51-Operating limitations for sUAS
Part 107 safety baseline

• Because of all the part 107 interdependencies on the LOS risk mitigation, waiver applications normally require a complete risk assessment of the operation for a waiver, when 107.31 is requested
  – Other rules have interdependencies including
    • 107.19
    • 107.23
Waiver experience

- 70-80% of waiver applications are disapproved for incomplete information
- The average waiver application is 1-2 sentences long
- Many applications do not address the whole risk and regulatory compliance for the proposed operation
Other Risk Tools

- FAA realizes traditional 8040 SRM process could be improved to account for sUAS operations
- Agency is actively working on augmenting the order to assist with UAS risk management
- SORA process has value in standardizing risk framework in operational applications
  - The underlying standards and support structure are not in place for SORA to be directly invoked
  - FAA is actively working on implementing SORA like methodology into the current Risk Management Framework