Safety Risk Management (SRM) Process Overview

Presented by: Everette C. Whitfield
Date: December 18, 2013 v0.2
Agenda

• Introduction

• System Overview

• Hazard Analysis Process
  + Describe System
  + Identify Hazards
  + Analyze Risk
  + Assess Risk
  + Treat Risk

• Close
  + Action Items
  + Next Step
Objective

- **SRM**
  - A methodology applied to all **NAS changes**
  - Ensures hazards are identified
  - Ensures an unacceptable risk is mitigated and accepted prior to making change

- A **NAS change** is any change to or modification of
  - Airspace
  - Airports
  - Aircraft
  - Pilots
  - Air navigation facilities;
  - Air traffic control (ATC) facilities
  - Communication
  - Surveillance, navigation and supporting technologies and systems
  - Operating rules
  - Regulations, policies, and procedures; and
  - People who implement, sustain, or operate the system components
AWD Safety Risk Analysis Phases

**Phase I**
- Change Proposed

**Phase II**
- Does it affect the NAS?
- Could this introduce safety risk into the NAS?
  - Yes: Further safety analysis conducted
  - No: No further analysis necessary

**Phase III**
- No further analysis necessary
  - Decision documented in SRMDM

**Phase IV**
- Further safety analysis conducted
  - Is Risk level Acceptable?
    - Yes: Risk level acceptable documented in SRMD
    - No: No further safety analysis necessary

**Phase V**
- Risk level Acceptable documented in SRMD

**Note:** Reference Phase V, mitigations initiatives can change previously "Unacceptable" threats to "Acceptable"
Figure 3.7: 5M Model

(hu)Man/Person:
- Operational Personnel
- Maintenance Personnel
- Engineering Personnel

Management:
- Operational Procedures
- Airspace Sectorization
- Maintenance Procedures

Machine:
- People’s interaction w/equipment
- Software
- Hardware

Media or Environment:
National Airspace System

Mission: Functions of system
Figure 3.5: SRM Safety Analysis Phases

1. **Describe System**
   - Define scope and objectives
   - Define stakeholders
   - Identify criteria and plan for risk management effort (including any modeling/simulation potentially required)
   - Describe system/change (use, environment, and intended function, including planned future configuration)

2. **Identify Hazards**
   - Identify hazards (what can go wrong?) that exist in the context of the NAS change
     - Use structured approach
     - Be comprehensive (and do not dismiss hazards prematurely)
     - Employ lessons learned and experience supplemented by checklists

3. **Analyze Risk**
   - For each hazard:
     - Identify existing mitigations/controls
     - Determine risk (severity and likelihood) of outcome
       - Qualitative or quantitative (preferred)

4. **Assess Risk**
   - Rank hazards according to the severity and likelihood of their risk
   - Select hazards for detailed risk treatment (based on risk)

5. **Treat Risk**
   - Identify feasible mitigation options
   - Develop risk treatment plans
   - Implement and verify
   - Monitor
Figure 3.9: Risk Matrix

- **Severity**
  - Minimal
  - Minor
  - Major
  - Hazardous
  - Catastrophic

- **Likelihood**
  - Frequent
  - Probable
  - Remote
  - Extremely Remote
  - Extremely Improbable

- **Risk Levels**
  - High Risk
  - Medium Risk
  - Low Risk

* Unacceptable with Single Point and/or Common Cause Failures
QUESTIONS?