Safety Management and the Use of EA

Presented to: NASEA Conference
By: James Daum, Safety Group Manager (AJP-19)
Date: June 25, 2009
Safety Management Basics

• What is safety?
  – Freedom from unacceptable risk

• What does the Safety Management System (SMS) provide?
  – The SMS provides a systematic and integrated method for managing the safety of Air Traffic Control (ATC) and navigation services in the NAS.

Aviation safety is the fundamental mission of the Federal Aviation Administration.
Safety Management System
Safety and NextGen

- **U.S. air transportation system (NAS) is the safest in the world**
- **NextGen safety objective**
  - Make the NAS **even more safe** than it already is.
- **Why the need to increase safety?**
  - Significant growth and increased complexity in the air transportation system requires commensurate improvement in safety performance.
- **How will we meet this NextGen safety objective?**
  - Evolve from today’s post-accident data analysis to integrated historical and prognostic evaluation and management of hazards and their potential safety risk to prevent future accidents.
  - Design the future air transportation system and safety management systems to control relatively benign events and how they combine in unexpected ways to create hazardous conditions.

> “ATO’s most fundamental imperative is to ensure the safety of the national airspace system. …

*Therefore, as we build the Next Generation Air Transportation System, the resulting cross-organizational changes to the NAS will require us to maintain an intensive, proactive, and systematic focus on safety. This focus is achieved through the implementation of the Safety Management System (SMS).”*  
Hank Krakowski, Chief Operating Officer, Air Traffic Organization
NextGen Safety Challenge

Maximized System

Safety

Efficiency
EA Helps Meet NextGen Safety Objectives

• **Programmatically via:**
  – The Safety Infrastructure Roadmap

• **Technically via:**
  – System Views to identify systems that support the SMS
  – Operational Views of how SMS integrates with NAS activities
  – Technical Views that document safety standards
  – System Views/Operational Views that feed the SRM process
  – System Views/Operational Views document SRM mitigations
  – System View Overlays to highlight areas of safety risk
Safety Infrastructure Roadmap

Safety Operational Improvements

NextGen Safety Objectives

EA Helps Meet NextGen Safety Objectives Programmatically via the Safety Infrastructure Roadmap

Safety Infrastructure Roadmap

Domain Infrastructure Roadmaps

Stakeholders

Safety Management and the Use of EA
6/25/09
Safety Systems

SV-1 System Interface Description

SV-4 Systems Functionality Description

EA Helps Meet NextGen Safety Objectives Technically via the System Views

Safety Management Services

• Trend Analysis
• Failure Prediction
• Risk Prediction
• Risk Management
• Safety Data Publication
Safety Management System

SMS Depiction in EA

Safety Management and the Use of EA

6/25/09

OV-5 Operational Activity Model
(future development)

EA Helps Meet NextGen Safety Objectives Technically via the Operational Views

SMS Integrated With NAS Activities
Safety Management Standards

### TV-1 Technical Standards Profile

<table>
<thead>
<tr>
<th>Standard Designation</th>
<th>Standard Title</th>
<th>Standard Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0 Aviation Related Standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.10 Safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAA NAS Mod SSMP</td>
<td>NAS Modernization System Safety Management Program</td>
<td>March 24, 2003</td>
</tr>
<tr>
<td>FAA AC 25.1309A</td>
<td>System Design Analysis</td>
<td>June 21, 1988</td>
</tr>
<tr>
<td>FAA Order 1100.161</td>
<td>Aviation Safety Oversight</td>
<td></td>
</tr>
<tr>
<td>FAA Order 8040.4</td>
<td>Safety Risk Management</td>
<td>June 26, 1998</td>
</tr>
<tr>
<td>FAA Order JO 1000.37</td>
<td>Air Traffic Organization Safety Management System</td>
<td></td>
</tr>
<tr>
<td>FAA SRMGSA V1.4a</td>
<td>Safety Risk Management Guidance for System Acquisitions</td>
<td>February 8, 2007</td>
</tr>
<tr>
<td>FAA SSH</td>
<td>System Safety Handbook</td>
<td>December 30, 2000</td>
</tr>
<tr>
<td>ICAO Annex 11</td>
<td>Convention on International Civil Aviation Aeronautical Telecommunication, Annex 11, Section 2.26</td>
<td></td>
</tr>
<tr>
<td>ICAO Doc 9859 AN/460</td>
<td>ICAO Safety Management Manual (SMM)</td>
<td>2006</td>
</tr>
<tr>
<td>RTCA DO-178B</td>
<td>Software Considerations in Airborne Systems and Equipment Certification</td>
<td>December 1, 1992</td>
</tr>
<tr>
<td>RTCA DO-264</td>
<td>Guidelines for Approval of the Provision and Use of Air Traffic Services</td>
<td>December 14, 2000</td>
</tr>
<tr>
<td></td>
<td>Supported by Data Communications</td>
<td></td>
</tr>
<tr>
<td>RTCA DO-278</td>
<td>Guidelines for Communications, Navigation, Surveillance, and Air</td>
<td>March 5, 2002</td>
</tr>
<tr>
<td></td>
<td>Traffic Management (CNS/ATM) Systems Software Integrity Assurance</td>
<td></td>
</tr>
<tr>
<td>SAE ARP4761</td>
<td>Aerospace Recommended Practice - Guidelines and Method for Conducting Safety</td>
<td>December 1, 1996</td>
</tr>
<tr>
<td></td>
<td>Assessment Process on Airborne Systems and Equipment</td>
<td></td>
</tr>
</tbody>
</table>

EA Documents Safety Management Standards Technically via the Technical Views

### TV-2 Technical Standards Forecast – in development

Safety Management and the Use of EA 6/25/09
EA Provides Input to SRM

Safety Risk Management Process
- Describe System
- Identify Hazards
- Analyze Risk
- Assess Risk
- Treat Risk

NASEA Views
SRM Results Feed EA

NASEA Views

Safety Risk Management Process

- Describe System
- Identify Hazards
- Analyze Risk
- Assess Risk
- Treat Risk

Mitigations Requiring Change in Architecture
EA Supports Integrated SRM

Integrated System of Systems Model-based Assessment

Mid-level Concept/Capability Safety Assessments

Acquisition Management System Safety Assessments: OSA, CSA, PHA, etc. (system- and program-level assessments)

Levels of Integrated Safety Analysis

Increasing integration

Step 1 - Automated Schedule Generation
Step 2 - ANSP Risk Assessment Evaluation and Sharing
Step 3 - ATCT/Ramp Coordination
Step 4 - FD Issues PDC
Step 5 - GC Issues Taxi Clearance
Step 6 - LC Issues Mid-level Takeoff Clearance
Step 7 - TRACON DC Monitors Departure Route

Model-Based Safety Risk Assessment

Schematic Block Diagrams
Interface Definition Diagrams
Architecture Block Diagrams

Safety Analysis

Safety Management and the Use of EA 6/25/09
Integrated SRM Supports EA

Levels of Integrated Safety Analysis

Increasing Integration

Assessment Results/Mitigations

NASEA Views
Safety Overlays

• Safety Overlays are currently in development for:
  - Far-Term SV-1, SV-2, & SV-4
  - Mid-Term SV-1, SV-2, & SV-4

• Safety Overlays highlight pertinent functions, systems, interfaces, etc. that could be a causal factor for catastrophic hazards should failure or degradation be realized.

EA Helps Meet NextGen Safety Objectives Technically via the Safety Overlays
Safety Management and the Use of EA

• **Summary**
  – NextGen safety objective → Make the NAS *even more safe* than it already is.
  – EA Helps Meet NextGen Safety Objectives via:
    • System View Overlays to highlight areas of safety risk
    • System Views to identify systems that support the SMS
    • Operational Views of how SMS integrates with NAS activities
    • Technical Views that document safety standards
    • System Views/Operational Views that feed the SRM process
    • System Views/Operational Views document SRM mitigations