ARMD Strategic Thrust 5: Real-time System-wide Safety Assurance Vision and Roadmap

Jessica Nowinski, Ph.D.
May 25, 2016
Why Real-time & System-wide?

10 year moving average accident rate per million flights*

*Below 10 years of operation, the moving average is based on the number of years of operation.

ARMD Roadmap Elements

Design Lifecycle

- Requirements
- Testing Certification Standards
- Best Practices Proficiency Standards
- Standard Procedures
- Scheduled Checks

Safety Assurance Methods

- FAA Airworthiness Directives
- ASRS Alerts
- Airline safety bulletins
- CBM

LIMITED MONITORING
RSSA Simplified Vision

**MONITOR**

Data Fusion

**ASSESS**

Monitor state, detect precursors & lead indicators

Prognostics, Prediction

Alerting

Decision Support

**MITIGATE**

Mitigation Response

**RSSA feedback loop:**
- More selective monitoring
- Improved models for assessment
- Evaluation and validation of mitigation strategies
- Supports existing offline safety assurance methods
System-wide and Distributed

- Awareness and analysis capabilities must be system-wide
  - Data sources cover the NAS for full system-awareness and accurate models
  - Analysis may occur at the domain level (e.g. models trained for a specific airport or aircraft type) but underlying capabilities are available and distributed system-wide

- Decision-making and authority must be distributed
  - Input for decision-making may be local or may require broader system-wide knowledge
  - Authority must be designated to the operator able to initiate real-time mitigations
## Community RSSA Outcomes by Epoch

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>2015</th>
<th>2025</th>
<th>2035</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Specific (Real-time) Safety Monitoring and Altering Tools</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrated Predictive Technologies with Domain Level Application</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Adaptive Real-time Safety Threat Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td>Expanded system awareness through increased access to safety relevant data and integrated analysis capability; improved safety through initial real-time detection and alerting of hazards at the domain level and decision support for limited operations</td>
<td>NAS-wide availability of real-time detection and alerting with initial assured decision support for mitigation response selection</td>
<td>Integrated detection, alerting and decision support tools; adaptive human-automation teaming for optimum threat management</td>
</tr>
</tbody>
</table>
## Community RSSA Outcomes by Epoch

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>2015</th>
<th>2025</th>
<th>2035</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Benefits</strong></td>
<td>Domain Specific (Real-time) Safety Monitoring and Alerting Tools</td>
<td>Integrated Predictive Technologies with Domain Level Application</td>
<td>Adaptive Real-time Safety Threat Management</td>
</tr>
<tr>
<td></td>
<td>Expanded system awareness through increased access to safety relevant data and integrated analysis capability; improved safety through initial real-time detection and alerting of hazards at the domain level and decision support for limited operations</td>
<td>NAS-wide availability of real-time detection and alerting with initial assured decision support for mitigation response selection</td>
<td>Integrated detection, alerting and decision support tools; adaptive human-automation teaming for optimum threat management</td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Safe/normal operation baseline</td>
<td>• Integrated system-level continuous monitoring in system-wide architecture</td>
<td>• Real-time intelligent safety monitoring</td>
</tr>
<tr>
<td></td>
<td>• Initial continuous real-time monitoring</td>
<td>• Assured access and analysis of secure data</td>
<td>• In-time integrated threat detection, prediction and mitigation process in a highly dynamic environment</td>
</tr>
<tr>
<td></td>
<td>• Real-time anomaly and precursor identification</td>
<td>• Trustworthy decision support tools</td>
<td>• Predictive safety-case for highly-automated and evolving aviation systems</td>
</tr>
<tr>
<td></td>
<td>• Real-time alerting of safety hazards</td>
<td>• Mitigation response capability for selected applications</td>
<td></td>
</tr>
</tbody>
</table>
Strategies for Thrust 5: RSSA

• Leverage growing sources of aviation data, commercial data analytics methods, “internet of things” to enable safety monitoring, prediction, and prognostics capabilities

• Conduct of fundamental safety research to understand the general or composite properties of, margins for, safe operations across the NAS and enable eventual broad RSSA capabilities

• Expand functionality through evolutionary development, demonstration and adoption of capabilities

• Leverage the strengths of both human and machine agents to support intelligent, adaptive mitigation strategies for optimum threat management

• Achieve stakeholder trust and consensus through frequent demonstration of benefits to ensure access to the rapidly growing body of safety relevant data from FAA, operators, and system providers
Key Dependencies

- **Data policy and regulation, stakeholder trust**
  - Access to sensitive data requires trust and cooperation of those who own key data sources (airlines, airports, ASIAS)
  - NASA can support trust and buy-in through rigorous assurance evidence and demonstration of benefits

- **Cybersecurity**
  - NASA is addressing some of the data assurance issues but will need to rely on the community effort and progress made by OGA, academia and industry.

- **Advances in Machine Learning and Computational Power**
  - Advances in machine learning—in particular advances in cognitive computing for support of automated response planning and execution—will require a community effort
  - Leverage the synergy of data analytics, intelligent systems technologies, machine learning, high performance computing and simulation from industry, academia and DoD

- **System-wide Implementation**
  - NASA will roll out assured methodologies and capabilities through individual operators (airlines, airports, ATC facilities)
  - Look to FAA for opportunities to support NAS-wide implementation (i.e., ASIAS, ASRS) to support a comprehensive, system-wide capability
Research Themes

Continuous System-wide Safety Awareness (Monitor)
Technical approaches and required architecture to support comprehensive safety monitoring through acquisition, integration and assurance of sensitive data from heterogeneous sources.

Safety Risk Identification and Evaluation (Assess)
Assured tools that improve the accuracy of real-time detection, diagnosis and prediction of hazardous states and the impact of these states on system safety.

Coordinated Prevention, Mitigation and Recovery (Mitigate)
Trusted methods for dynamic, multi-agent planning, evaluation, and execution of real-time risk mitigating response to hazardous events.

Experimentation, Demonstration and Assessment
Experimentation, demonstration, benefits analysis and transition of new RSSA technologies within all elements of the airspace.
# Real-time System-wide Safety Assurance

<table>
<thead>
<tr>
<th>2015</th>
<th>2025</th>
<th>2035</th>
</tr>
</thead>
</table>

## Monitoring
- Requirements for data capture and fusion
- System-wide models and metrics to characterize safe operations

## Assessment
- Matured analysis tools and techniques
- Tools to manage assurance throughout system-wide evolution
- Framework for Uncertainty Representation
- Tools for state awareness of all elements of the NAS

## Mitigation
- Initial decision support tools
- Methodologies and tools for integrated PMR plans with information uncertainty and system dynamics

## Demonstration
- Demonstration of data fusion and analysis tool predictive capability effectiveness for precursor detection
- Demonstration of notification and guidance to end users for domain specific individual safety event detection and mitigation

## Integration
- Integrated data transfer and fusion
- Operational integrity assurance on inputs to critical decision-making functions
- Design that enables full state awareness

## Applications
- Integrated Framework for interoperability with SMART-NAS
- RSSA communication application
- Monitoring frameworks for known risks

## Technologies
- Assured tools for complex airspace / aviation system-of-systems
- Assurance tools for predictive system components
- Tools for uncertainty propagation
- Design that enables full state awareness

## Tools
- Automated safety assurance for aviation state assessment systems
- Automated safety assurance for aviation state assessment systems
- Automated intelligent safety monitors for real-time system-wide aviation data collection approaches

## Systems
- Methods for automated tactical and strategic decision making
- Adaptive human-automation teaming for optimum threat management
- Automated execution agents for safety threat management

## Demonstrations
- Demonstration of integrated predictive capability effectiveness for safety relevant anomaly detection and mitigation across the entire NAS
- Demonstration of effective alert notification and guidance to end users for NAS-wide/system-wide safety event mitigation
- Demonstration of feasibility and effectiveness of autonomous/automated event mitigation based on RSSA detection and guidance
# Real-time System-wide Safety Assurance

<table>
<thead>
<tr>
<th>Year</th>
<th>Domain Specific (Real-time) Safety Monitoring and Alerting Methodologies and Tools</th>
<th>Integrated Predictive Technologies with Domain Level Application</th>
<th>Adaptive Real-time Safety Threat Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>Requirements for data capture and fusion</td>
<td>Integrated data transfer and fusion</td>
<td>Accommodation of dynamically evolving requirements, datasets, scenarios, and models</td>
</tr>
<tr>
<td></td>
<td>System-wide models and metrics to characterize safe operations</td>
<td>Operational integrity assurance on inputs to critical decision-making functions</td>
<td>Automated intelligent safety monitors for real-time system-wide aviation data collection approaches</td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
<td>Integrated Framework for interoperability with SMART-NAS</td>
<td>Automated safety assurance for aviation state assessment systems</td>
</tr>
<tr>
<td></td>
<td>Assessment</td>
<td>RSSA communication application</td>
<td>Multi-objective safety decision making</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>Methods for automated tactical and strategic decision making</td>
<td>Adaptive human-automation teaming for optimum threat management</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>Adaptive human-automation teaming for optimum threat management</td>
<td>Automated execution agents for safety threat management</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>Interface for automated mitigation</td>
<td>Demonstration of automated RSSA System in real world operations and hardware systems</td>
</tr>
<tr>
<td>2035</td>
<td>Demonstration of data fusion and analysis tool predictive capability effectiveness for precursor detection</td>
<td>Safe and effective human/machine teaming in PMR executions</td>
<td>Demonstration of feasibility and effectiveness of autonomous/automated event mitigation based on RSSA detection and guidance</td>
</tr>
<tr>
<td></td>
<td>Demonstration of integrated predictive capability effectiveness for safety relevant anomaly detection and mitigation across the entire NAS</td>
<td>Assurance tools for safety preservation systems</td>
<td></td>
</tr>
</tbody>
</table>
## Thrust 5

<table>
<thead>
<tr>
<th>Industry (OEM or operator)</th>
<th>Foundational safety research, including safety modeling and requirements</th>
<th>Product requirements</th>
<th>Supporting comm networks and architecture</th>
<th>Conceptual design</th>
<th>Capability design and test</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry (OEM or operator)</td>
<td>Foundational safety research, including safety modeling and requirements</td>
<td>Product requirements</td>
<td>Supporting comm networks and architecture</td>
<td>Conceptual design</td>
<td>Capability design and test</td>
<td>Operations</td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>NASA</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>FAA/Regulators</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DoD</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>University</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>