



Safety Requirements V & V

Mitigations to Safety Requirements and V&V

James Daum

Safety and Information Security Division Mgr, NAS Systems Engineering



FAA

Safety and Information Security Division, ANG-B

Safety Group

- SMS Implementation and Sustainment for ANG
- ANG SRM expertise and facilitation (Primarily Demos and Prototypes)
- System Safety support to Enterprise Architecture

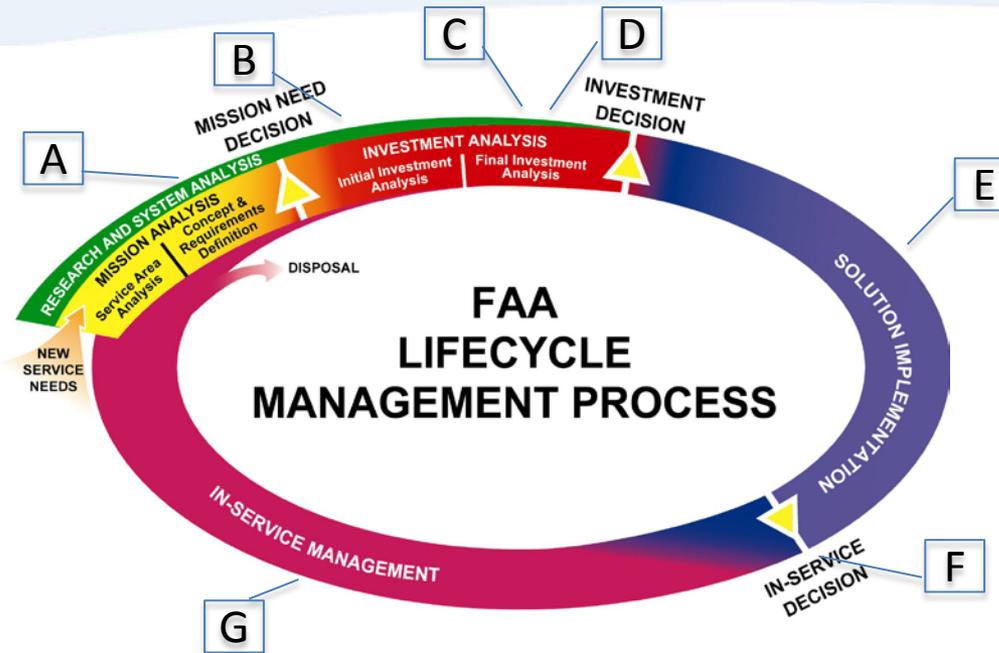
Information Security Group

- Information System Security authorization program for ANG
- ISS support to Enterprise Architecture

“STEWARDS OF THE NAS”



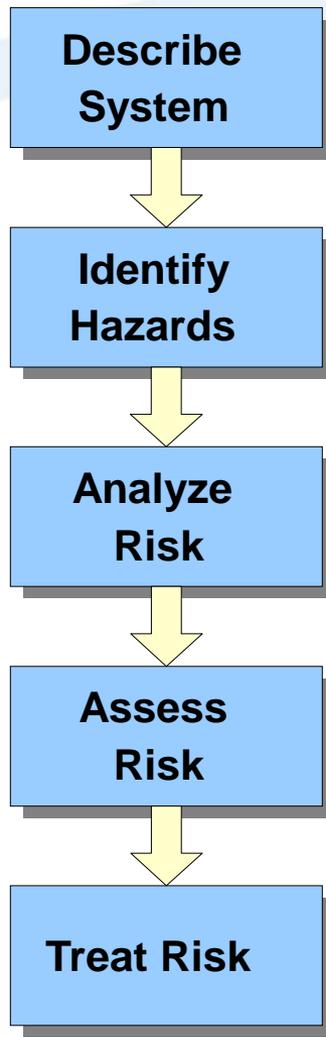
Safety Risk Management in the AMS



- A -- Operational Safety Assessment (OSA)
- B -- Comparative Safety Assessment (CSA)
- C -- Preliminary Hazard Analysis (PHA)
- E -- Sub System Hazard Analysis (SSHA)
 - System Hazard Analysis (SHA)
 - Operating & Support Hazard Analysis (O&SHA)
- F -- System Safety Assessment Report (SSAR)
- G -- Hazard Tracking & Risk Resolution (HTRR)
- Health Hazard Assessment (HHA)



SRM process



- 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)
- 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
- For each hazard:
- Identify existing mitigations/controls
 - Determine risk (severity and likelihood) of outcome
 - Qualitative or quantitative (preferred)
- Rank hazards according to the severity and likelihood of their risk
 - Select hazards for detailed risk treatment (based on risk)
- Identify feasible mitigation options
 - Develop risk treatment plans
 - Implement and verify
 - Monitor

Safety Risk Management

Severity \ Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	Low Risk	Medium Risk	High Risk	High Risk	High Risk
Probable B	Low Risk	Medium Risk	High Risk	High Risk	High Risk
Remote C	Low Risk	Low Risk	Medium Risk	High Risk	High Risk
Extremely Remote D	Low Risk	Low Risk	Low Risk	Medium Risk	High Risk
Extremely Improbable E	Low Risk	Low Risk	Low Risk	Low Risk	High Risk *

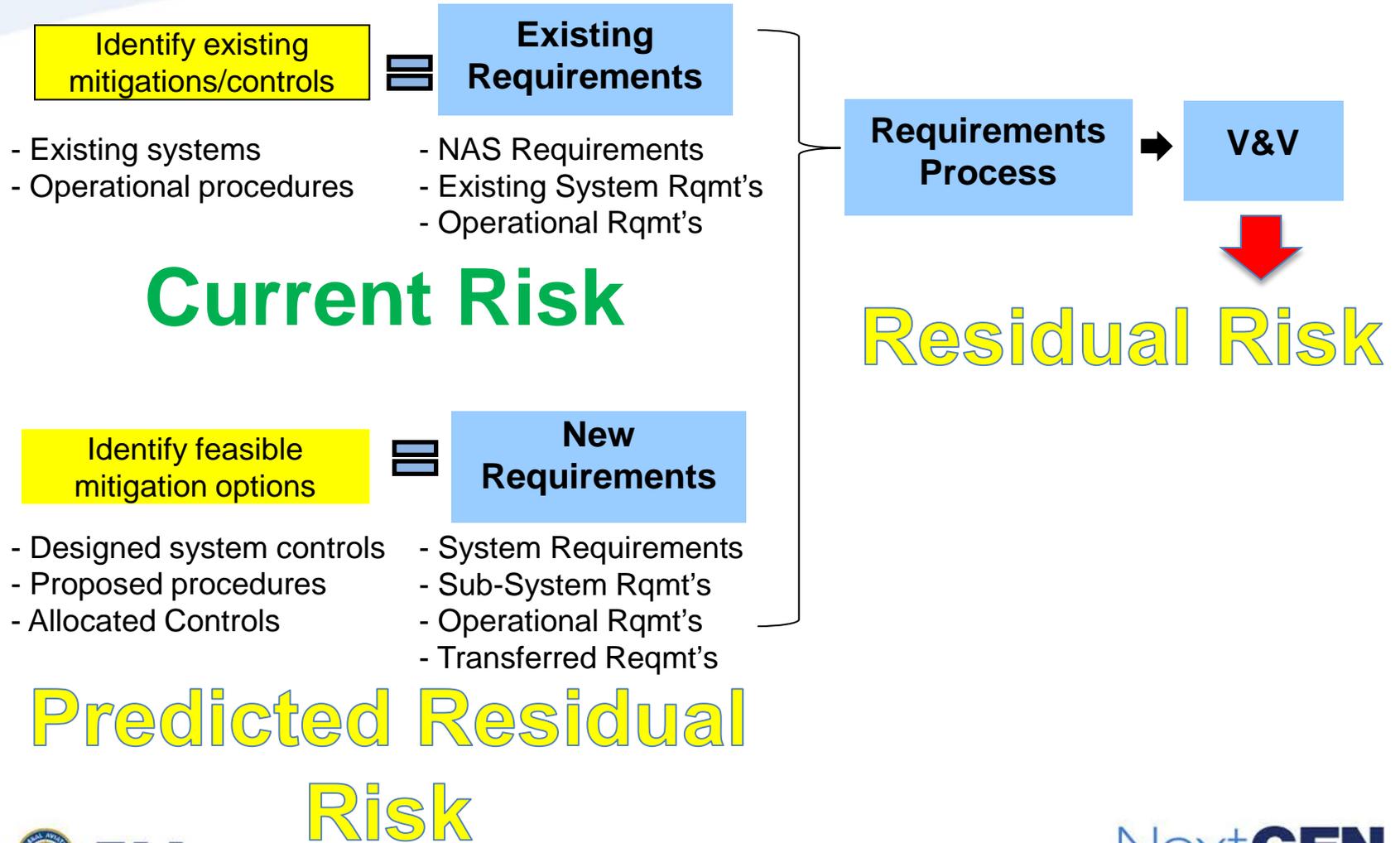
High Risk
Medium Risk
Low Risk

* Unacceptable with Single Point and/or Common Cause Failures

Where do Safety Requirements come from?

- SMS Manual v2.1:
 - **Safety Objective.** The least likelihood to achieve at least the minimum level of acceptable risk.
 - **Mitigation.** Actions taken to reduce the risk of a hazard's effects.
 - **Control.** Anything that **mitigates** the risk of a hazard's effects. A control is the same as a safety requirement. All controls are written in requirement language.
 - **Safety Requirement.** A **control** written in requirements language.

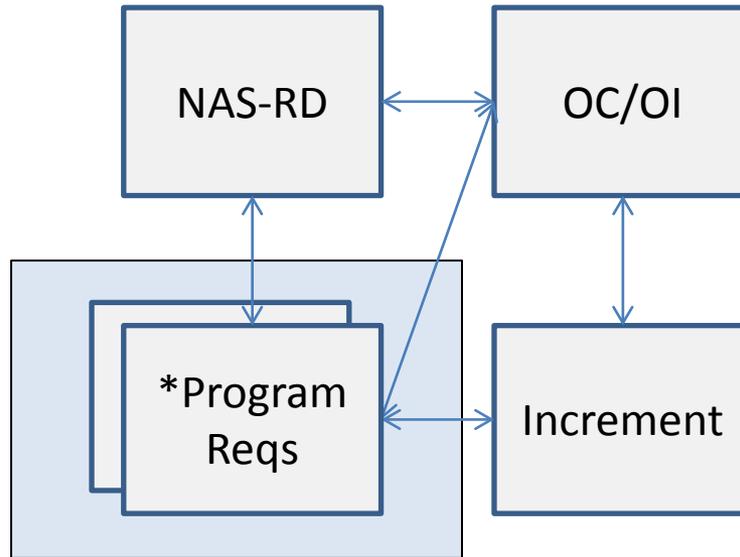
Safety Requirements Process



Current State

- Implementation of The Safety Management System has increased the awareness of SRM
- AMS requirements for SRMDs have improved the identification of hazards and the mitigations that have the potential to reduce safety risk
- With few exceptions SRMDs become “shelf ware” that have limited effect on reducing NAS safety risk
- Traceability of safety requirements to SRMDs is required to conduct V&V that results in accurate assessment of system residual risk
- Automation is required to provide associative links and relationships to V&V NAS Requirements

Benefit of DOORS: Traceability



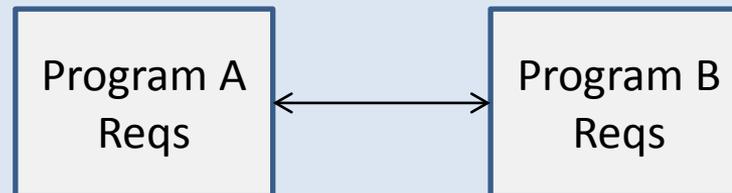
Attributes:

- Schedule
- Domain
- Performance Param
- Availability
- Success
- Benefits

Modules

- OC/OI, Inc, TF5
- Program
- NAS RD

** Dependent programs need to be linked as well*

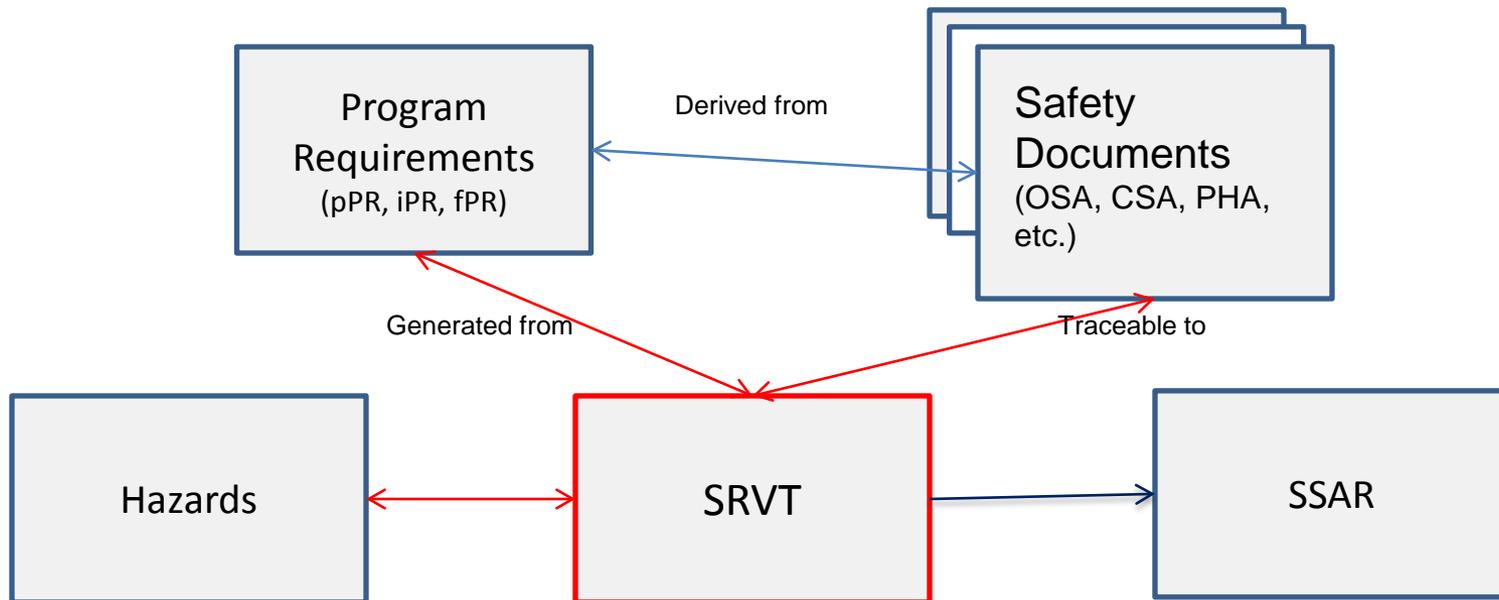


Benefit of DOORS: To Safety Requirements

Provide test engineers a tool to trace their safety requirements to the hazards they are mitigating.

Automate the generation of the Safety Requirements Verification Table (SRVT)

Identify accurate residual risk through V&V of safety requirements



DOORS: The Requirement – Hazard Connection

Requirements can be obscure and difficult to test without context to the hazard it's mitigating.

Requirement:

- 1: N JO 7110.xxx, 6c Inform all appropriate positions before terminating or reinstating use of the fusion automation system at a control position.
- 2: DO-260A 2.2.15 Power Interruption. The ADS-B transmitting and/or receiving equipment shall regain operational capability to within its operational limits within two seconds after the restoration of power following a momentary power interruption. [E02.102]

Hazard:

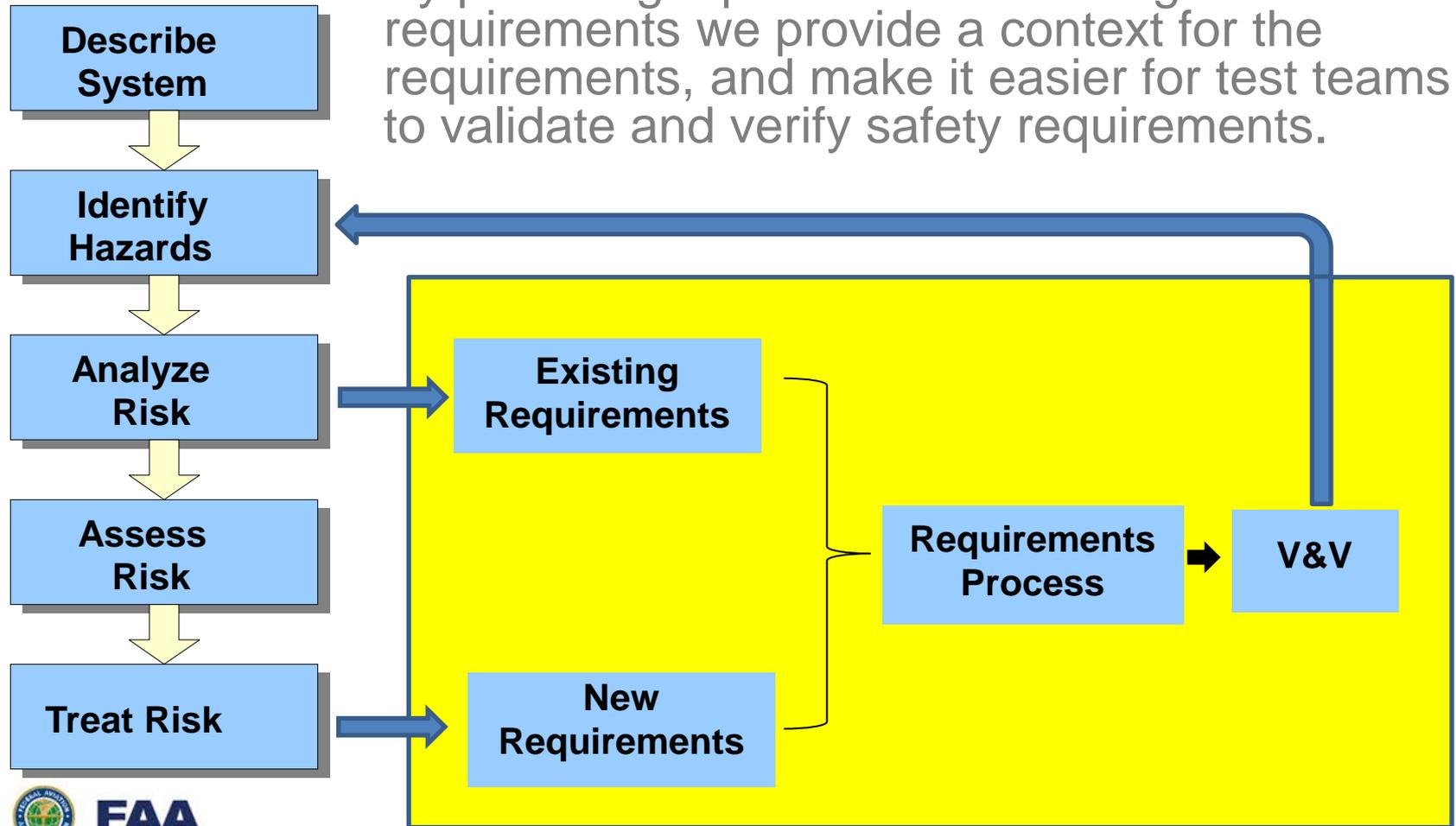
Loss of Surveillance for Multiple Aircraft on ATC Display While in Fusion Display Mode

Causes:

Power Distribution Unit Failure, Backup Generator Fails, ADS-B Server Hardware Failure, Power Failure Affecting the ADS-B Server , Switchover Between Ethernet 1 and 2 Does Not Complete

Making the Connection

By providing a process to turn mitigations into requirements we provide a context for the requirements, and make it easier for test teams to validate and verify safety requirements.



The Good News and The Bad News

Good News

- DOORS is now an AMS requirement
- Linkages to NAS and NextGen artifacts are currently being defined
- Automation is easy

Bad News

- Cross organizational collaborative processes are still needed to effectively and efficiently utilize the capability
- It may take time to develop enough data to provide enterprise analysis capability



Expansion of Capabilities: Traceability can be shown between...

- Enterprise Safety Requirements to Program Level Safety Requirements
- Enterprise Safety Requirements to Increments and Operational Improvements
- Program Level Safety Requirements to the Increments and Operational Improvements
- Program Level Safety Requirements to Program Level Hazards
- Portfolio Level Safety Requirements/Hazards

How do we achieve success

- Continue to provide your requirements that will maximize impact of the tool
- Collaborate to develop processes that provide mutual benefits

Questions:

James Daum

James.Daum@faa.gov

