

System Safety & Security

Exploring the technical and programmatic efficiencies to be achieved by integrating safety and security in a unified system lifecycle process

Ron Stroup
AIO-200
September 20, 2001

AIO-1 Brf



What is it we want to do?

- Jointly:
 - Develop a common mission
 - Jointly participate in all system (safety & security) analyses
 - Develop a common risk index
 - Develop common mitigation techniques
 - Develop a common lifecycle strategy
 - Develop an enterprise process to share, track, and monitor safety and security risks throughout the systems lifecycle and the NAS

Elements to achieving our goal?

- Commonality:

- Mission - Strategies
- Language - Process
- Model - Techniques
- Index

***Safety** is the state in which the associated **risks** that have been **identified** have been **accepted** provided that all identified **controls** are **implemented** and **enforced**.

- Communications & Coordination

- Roles and Responsibilities
- Program status
- Evidence of completion

****Information Security** is the security **measures** taken to **protect** information systems and the information of FAA information resources either individually or collectively.

*FAA System Safety Handbook

**FAA Order 1370.82

Common Mission ?

- Information Security:

- The FAA must **ensure** that **all information systems are protected from threats to integrity, availability, and confidentiality of those systems that support** the agency, **aviation safety and security**, and the NAS

(FAA Order1370.82)

- **Securing** the ATC computer systems that provide **information to controllers and flight crews is critical to the safe** and expeditious movement of aircraft

(FAA, Office of Information System Security, Program Management Plan, Version 1.0, August 29, 2000)

- Protect the FAA's information infrastructure through leadership in innovative information assurance initiatives

(FAA, Office of Information System Security, Program Management Plan, Version 1.0, August 29, 2000)

- Safety:

- By 2007, reduce U.S. aviation accident rates by 80 percent from 1996 levels.

(FAA Strategic Plan)

Language

Security

Asset

Criticality

Threats

Countermeasures

Vulnerability

Risk



Safety

System (People, Procedures, Equipment, Environment)

Severity

Hazard

Controls

Likelihood of Occurrence

Risk

Proposed Common Risk Index

Likelihood

Safety	Security	Definitions
Probable		Qualitative: Anticipated to occur one or more times during the entire system/operational life of an item. Quantitative: Probability of occurrence per operational hour is equal to or greater than 1×10^{-5}
	Extremely High	Given no changes, the vulnerability is so severe that if a threat occurs the probability that it will be successful in causing a loss event is extremely high.
Remote		Qualitative: Unlikely to occur to each item during its total life. May occur several time in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-5} , but greater than 1×10^{-7}
	Very High	The vulnerability is such that if a threat occurs the threat or loss event is much more likely to occur than not to occur.
Extremely Remote		Qualitative: Not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-7} but greater than 1×10^{-9}
	Moderately High	The threat or loss event is more likely to occur than not to occur.
Extremely Improbable		Qualitative: So unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet. Quantitative: Probability of occurrence per operational hour is less than 1×10^{-9}
	Low	The threat or loss event is less likely to occur than not to occur.



Safety		Security		No Effect	Minor	Major	Hazardous
Severity Likelihood	Severity Likelihood				Not Serious	Moderately Serious	Very Serious
Probable	Extremely High						High Risk
Remote	Very High						
Extremely Remote	Moderately High			Low Risk			
Extremely Improbable	Low						

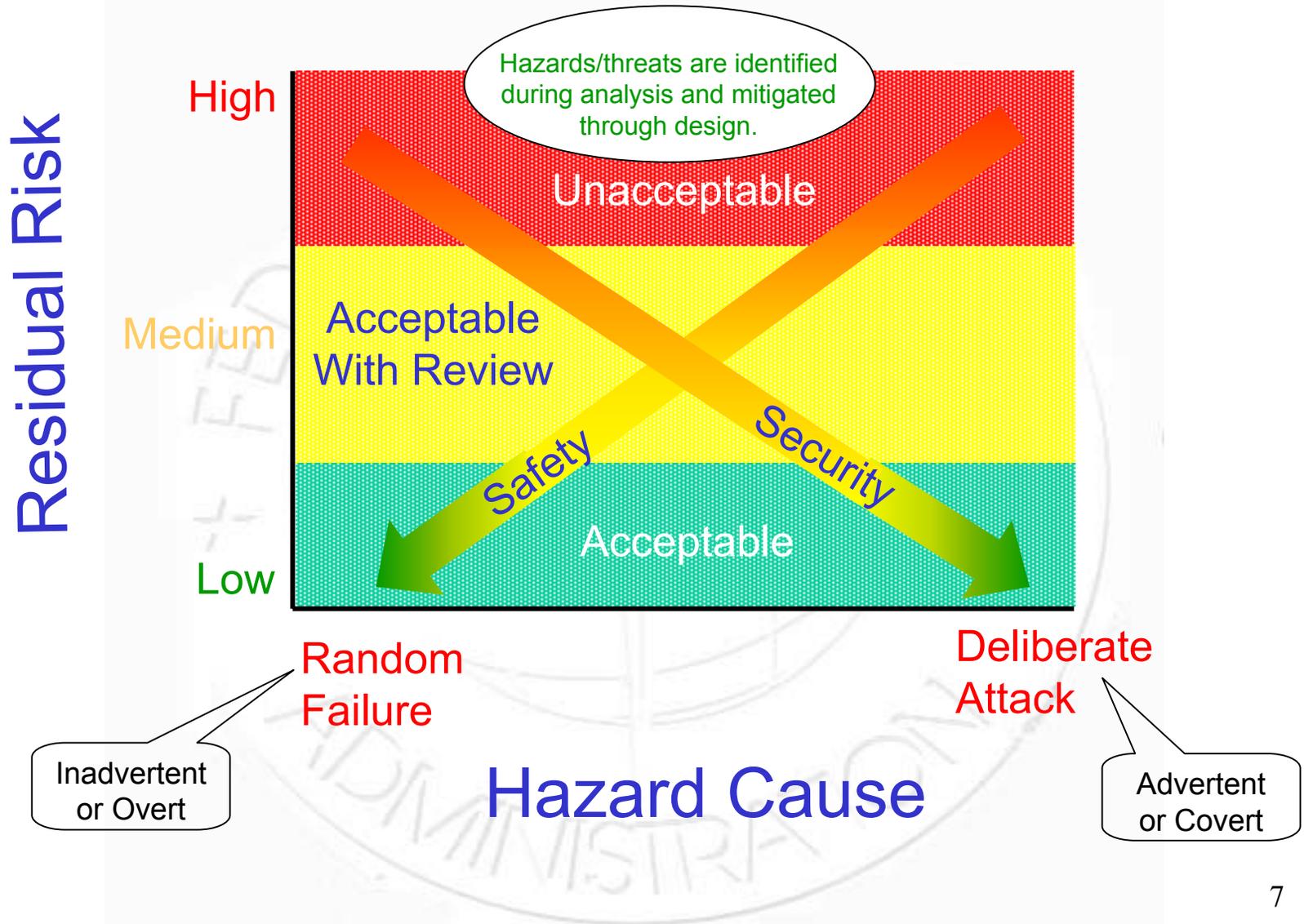


Severity



	Safety	Security	Programmatic Risk	
			Schedule	Cost
Catastrophic	Unacceptable – results in fatalities and/or system loss	Loss of mission capability for extended period.	No known way to meet program milestones	Development or acquisition costs increase > 10%
Hazardous	Large reduction in safety margin or functional capability	Consistent severe impairment of mission capability	Program critical path impact with workaround available	Development or acquisition costs increase .GT. 5% & .LTEQ. 10 %
Major	Significant reduction in safety margin or functional capability	Noticeable impact of the capability	Minor schedule slip, will miss need date without workaround	Development or acquisition costs increase .GT. 1% & .LTEQ. 5%
Minor	Slight reduction in safety margin or functional capability	No noticeable impact	Additional tasks required, able to meet key milestones	Development or acquisition costs increase .LTEQ. 1%
No Effect	No effect on safety	No effect on security	Minimal impact	Minimal impact

Collaborative Safety & INFOSEC Methodology



Techniques to Mitigate Risk

Order of Precedence

1. Design for defined acceptable risk
2. Incorporate safety devices
3. Provide warning devices
4. Develop procedures and training

Safety

Barriers/Partitioning

Monitoring

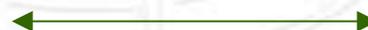
Protocol

Password

Checksums/CRC's

Safety Kernel

Procedures/Training



Security

Firewall

Monitoring

Handshake

Password

Encryption

Security Kernel

Procedures/Training

Next Steps

- Continue stakeholder briefings (ACO, ISSM, etc.)
- Create a core team (6-8 SME's)
- Develop common risk index
- Develop common risk mitigation techniques
- Propose and implement policy and implementation guidance

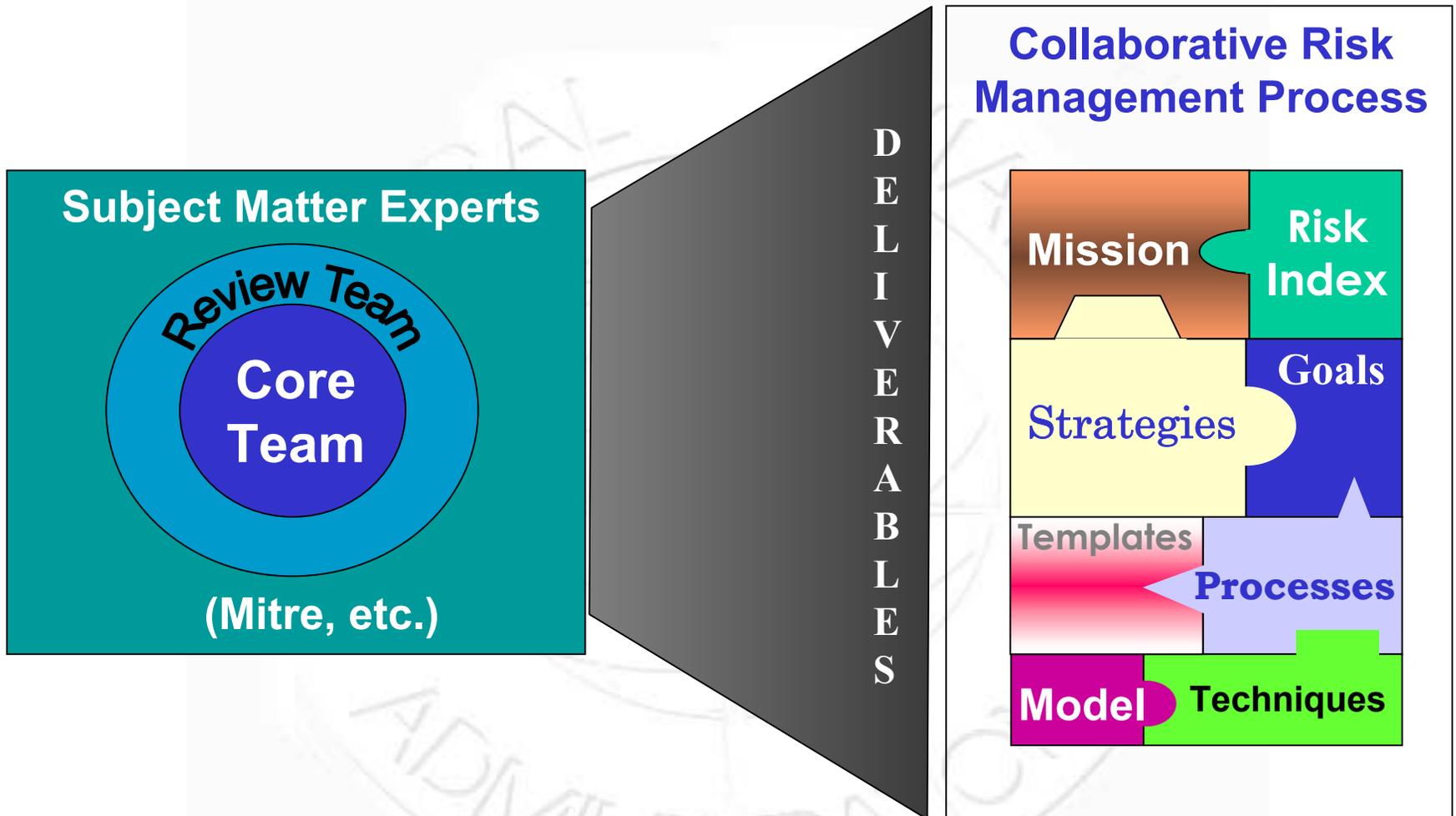
What do we need from you?

- We need ISS resources to participate on the core team
- We need to brief the ISSMs
- We need AIO to accept and identify the integration of safety and security as a priority in the FY02 Work Plan

Back-up Slides



Team Strategy



Do we proceed in a formal or informal manner? ¹²

Safety and Security Definitions:

- **Safety** is the state in which the associated risks that have been identified have been accepted provided that all identified controls are implemented and enforced.

FAA System Safety Handbook

- **Information Security** is the security measures taken to protect information systems and the information of FAA information resources either individually or collectively.

FAA Order 1370.82

**Primary Goal: Enhanced Safety &
Security While Maintaining Performance**

Goals

ENHANCED SAFETY & SECURITY WHILE MAINTAINING PERFORMANCE

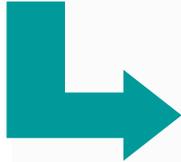
- Develop a common mission
- Improve cooperation:
 - Promote a common, coordinated, and comprehensive assessment process
 - Develop and participate in a joint assessment review
 - Prevent conflicting requirements
 - Develop common mitigation techniques
 - Information sharing
 - Lifecycle monitoring
- Ensure product team focuses on implementing requirements

Common Safety/Security Strategies? (Proposed)

- Error prevention through design assurance that could potentially lead to accidents
- Safety information sharing and analysis
- Approval and lifecycle monitoring
- Ensure coordinated goals among all stakeholders

Safety and Security Process

ANALYSIS



REQUIREMENTS



SOLUTION



VERIFICATION

SECURITY

- Threat Assessment
- Risk Determination
- Security Requirements
- Penetration testing

—
—

SAFETY

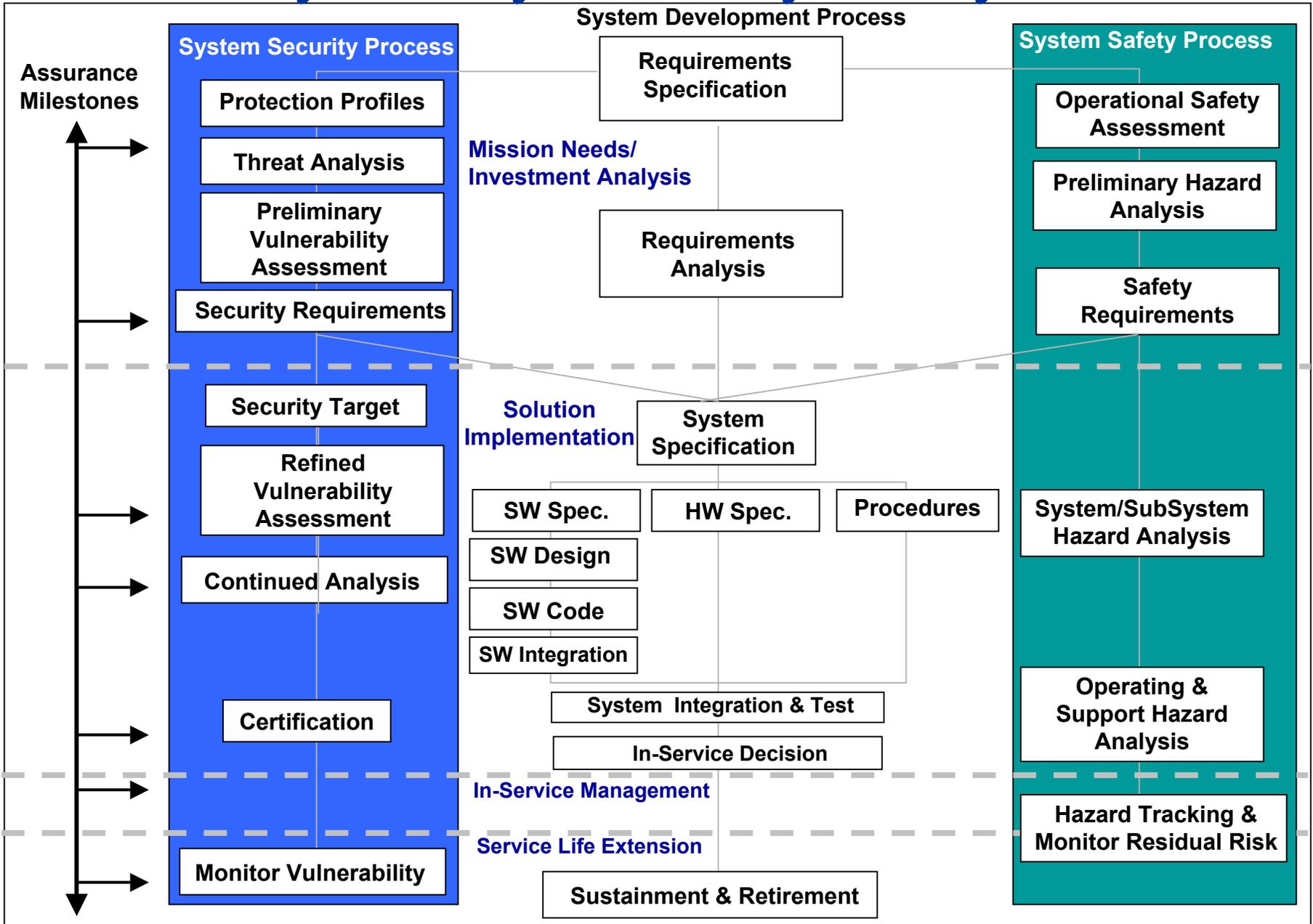
- Hazard Analyses
- Risk Determination
- Safety Requirements
- Requirements-based testing

Benefits

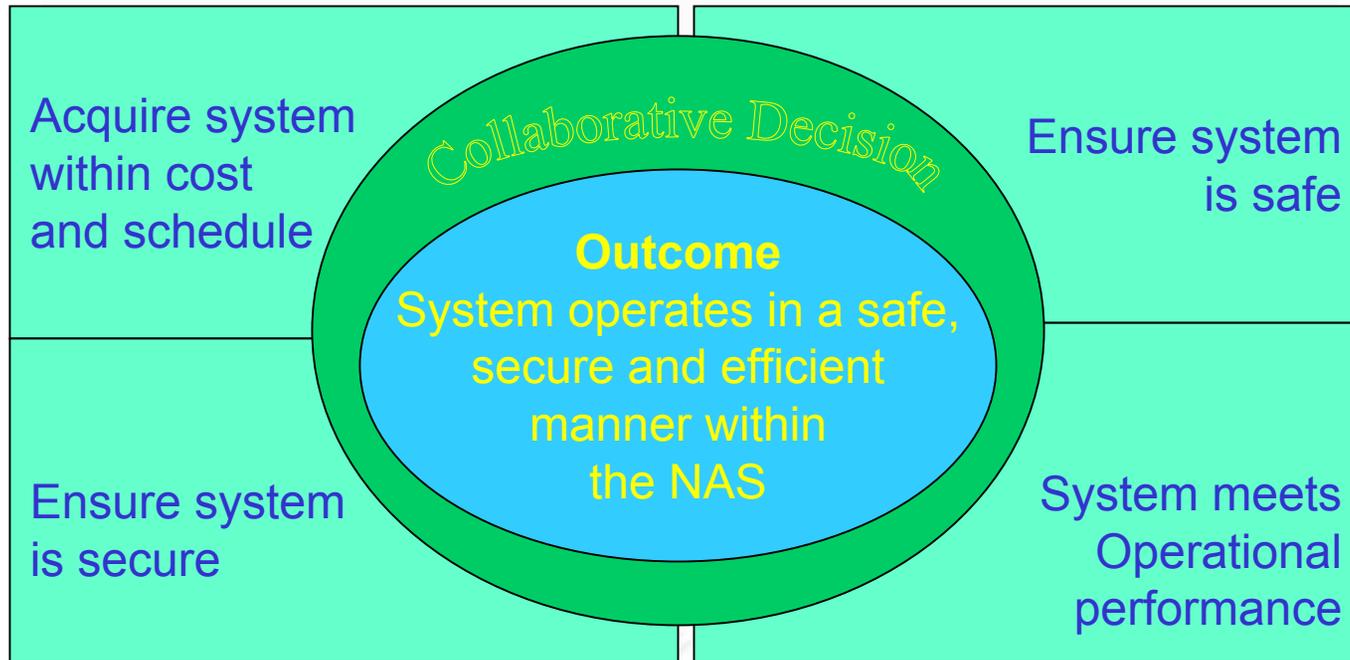
Benefits of a Common, Coordinated, and Comprehensive NAS Safety and Security Process:

- ✓ **Reduction of wasteful false starts**
- ✓ **Reduced costs**
- ✓ **More timely completion of needed changes**
- ✓ **Improved coordination with internal and external stakeholders**
- ✓ **Mitigation of conflicting requirements**
- ✓ **Building safer and more secure systems**

Preliminary Safety/Security Analyses Model



Communications & Coordination

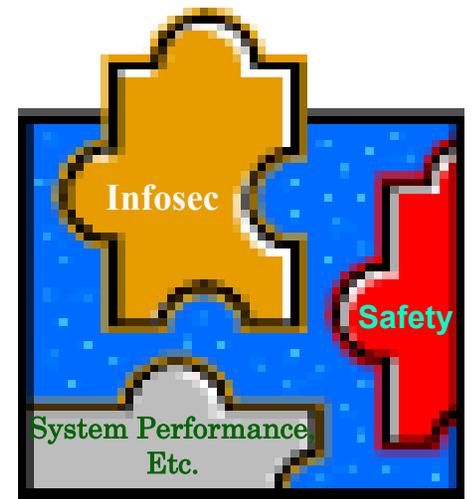
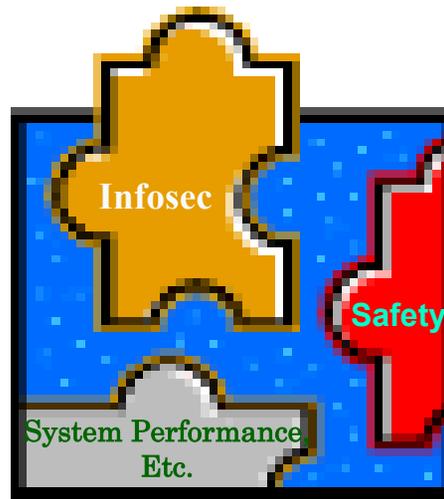
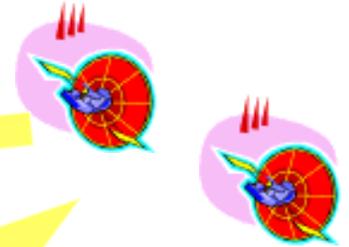
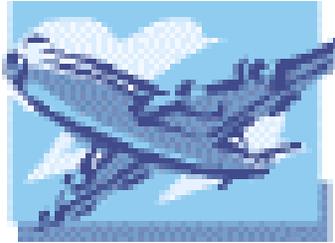


What must be communicated & coordinated

- Operational Concept Definition
- Performance Standards
- Risk Assessments
- Schedules and Commitments

Goal: Enhance Safety and Security while Maintaining Performance?

National Airspace System



Informed Decisions – Where Do We Spend \$\$\$?

