



# ***Security Certification and Accreditation Analysis for UAS Control & Communications***

Chris A. Wargo  
Mosaic ATM, Inc.



# Outline

---

- Background of RTCA SC-203 Unmanned Aircraft Systems (UAS) standards development activities
- Overview of the Federal Information Systems Security (ISS) requirements – policy framework
- ISS and the UAS perspective
- Overview of study approach
- Building requirements using the risk management methodology
- Summary and status

Disclaimer: Informational Paper Only

# RTCA Activity Background

---

- RTCA SC-203 Unmanned Systems
  - Joint Government and Industry Consensus body to develop technical performance requirements and standards
  - Published results in MASPS and MOPS that become the common standards for acquisition/equipage by all stakeholders
  - Use for certification invoked by subsequent FAA Order
- Working Group 2: Control & Communications
  - Air-to-Ground Communications
    - ATC Communications
    - Classic UAS Control
  - Multiple Connectivity Approaches
    - Includes alternative network alternatives for air traffic control communications
    - Voice and Data
  - Ad-hoc Information System Security Subgroup
    - 1<sup>st</sup> Issue Paper Security Concerns and Technology Approaches
    - 2<sup>nd</sup> Issue Paper is an attempt to focus on Analysis Task Plan to Determine Requirements
- Start of activities under SC-216 Aeronautical Systems Security

MASP: Minimum Aviation Systems Performance Standards

MOPS: Minimum Operational Performance Standards



# SC-216 Aeronautical Systems Security

---

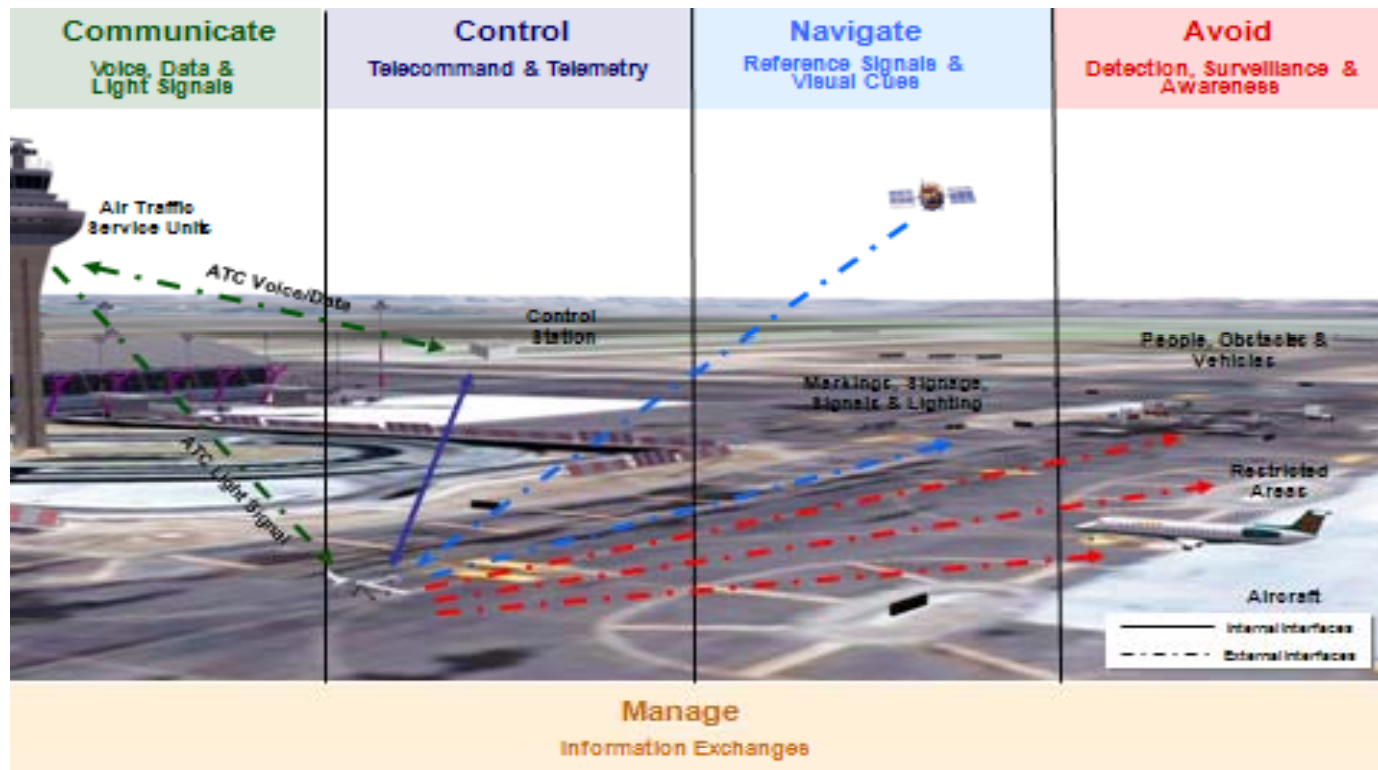
- Ongoing RTCA review of a number of committees seeking security guidance
- Results of recent SC-203 Plenary and WG 2 discussion
- SC-203 leadership wants to take another try at passing security requirements action to SC-216

# NIST/FISMA/FAA Order 1370.82A

---

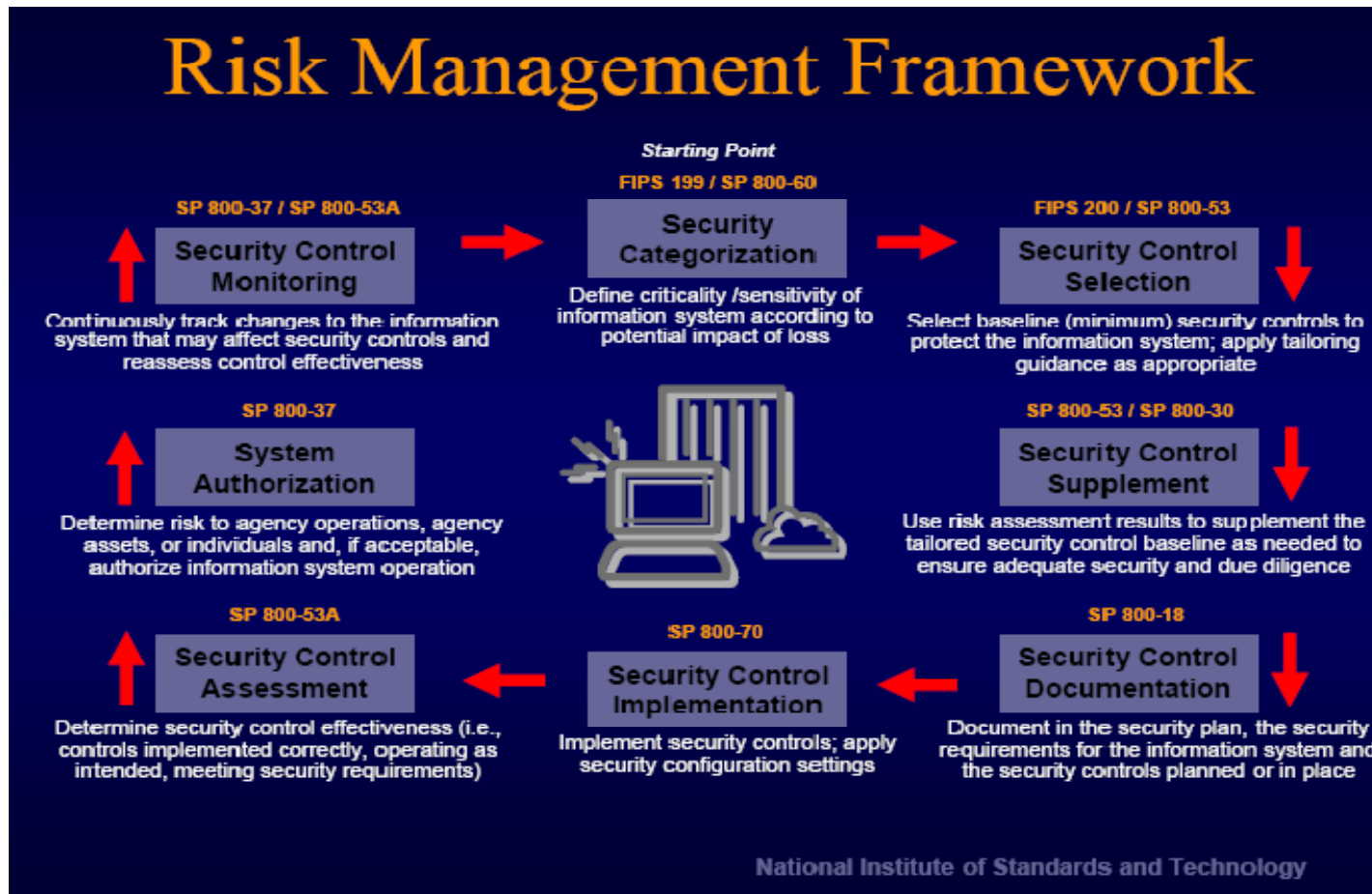
- Background on NIST and Federal developments for Information Systems Security
- Basis of the FAA's Information Security Program
  - FAA Order 1370.82A
  - Use of Federal Publication F199 to “Characterize the System”
    - Risk Management Framework Approach
    - Outcome is to characterize the level information assurance controls imposed – Example:  
$$SC_{xxx} = \{(\mathbf{Confidentiality}, \text{Moderate}), (\mathbf{Integrity}, \text{low}), (\mathbf{Availability}, \text{low})\}$$
- Documenting the System Characterization and ISS Plan (ISSP) – third product is the Continuity and Disaster Recovery Plan.

# UAS Operational View



Range of Mission Types

# NIST Process Framework



## WG2 ISS Subgroup - Risk Management Framework

---

- For our purpose we took the RMF to be six steps:
  - Categorize the System
    - Use of Enterprise, or Industrial Controls
  - Perform the Threat Identification
  - Vulnerability Identification\*
  - Select an Initial Set of Controls
  - Authorize the System
  - Monitor the System
- \* Risk Management Framework works best on a “well” designed system; i.e., one that the components can be described in detail.
  - How to go about setting a standard..... We don't have the luxury of one fully documented and designed system?

# Initial Consensus – Work Plan Premise

---

- WG2 ISS Subgroup work efforts should follow the FAA ISS Process (FISMA/NIST based).
- The analysis must take a “whole systems” point of view – i.e., cannot just address Control and Communications Link in isolation.
- Would use the approach of defining a “Reference Model”
- Work products should conform to FAA templates were possible.
- Expect to engage FAA for review and consensus
- Work is Information Assurance (IA) controls centric
- Additional work will be required to translate the results into requirements.
- Need to conduct work in open forum

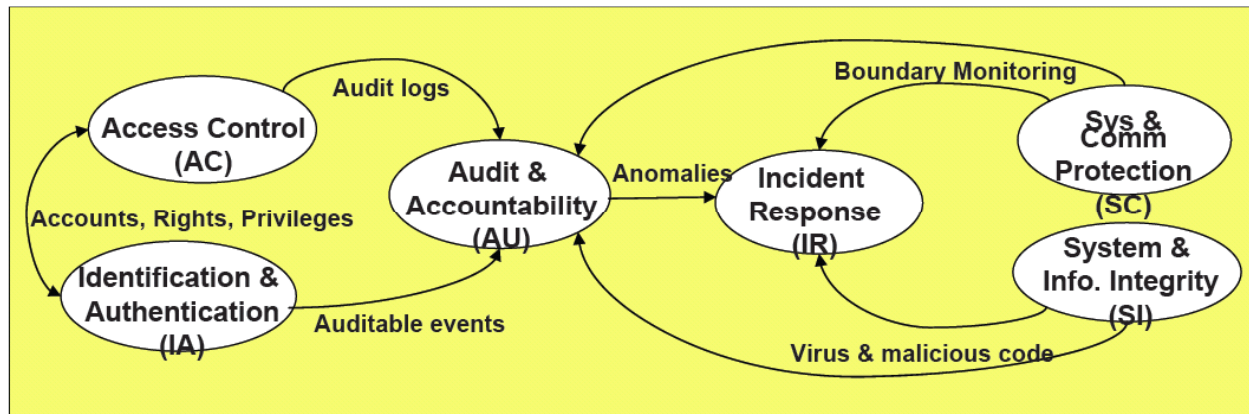
# IA Controls

---

- NIST 800-53 Definitions
  - Management, Operational and Technical
  - For Example, Moderate Level has 283 IA Controls (counting enhanced controls)
- Use of DOT Standard Implementation Guidance for some controls.
- To aid in confirming what constitutes sufficient migration, it would be expected to engage FAA ISSM Office for review and comment
- Desire to follow current NAS intent to use Enterprise Controls

# IA Control Types

## NAS Security Environment – 6 Technical Control Areas



- Identifying Enterprise and System Requirements
  - Access Control (AC)
  - Identification & Authentication (IA)
  - Audit & Accountability (AU)
  - Incident Response (IR)
  - System and Communication Protection (SC)
  - System & Information Integrity (SI)

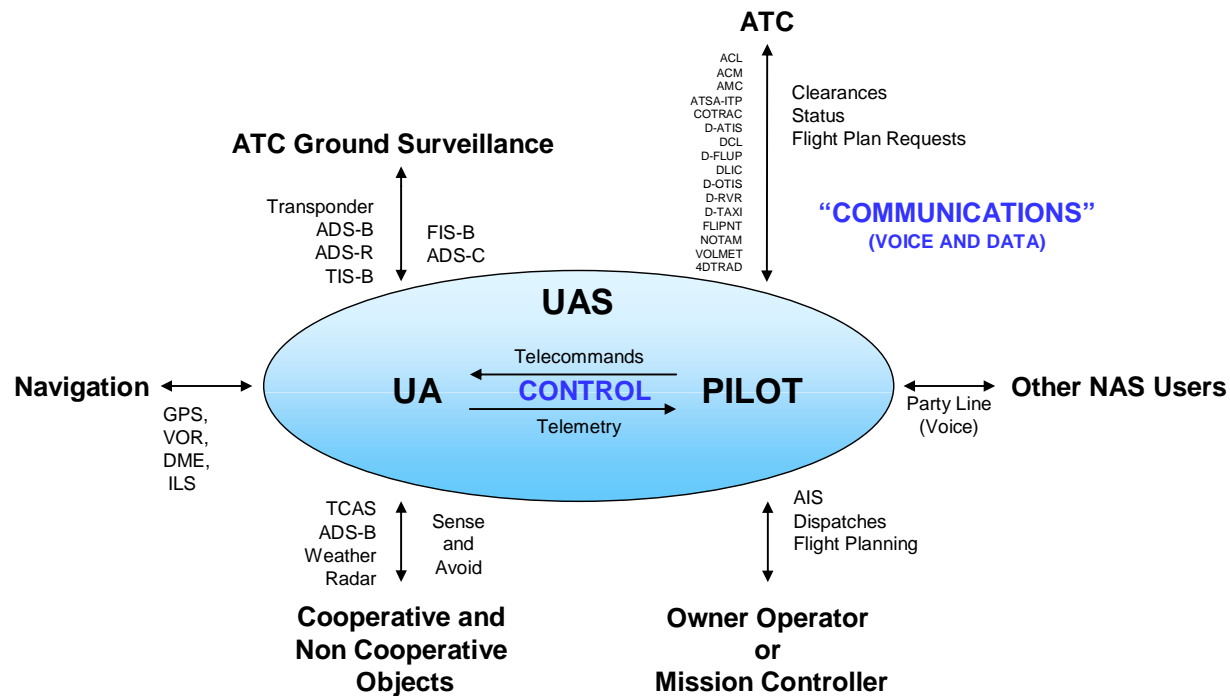
# Defining the Reference Model

---

- Want to keep generic as possible, but need very specific components.
- Dealing with multiple architecture approaches:
  - Currently ten different approaches defined by WG2
  - Differing points of connectivity for information flows
  - Wide range of possible combination of controls

# Types of Information Flows

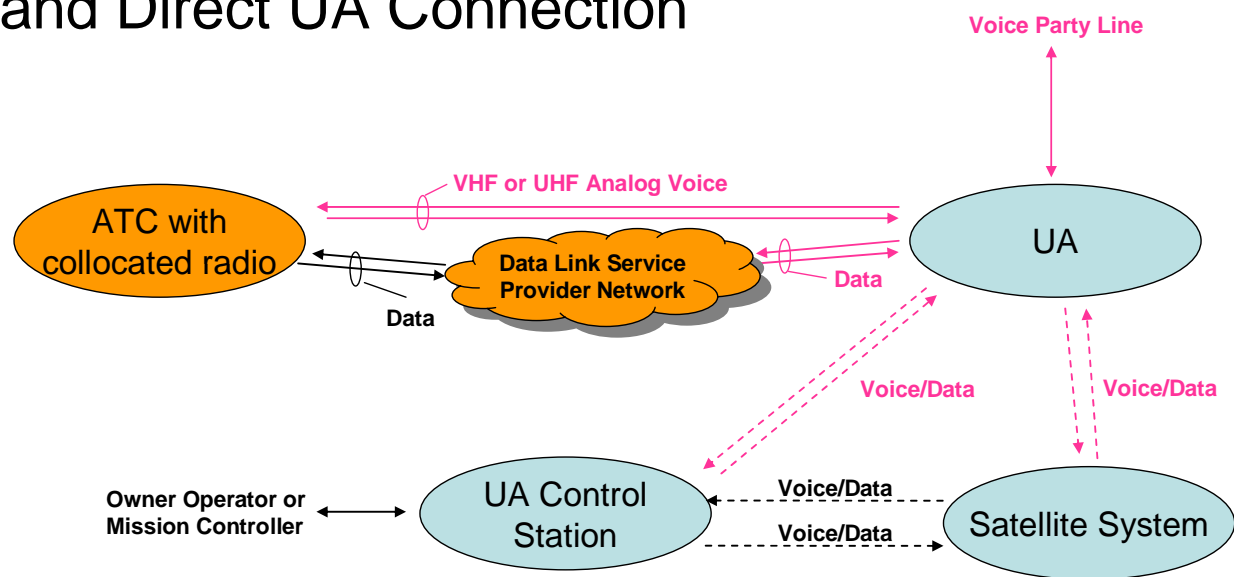
## UAS Internal and External Information Exchange



# WG2 Has Defined Multiple Architectures

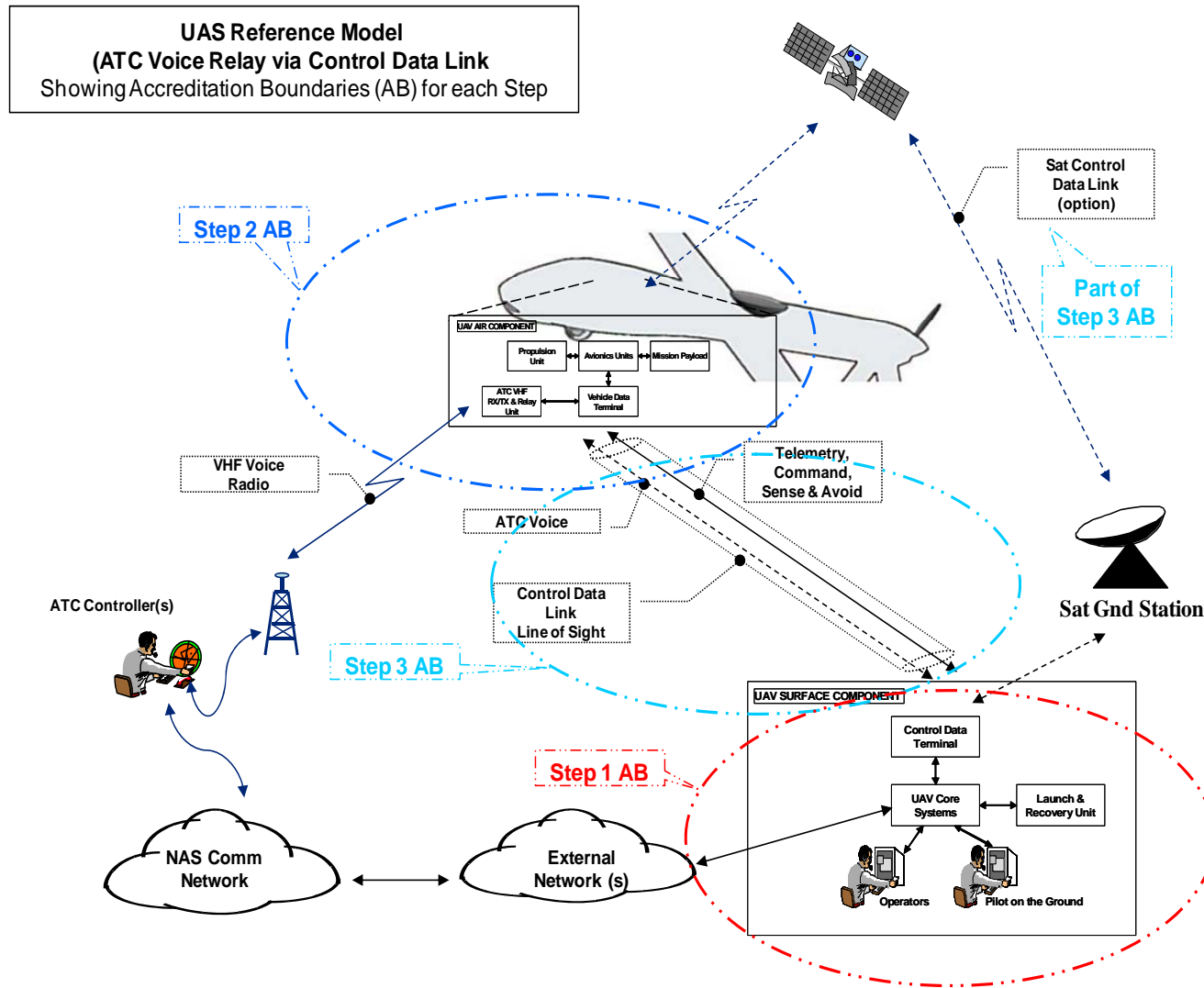
*Example: UA Relay 1 (CD) which is one of ten defined C & C Architectures*

## UA Relay Architecture ATC with Collocated Radio and Direct UA Connection



UA Relay 1  
(CD)

# UAS System – High-level Reference Model



# WG2 ISS Subgroup Task Pan

---

- Task 0: Definition of the Reference Model
  - High-level Definition
  - Incremental Low-level detail expansion (same technique as in defining a WBS)
- Task 1: Categorize the System
  - Subtask 1A: Determine the System Categorization
  - Subtask 1B: Determine the accreditation Boundary
- Task 2: Risk Assessment, Security Controls and Security Plan
  - Subtask 2A: Risk Assessment
  - Subtask 2B: Recommendation of Selected Controls
  - Subtask 2C: ISSP Preparation
- Task 3: Translation to Requirements

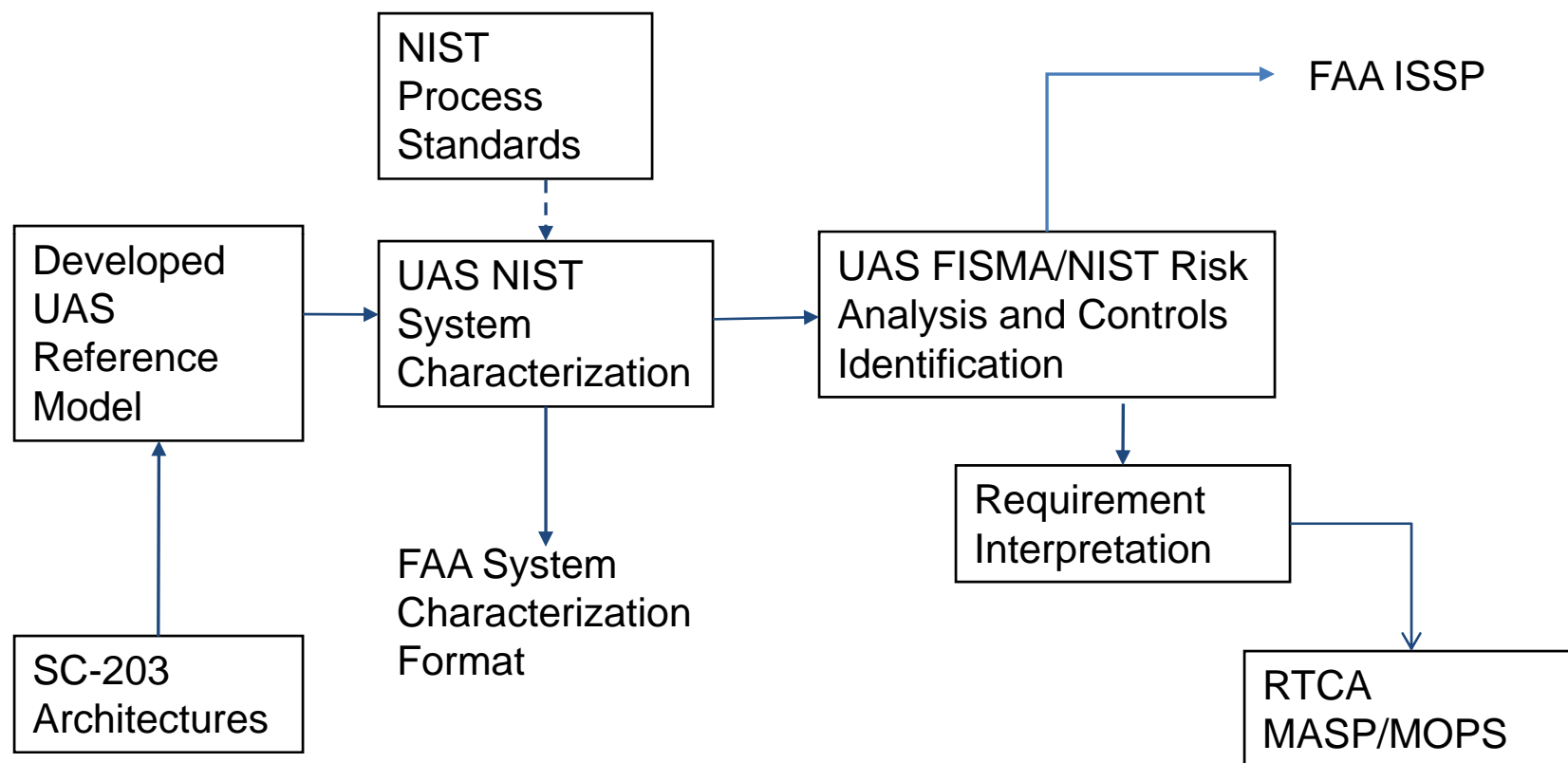
# Challenge Issues

---

- Level of definition to specify a security requirement
- Safety and Security
- Do the level of imposed controls vary by Class of UAS?
- Degree to which the Pilot on ground is seen as “part of NAS” and thus all Information Systems are viewed as under FAA Order 1370.82A

# Security Analysis Workflow

---



# UAS Information Security Analysis Plan

FAA C & A	Joint Benefit	RTCA UAS SC-203 WG2 Ad-hoc ISS SG
<ul style="list-style-type: none"> <li>• FAA Order 1370.82A</li> <li>• DOT FAA Information Security C&amp;A Handbook</li> </ul>	<ul style="list-style-type: none"> <li>• Using the same NIST Based Approach (FISMA):</li> <li>• FIPS 199 Security Categorization and use of NIST 800-53 Information Assurance Controls</li> <li>• NIST SP-800-30 Risk Management Guide</li> </ul>	<ul style="list-style-type: none"> <li>• WG 2 Control and Communications Issue Paper WG2-S1-010-D.</li> <li>• WG 2 consensus on plan approach achieved Oct 08</li> </ul>
<ul style="list-style-type: none"> <li>• System Characterization Document FAA FY09 Template</li> </ul>	<ul style="list-style-type: none"> <li>• System FIPS 199 Security Categorization = { Confidentiality, Integrity, Availability }</li> <li>• Impact Level of Information Assurance Controls can be presented for FAA Review by ISS Management and Certification Office</li> </ul>	<ul style="list-style-type: none"> <li>• Reference Model Characterization (use of System Characterization FAA Templates):</li> <li>• Information Category Interfaces Analysis:               <ul style="list-style-type: none"> <li>A. Ground Control</li> <li>B. Control link</li> <li>C. Air Vehicle</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>• Information System Security Plan (FY09 Template)</li> </ul>	<p>Results can be presented to FAA for review by ISS Management and Certification office</p>	<ul style="list-style-type: none"> <li>• Analyze each applicable IA Control (Use FAA Template)</li> <li>• Translation to MASP Requirements</li> </ul>
Continuity and Disaster Recovery Plans	TBD	TBD

**ISS: Information Systems Security**

**NIST: National Institute of Standards and Technology**

**WG2-S1-010-D: Approach for Certification and Accreditation Analysis for Security of the Control and Communications Link for Unmanned Aircraft Systems**



# SC-203 Security Analysis Work Plan

---

- Three Phase Approach
  - Ground Control Element
  - Control Data Link
  - Air Vehicle
- Leverage technical results from the unfolding SC-216 initiative
- Study to focus on the most likely Reference Model(s)
  - With two options (LOS VHF and BLOS SATCOM)
  - Need to decide on how to fit with Ground-Based Sense and Avoidance into Reference Model
- Next Steps
  - Await SC-216 response

BACK-UP

# 4.0 TECHNICAL CONTROLS (example)

---

- 4.1. Identification and Authentication (IA)
- 4.1.1. Identification and Authentication Policy and Procedures (IA-1)
- 4.1.2. User Identification and Authentication (IA-2)
- 4.1.3. Device Identification and Authentication (IA-3)
- 4.1.4. Identifier Management (IA-4)
- 4.1.5. Authenticator Management (IA-5)
- 4.1.6. Authenticator Feedback (IA-6)
- 4.1.7. Cryptographic Module Authentication (IA-7)
- 4.2. Access Control (AC)
- 4.2.1. Access Control Policy and Procedures (AC-1)
- 4.2.2. Account Management (AC-2)
- 4.2.3. Access Enforcement (AC-3)
- 4.2.4. Information Flow Enforcement (AC-4)
- 4.2.5. Separation of Duties (AC-5)
- 4.2.6. Least Privilege (AC-6)
- 4.2.7. Unsuccessful Login Attempts (AC-7)
- 4.2.8. System Use Notification (AC-8)
- 4.2.9. Session Lock (AC-11)
- 4.2.10. Session Termination (AC-12)
- 4.2.11. Supervision and Review—Access Control (AC-13)
- 4.2.12. Permitted Actions without Identification or Authentication (AC-14)
- 4.2.13. Remote Access (AC-17)
- 4.2.14. Wireless Access Restrictions (AC-18)
- 4.2.15. Access Control for Portable and Mobile Devices (AC-19)
- 4.2.16. Use of External Information Systems (AC-20)

# Technical Control Example (Cont'd)

---

- 4.3. Audit and Accountability (AU)
- 4.3.1. Audit and Accountability Policy and Procedures (AU-1)
- 4.3.2. Auditable Events (AU-2)
- 4.3.3. Content of Audit Records (AU-3)
- 4.3.4. Audit Storage Capacity (AU-4)
- 4.3.5. Response to Audit Processing Failures (AU-5)
- 4.3.6. Audit Monitoring, Analysis, and Reporting (AU-6)
- 4.3.7. Audit Reduction and Report Generation (AU-7)
- 4.3.8. Time Stamps (AU-8)
- 4.3.9. Protection of Audit Information (AU-9)
- 4.3.10. Audit Record Retention (AU-11)
- 4.4. System and Communications Protection (SC)
- 4.4.1. System and Communications Protection Policy and Procedures (SC-1)
- 4.4.2. Application Partitioning (SC-2)
- 4.4.3. Information Remnance (SC-4)
- 4.4.4. Denial of Service Protection (SC-5)
- 4.4.5. Boundary Protection (SC-7)
- 4.4.6. Transmission Integrity (SC-8)
- 4.4.7. Transmission Confidentiality (SC-9)
- 4.4.8. Network Disconnect (SC-10)
- 4.4.9. Cryptographic Key Establishment and Management (SC-12)
- 4.4.10. Use of Cryptography (SC-13)
- 4.4.11. Public Access Protections (SC-14)
- 4.4.12. Collaborative Computing (SC-15)
- 4.4.13. Public Key Infrastructure Certificates (SC-17)
- 4.4.14. Mobile Code (SC-18)
- 4.4.15. Voice Over Internet Protocol (SC-19)
- 4.4.16. Secure Name /Address Resolution Service (Authoritative Source) (SC-20)
- 4.4.17. Architecture and Provisioning for Name/Address Resolution Service (SC-22)
- 4.4.18. Session Authenticity (SC-23)