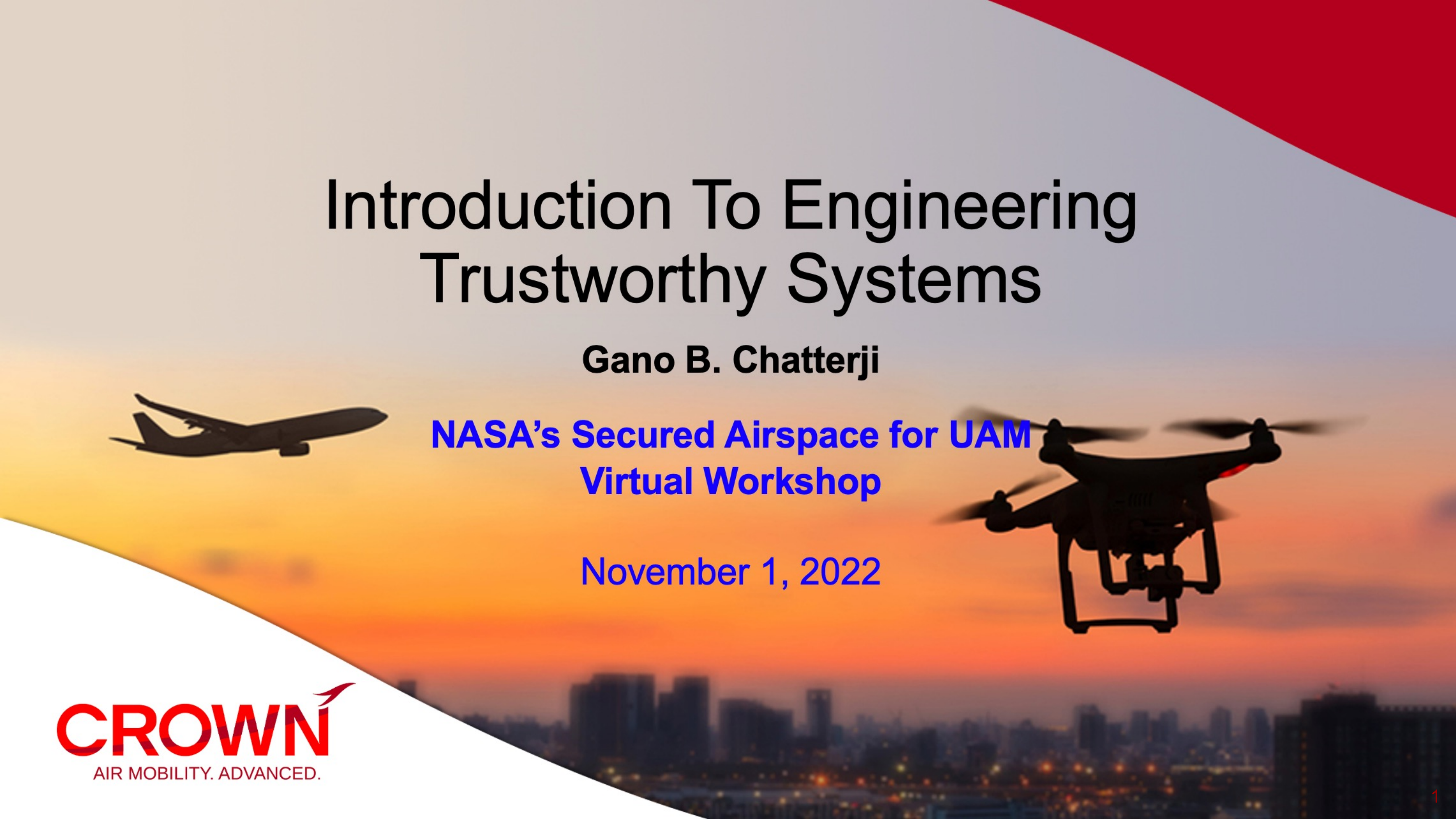


Introduction To Engineering Trustworthy Systems

Gano B. Chatterji

NASA's Secured Airspace for UAM Virtual Workshop

November 1, 2022

CROWN
AIR MOBILITY. ADVANCED.

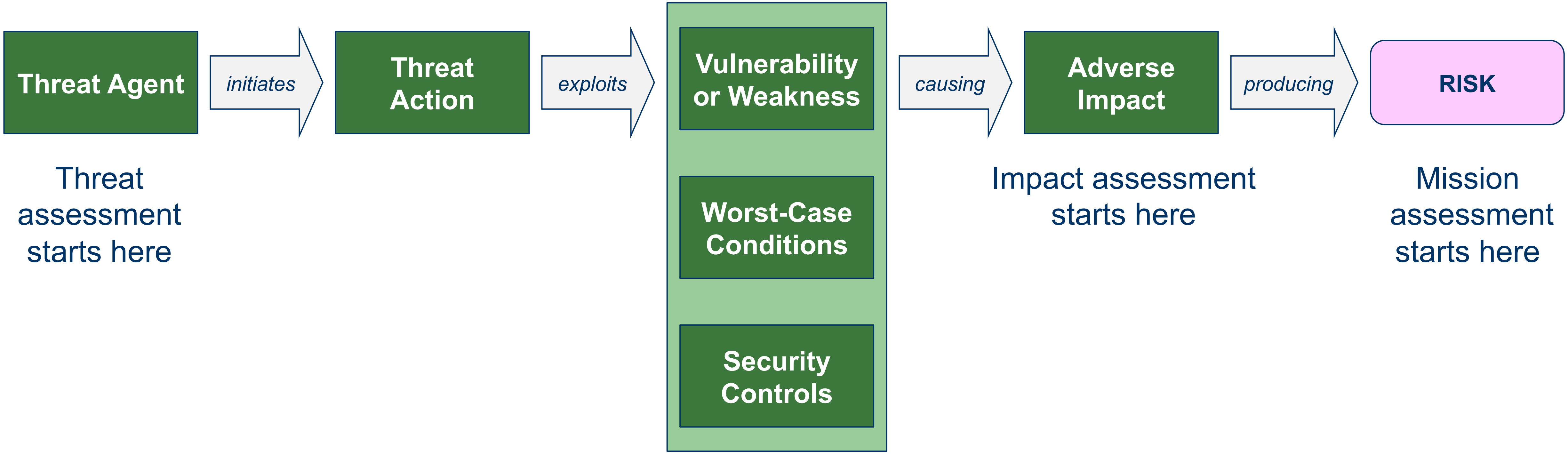
Outline

- Motivation
- Cyber Physical System Risk Model
- Establishing Trust
- Approach for Building Cyber Resilient Systems
- Key Principles of Cyber Security Engineering
- System Theoretic Process Analysis
- Aerospace Systems Standards

Motivation

- The future Air Traffic Management (ATM) system needs to ensure availability, integrity, confidentiality and safety of operations
- Safety of vehicles and operations is paramount for successful integration of Urban Air Mobility (UAM) and Unmanned Aerial Systems (UAS) with the conventional aviation operations in the National Airspace System
- Security is becoming critical because the sensors, networks and computers are far more vulnerable to bad actors than their mechanical or human predecessors
- The goal therefore is to design and develop cyber-resilient systems

Cyber Physical System Risk Model



Threat Agent → *initiates* → Threat Action → *exploits* → Vulnerability or Weakness / Worst-Case Conditions / Security Controls → *causing* → Adverse Impact → *producing* → RISK

Threat assessment starts here

Vulnerability assessment starts here

Impact assessment starts here

Mission assessment starts here

Common Threats

Threat	Description
Data interception	Unauthorized access of sensitive data
Jamming	Interfere with communications, especially wireless
Denial-of-Service	Overloading of system resources for preventing normal operations and functions
Masquerade	Act as an authorized entity to gain access
Replay	Retransmit old valid data repeatedly
Software Threats	Misconfiguration, programming errors, installation of malicious programs
Supply Chain	Unauthorized and malicious hardware, firmware

What is Trust?

- Trust is the foundation of Cyber-Resilient Autonomy
- Trust is confidence that the system:
  - Blocks access to data or information without proper credentials — confidentiality
  - Protects data and itself from getting corrupted — integrity
  - Continues to operate and complete its mission even when attacked — availability
  - Continues to operate safely and protect crew and equipment in degraded conditions — safety

NASA Saw Apollo 13 as a Fiasco. 50 Years Later, Astronaut Jim Lovell Has Made Peace With the 'Successful Failure' by Jeffrey Kluger, April 10, 2020, https://time.com/5816937/apollo-13-50th-anniversary/

"Lovell was the successful commander of a triumphantly successful mission. That historical reckoning comes not despite the fact that his fragile, fickle spacecraft denied him the chance to set foot on the moon, but because of it."

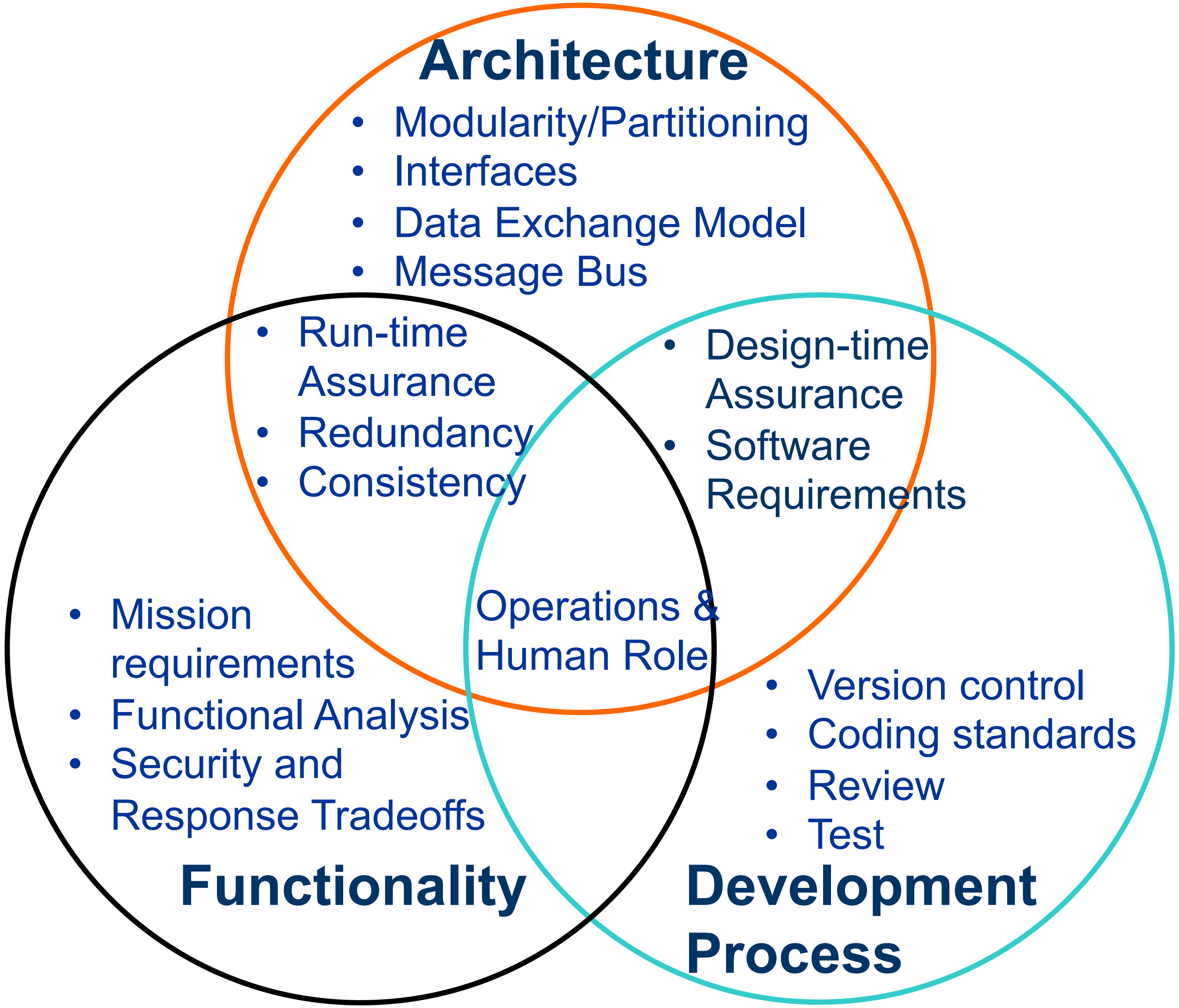
Establishing Trust

- Ensured with comprehensive understanding of the system and implementing policies and procedures
- Examples:
  - Hierarchy of mission objectives defined and documented
  - Process for tracing system requirements to mission objectives
  - Process for tracing system functions to the requirements
  - Graphical User Interface (GUI) software tools for defining architecture from requirements
  - Software tools for code generation based on defined architecture
  - Coding standards including checks for parameter ranges and units
  - Tools for managing software development lifecycle processes (task tracking, reviews, bug tracking and version control)

Establishing Trust (contd.)

- Examples (contd.):
  - Automated workflow processes for error and status reporting and approval
  - Policies and tools for establishing chain of control
  - Data collection policies and procedures including for duration of archival for audit
  - Architecture for supporting scalability, redundancy, obsolescence, testing, runtime performance monitoring and runtime update
  - Understanding of failure modes and their relationship to mission objectives
  - Simulation and modeling tools for characterizing system performance and discovering failure modes
  - Contingency policies for graceful degradation
  - Data at rest and data in transit policies
  - Within the system and external access control policies and procedures

Approach for Building Cyber Resilient Systems



Architecture

- Modularity/Partitioning
- Interfaces
- Data Exchange Model
- Message Bus

- Run-time Assurance
- Redundancy
- Consistency

- Design-time Assurance
- Software Requirements

Operations & Human Role

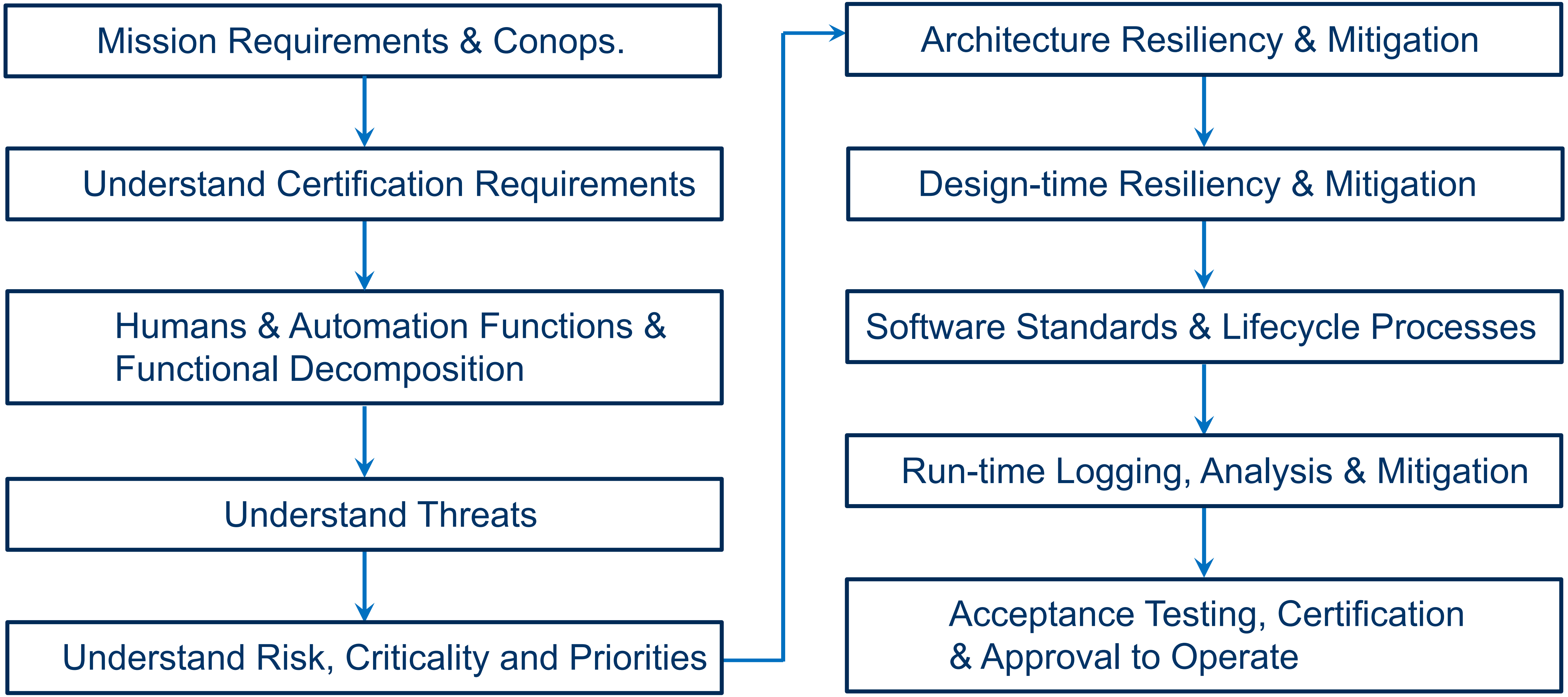
- Mission requirements
- Functional Analysis
- Security and Response Tradeoffs

- Version control
- Coding standards
- Review
- Test

Functionality

Development Process

Cyber Resilient System Development Approach



Mission Requirements & Conops.

Understand Certification Requirements

Humans & Automation Functions & Functional Decomposition

Understand Threats

Understand Risk, Criticality and Priorities

Architecture Resiliency & Mitigation

Design-time Resiliency & Mitigation

Software Standards & Lifecycle Processes

Run-time Logging, Analysis & Mitigation

Acceptance Testing, Certification & Approval to Operate

Key Principles of Cybersecurity Engineering

1. Cybersecurity's goal is to optimize mission effectiveness; cybersecurity is never an end unto itself.
2. Cybersecurity is about understanding, and mitigating cyberattack risk.
3. Assume your adversary knows your mission and cybersecurity system better than you; the opposite assumption is folly.
4. Defense in depth without defense in breadth is useless; breadth without depth is weak.
5. Failing to plan for cybersecurity failure, guarantees catastrophic failure.
6. Cybersecurity strategy and tactics knowledge comes from deeply analyzing cyberattack encounters.

Cybersecurity Engineering Principle 1

Cybersecurity's goal is to optimize mission effectiveness;
cybersecurity is never an end unto itself

- Systems have a primary mission
  - Fly to the moon and return safely, fly the specified trajectory, control the attitude of the spacecraft, send and receive data packets

- System's mission value affected by
  - Its probability of failure
  - Multitude causes, including cyberattack and component failure

- The purpose of cybersecurity design
  - Reduce probability of failure from cyberattack to maximize mission effectiveness

Cybersecurity Engineering Principle 2

Cybersecurity is about understanding, and mitigating cyberattack risk

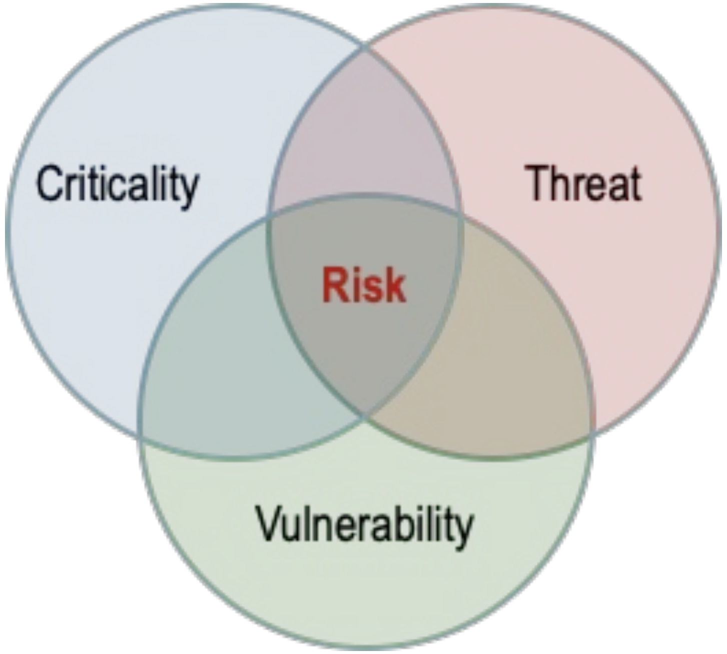
- Engineering disciplines require metrics to characterize, evaluate, predict and compare especially for control and mitigation
- Formulation of risk metrics is fundamental to cybersecurity
  - Understanding nature and sources of risk is key to risk mitigation
  - Risk measurement is foundational for control/mitigation
- Cybersecurity risk quantification
  - Potential damages and impact — consequence — on mission resulting from attack
  - Probability of cyberattacks occurring multiplied by consequence or cost
- Estimating both quantities is challenging, but possible

Risk Assessment

- The Institute for Defense Analysis (IDA) study comparing various mission based cyber risk methodologies found:
  - More than 20 unique methodologies in use
  - Most models use the same three elements combined in different ways to determine risk

- These three common elements are
  - Criticality (Impact)
  - Threat
  - Vulnerability

- Risk occurs at the intersection of criticality, threat and vulnerability



Cybersecurity Engineering Principle 3

Assume your adversary knows your mission and cybersecurity system better than you; the opposite assumption is folly

- Secrecy is fleeting
  - Never depend on it more than is absolutely necessary
  - Applies to both the system and the data
- Don’t make rash and unfounded assumptions
  - Safer to assume adversary knows as much about the system as the designer
- Beyond adversary’s knowledge of the system
  - Assume part of system co-opted sometime during its lifecycle
  - A component might have been altered/replaced during development or maintenance to have some degree of control
- Consider “zero trust” architectures

Cybersecurity Engineering Principle 4

Defense in depth without defense in breadth is useless;
breadth without depth is weak

- Principle of defense in depth (detail)
  - Layering cybersecurity approaches (people, tech, process)
  - Need precision to be useful in design process: layer how, w.r.t. what?
- W.r.t. cyberattack space covering gamut of possible attack classes
  - Mechanisms useful against one attack class useless against other classes
  - Creating depth to point of making a class of attack prohibitive
  - Adversary may simply move to an alternative attack
- Thus, companion principle: defense in breadth (scope)
  - For all avenues of attack
  - For all attack classes

Cybersecurity Engineering Principle 5

Failing to plan for cybersecurity failure guarantees catastrophic failure

- System failures are inevitable
  - Pretending otherwise is almost always catastrophic
  - Applies to mission system and cybersecurity subsystem that protects it
  - Cybersecurity systems, like all systems, are subject to failure
- Engineers must understand how their systems can fail, including
  - Underlying hardware (microprocessors, internal buses)
  - Systems on which they depend (network, memory, ext. storage)
- A student of cybersecurity is a student of failure, dependability and control
  - Security requires reliability; reliability requires security
- Cybersecurity mechanisms not endowed with nonfailure powers
  - Subject to same Engineering-V failures as all system
  - Security code handle complex timing issues and hardware control

> **One should expect that the expected can be prevented, but the unexpected should have been expected.**
>
> **— Norman Augustine**

CROWN

Cybersecurity Engineering Principle 6

Cybersecurity strategy and tactics knowledge comes from deeply analyzing cyberattack encounters

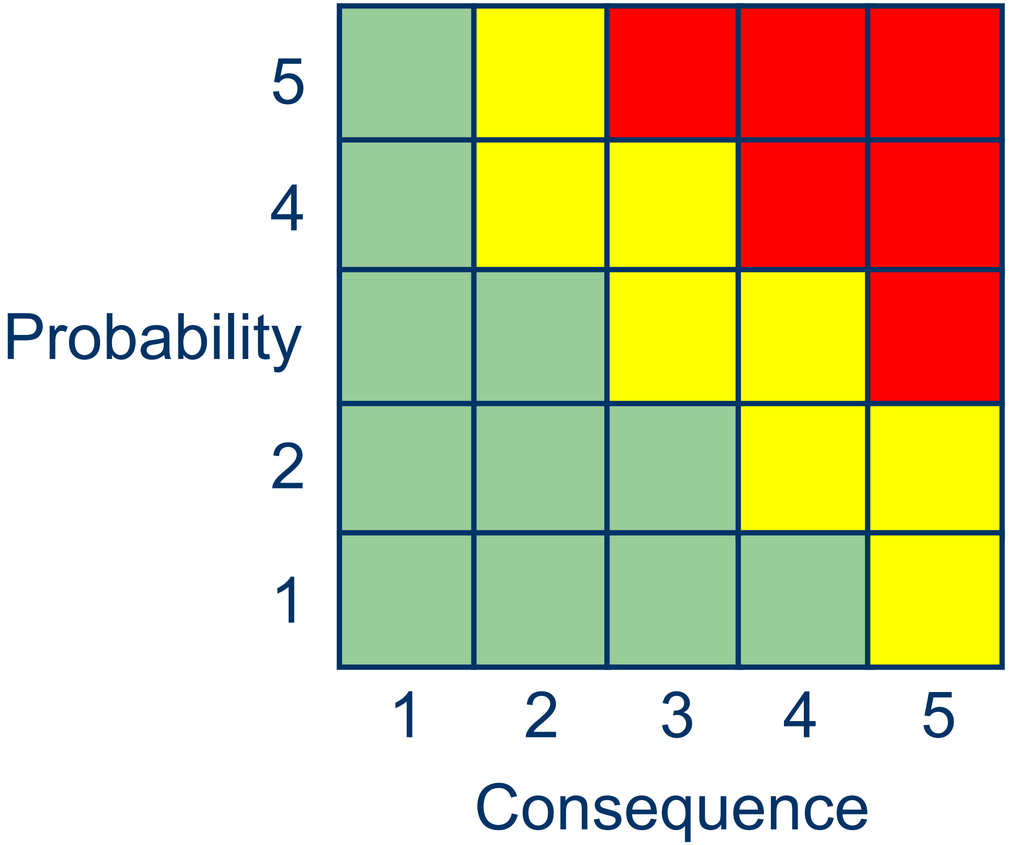
- Good cybersecurity operations is as important as good design
  - Cybersecurity mechanisms are highly configurable (e.g., firewall rules)
- What are optimal settings of various mechanisms?
  - Depends on variations in mission, system environment, attack status
  - Settings dependent on trade-off space for addressing entire spectrum of attacks & failures
  - Static optimal setting for all cyberattack scenarios is difficult, if not impossible
- Knowledge to set parameters according to situation?
  - Analyzing cyberattack encounters: real and simulated, and yours and other’s
  - Theory: game theory, control theory
  - Strategic knowledge to guide default postures & future designs
  - Tactical knowledge (learning) to improve quality and speed of response

System Theoretic Process Analysis (STPA)

- Consists of four steps:
  1. Define purpose of analysis — identify losses, hazards and system safety constraints
  2. Model the control structure — detail the responsibilities, control algorithms, control actions, software/human errors, and process/mental models of each element, and their interactions
  3. Identify unsafe control actions — actions that in a certain situation will lead to a hazard
  4. Identify loss scenarios — unsafe controller behavior, information, control path, process behavior
- Modeling of complex systems, unsafe component interactions, and interactions of human and software controllers
- Analysis of conceptual architectures before detailed design, leading to safety-security driven design
- Iteration throughout Systems Engineering process adding new details and providing traceability through V&V

Scoring via Risk Cubes

- Ranking likelihood and consequence 1-5 levels
- Provides a simple representation for decision makers
- Issues reported with this approach:
  - Cognitive bias and overconfidence
  - Inconsistent scoring even with strict categorization
  - Users feel better about risk, even if they don’t understand it better
  - Multiple areas on risk cubes where unambiguous scoring of randomly selected pairs of hazards is difficult
  - Range compression



5	🟩	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
Probability	🟩	🟩	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5

Consequence

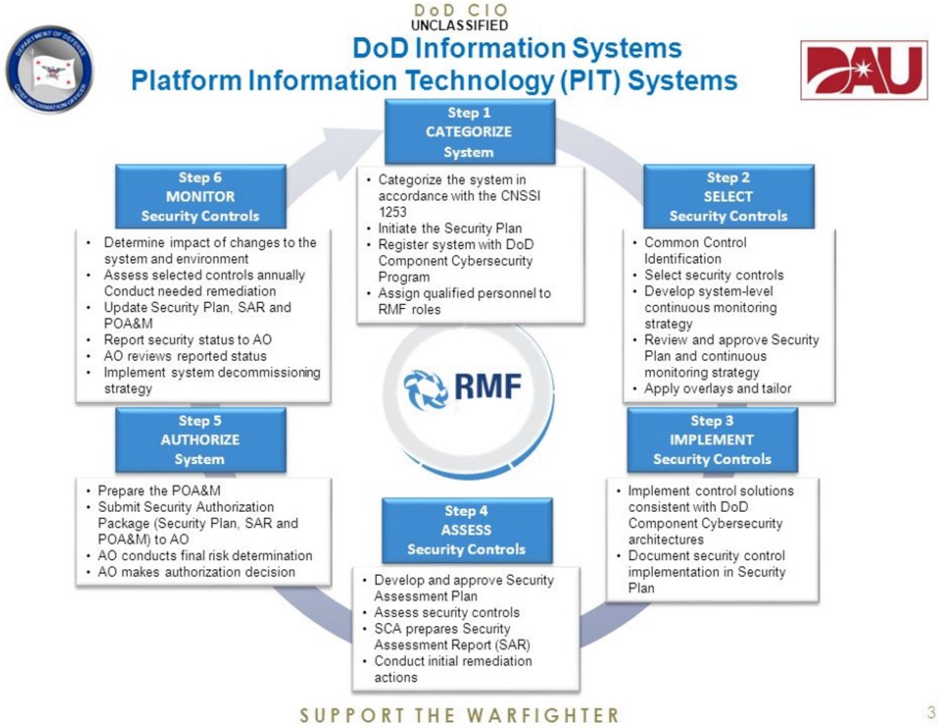
Aerospace System Standards

Organization	Title of Standard	Applicability / Scope	Link to Standard	Description of Standard
CNSS	CNSSI 1200 National Information Assurance Instruction for Space Systems Used to Support National Security Missions	Ground & Spacecraft for National Security System (NSS) only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	It elaborates on how to appropriately integrate Information Assurance (IA) into the planning, development, design, launch, sustained operation, and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems.
CNSS	CNSSI 1253F Attachment 2 Space Platform Overlay	Unmanned spacecraft for NSS only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	This overlay applies to the space platform portion of all space systems that must comply with CNSS Policy No. 12. The controls specified in this overlay are intended to apply to the space platform after it is launched and undergoing pre-operational testing and during operation. This overlay attempts to mold NIST 800-53 for the space segment.
Consultative Committee for Space Data Systems (CCSDS)	352.0-B Cryptographic Algorithms	Civilian Space Communications	https://public.ccsds.org/Pubs/352x0b2.pdf	This standard provides several alternative authentication/integrity algorithms which may be chosen for use by individual missions depending on their specific mission environments. It does not specify how, when, or where these algorithms should be implemented or used. Those specifics are left to the individual mission planners based on the mission security requirements and the results of the mission risk analysis.
Consultative Committee for Space Data Systems	355.0-B Space Data Link Security (SDLS) Protocol	Civilian Space Communications	https://public.ccsds.org/Pubs/355x0b1.pdf	This protocol provides a security header and trailer along with associated procedures that may be used with the CCSDS Telemetry, Telecommand, and Advanced Orbiting Systems Space Data Link Protocols to provide a structured method for applying data authentication and/or data confidentiality at the Data Link Layer.
Consultative Committee for Space Data Systems	356.0-B Network Layer Security	Civilian Space Communications	https://public.ccsds.org/Pubs/356xb1.pdf	This standard provides the basis for Network Layer security for space missions utilizing the Internet Protocol (IP) and complying with IP over CCSDS Space Links
Consultative Committee for Space Data Systems	357.0-B Authentication Credentials	Civilian Space Communications	https://public.ccsds.org/Pubs/357x0b1.pdf	In the CCSDS space environment, credentials are needed to allow communicating entities to authenticate each other to determine potential authorization and access control actions. CCSDS recommends two types of credentials in this standard: X.509 certificates and protected simple authentication.
Aerospace Industries Association	NAS9933 Critical Security Controls for Effective Capability in Cyber Defense	Department of Defense (DoD) Aerospace Contractors Enterprise/Ground Infrastructure	http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf	To align the fragmented and conflicting requirements that the DoD contracting process imposes on industry. Rather than different DoD organizations using different tools to assess a company's security across different contracts, this standard is designed to apply common and universal elements of cybersecurity across each enterprise.

Aerospace System Standards (contd.)

Organization	Title of Standard	Applicability / Scope	Link to Standard	Description of Standard
NASA	Space System Protection Standard	Applicable to all NASA programs and projects (starting in 2020)	https://standards.nasa.gov/sites/default/files/standards/NASA/PUBLISHED/Baseline/nasa-std-1006.pdf	This NASA Technical Standard establishes Agency-level protection requirements to ensure NASA missions are resilient to threats and is applicable to all NASA programs and projects starting in 2020.
NIST	Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	Ground & Spacecraft systems	https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final	This publication addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems.

DoD Risk Management Framework (RMF)



DoD CIO

UNCLASSIFIED

DoD Information Systems

Platform Information Technology (PIT) Systems

Step 1 CATEGORIZE System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2 SELECT Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3 IMPLEMENT Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4 ASSESS Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5 AUTHORIZE System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6 MONITOR Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

SUPPORT THE WARFIGHTER