National Institute of Standards and Technology
U.S. Department of Commerce

Next Generation Mission-Based Security for Systems Engineers

Protecting Space Systems and Technologies

Cybersecurity and Risk Management Frameworks

Systems and Security Engineering

We have reached a cybersecurity fork in the road…

Protecting Space Missions in the Age of Cyber-Physical Systems

- What are the appropriate processes?
- What are the appropriate tools?
- What are the expected outcomes?

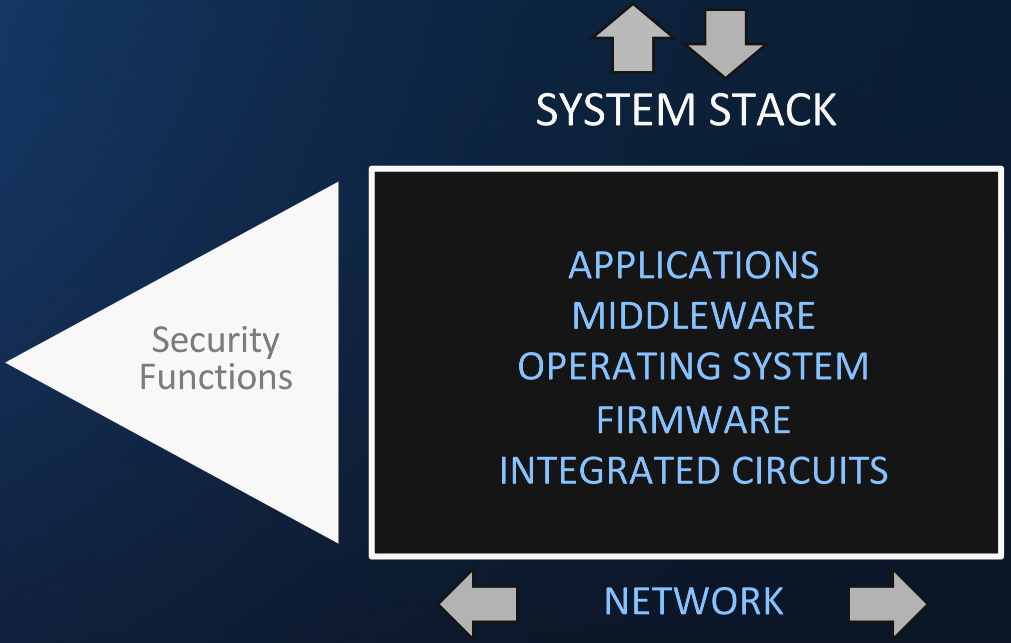
Ubiquitous connectivity produces shared risk

From Earth to Space...

Houston, we have a problem…

Little or no understanding of what’s in the ”black box.”

Transparency
Traceability
Visibility
Assurance



SYSTEM STACK

Security Functions

APPLICATIONS
MIDDLEWARE
OPERATING SYSTEM
FIRMWARE
INTEGRATED CIRCUITS

NETWORK

Threats to Space Systems

- Structural failures of organization-controlled resources
- Human errors of omission or commission
- Natural and man-made disasters, accidents, and failures beyond the control of the organization
- Hostile cyber or physical attacks

Source: NIST SP 800-30

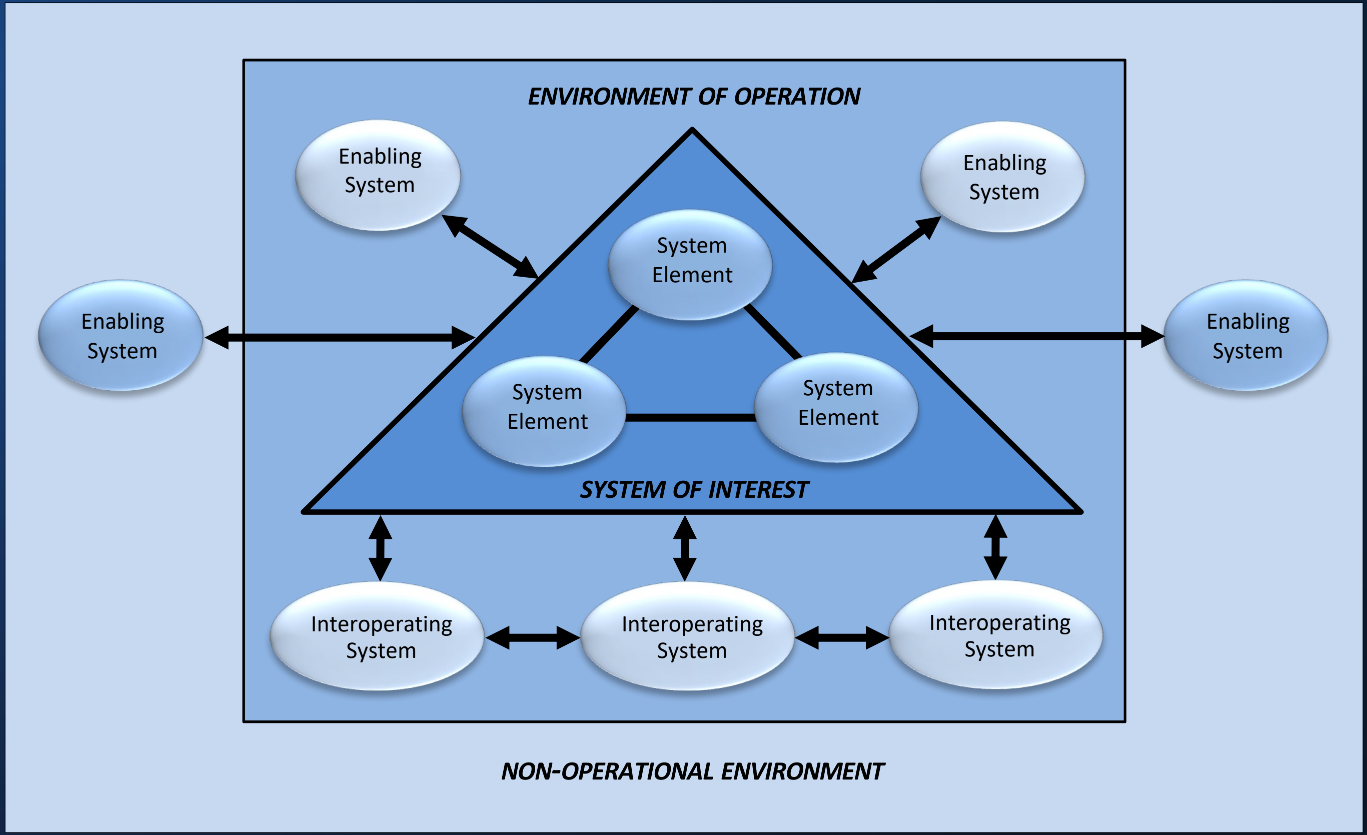
Hostile cyber attacks

by capable and determined adversaries…

- Exfiltrate information
- Preposition malicious code
- Bring down capability
- Create deception

The speed, complexity, and volume of cyber threats appears to be increasing which precludes a purely defensive posture

System of Systems



Critical interdependencies and relationships among internal system elements, systems within enterprise environments, and systems in external environments that affect security solutions.

Current Landscape

- Space technologies and assets are integrated into almost all essential sectors and functions, including defense, agriculture, transportation, energy, healthcare, and telecommunications
- US currently operates in “contested space” where space technology is a high-value target for adversaries
- The civil space community is a critical part of the nation’s cyber defenses, particularly in protecting the space ecosystem that has become vital to U.S. national and economic security

System security is an inherent part of assuring mission success…

Not only for space systems but all systems that are part of the critical infrastructure or vital to US national and economic security.

Traditional cybersecurity risk management—1

- Does not adequately address risks involving cyber-physical assets (e.g., Application Specific Integrated Circuits [ASIC], PLCs, Robotic Actuators, FPGAs)
- Does not adequately support trade-off analyses that include cyber risks (e.g., trade-off analysis with safety and reliability)
- Poorly integrates cyber risks into the well-established framework for overall project risks

Traditional cybersecurity risk management—2

- Lacks alignment with a mission’s natural engineering lifecycle, creating a disconnected process
- Does not adequately address the conversion of threat intelligence into actionable items by mission engineers
- Provides ambiguous ROI (e.g., unknown confidence against a specified spectrum of cyberattacks)
- Provides a questionable level of resilience against attacks because the underlying engineered system is effectively a “black box.”

Need for fundamental strategic rethinking—

- Cultural, technical, training, and policy modifications are necessary to establish engineering-level security into the lifecycle of a mission
- System security engineers are critical in the engineering lifecycle of a mission
- Selection of appropriate risk management processes and tools are necessary to protect critical space systems and technologies

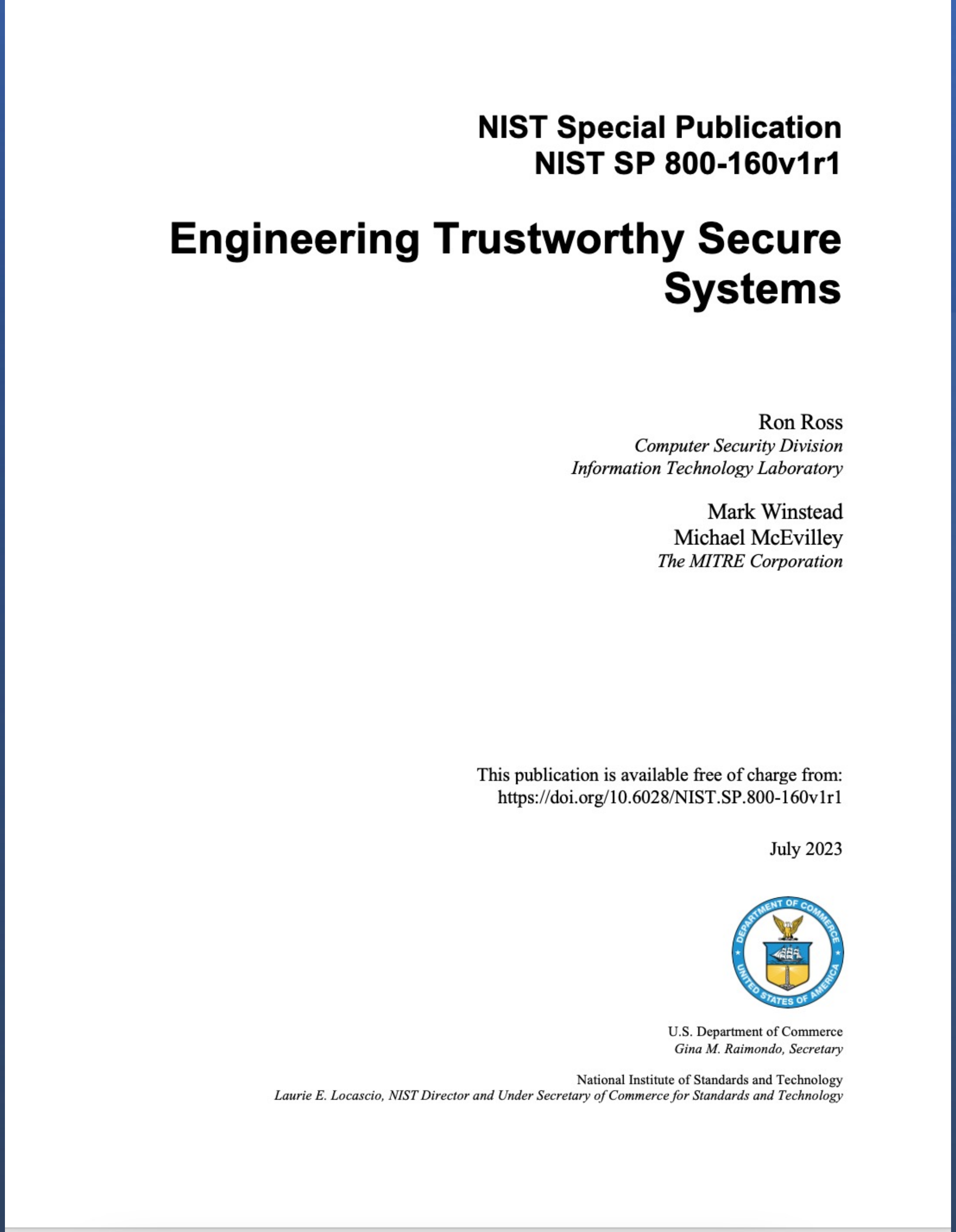
Space Cybersecurity Systems Engineering Pilot Project

NASA, Science Mission Directorate
National Institute of Standards and Technology
Jet Propulsion Laboratory, California Institute of Technology

Pilot Project Goals and Objectives

	Goal	Objectives
Requirements	Address mission requirements, including cybersecurity, across system lifecycle using flight-project engineering processes	Trade off across varying classes of risks to mission (e.g., between safety, reliability and security)
Verification and Validation	Support claims that mission systems meet security, reliability and performance requirements	System authorization to operate (ATO) as a side-effect of sound systems engineering
Principles	Identify a set of repeatable principles, concepts, and activities needed to develop trustworthy, defensible, and survivable mission systems	Resilience to evolving cyberattacks
Planning	Understand cost, complexity, and challenges of applying security design principles and concepts into systems engineering lifecycle	Identify and plan follow-on work needed to realize objectives across NASA and JPL

Multidimensional Protection Strategy



NIST Special Publication
NIST SP 800-160v1r1

Engineering Trustworthy Secure Systems

Ron Ross
Computer Security Division
Information Technology Laboratory

Mark Winstead
Michael McEvilley
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-160v1r1

July 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

- Penetration-resistant architecture
- Damage-limiting operations
- Designs to achieve trustworthy secure systems

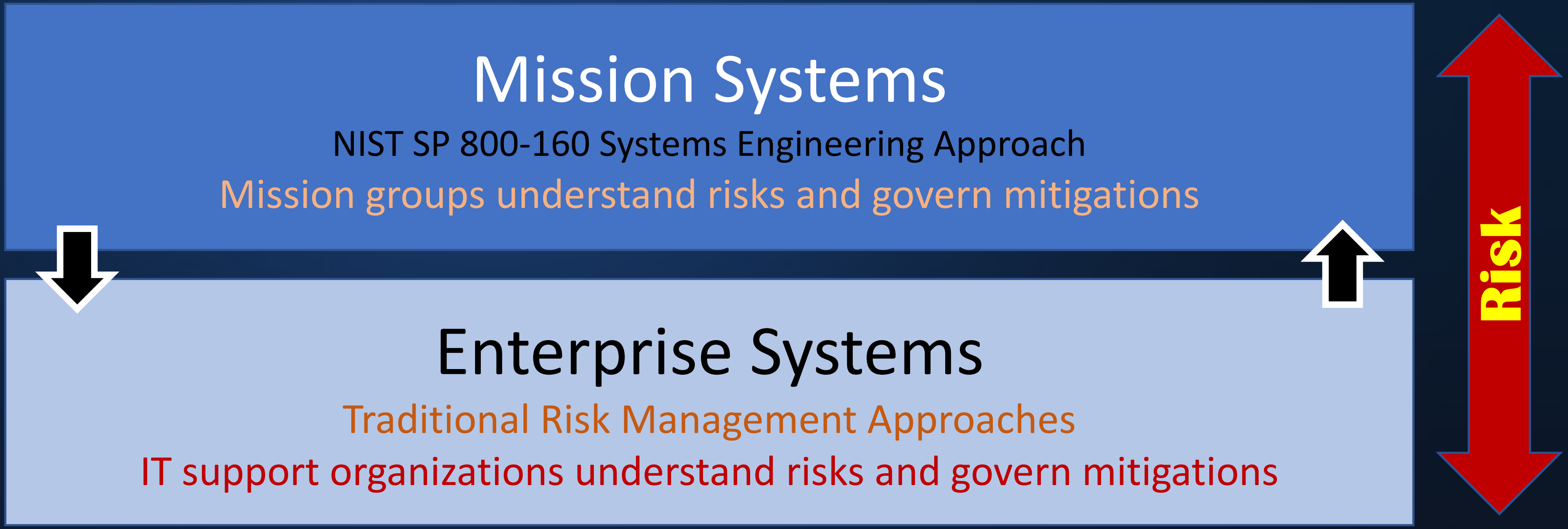
https://doi.org/10.6028/NIST.SP.800-160v1r1

Why Systems Security Engineering Approach?

Engages the rigor of systems engineering processes to provide evidence regarding the trustworthiness of a system to withstand and survive well-resourced, sophisticated attacks

	Traditional Risk Management Approach	Systems Engineering Approach
Focus	A myriad of safeguards and countermeasures	Resilience and trustworthiness of engineered systems
Mission	Mission agnostic	Mission-centered context
Coverage	Implicit, unprioritized	Explicit, prioritized
Timing	After system is built	Throughout the system lifecycle
Risk Mgt.	Separate ATO process	Part of mission risk processes
Leverage	Creates siloed processes	Existing rigorous SE processes
Innovation	Based on historical attacks	Anticipates and mitigates future attacks

Layered Technical and Governance Approach



Mission Systems

NIST SP 800-160 Systems Engineering Approach

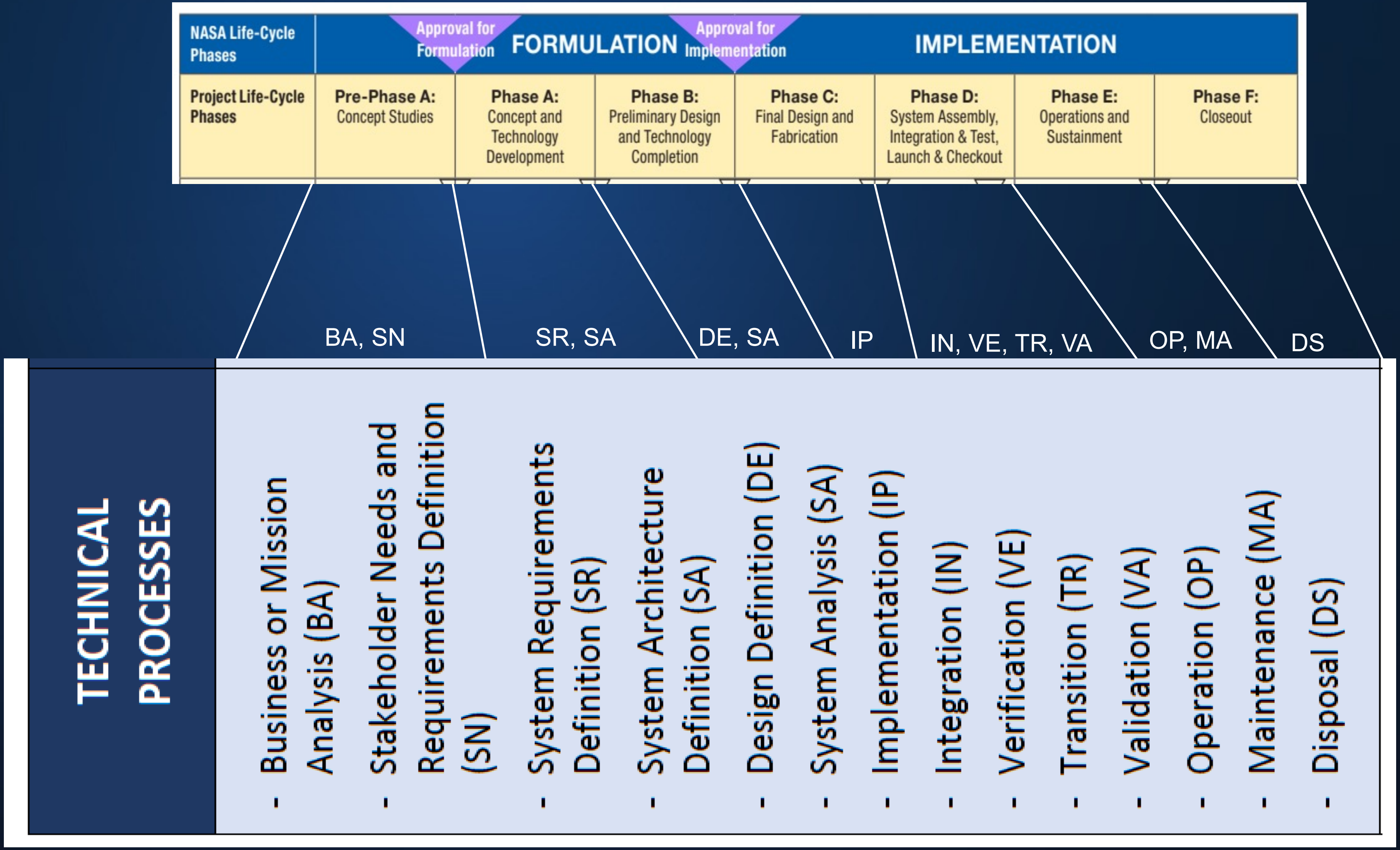
Mission groups understand risks and govern mitigations

Enterprise Systems

Traditional Risk Management Approaches

IT support organizations understand risks and govern mitigations

Mapping SP 800-160 into the Mission Lifecycle



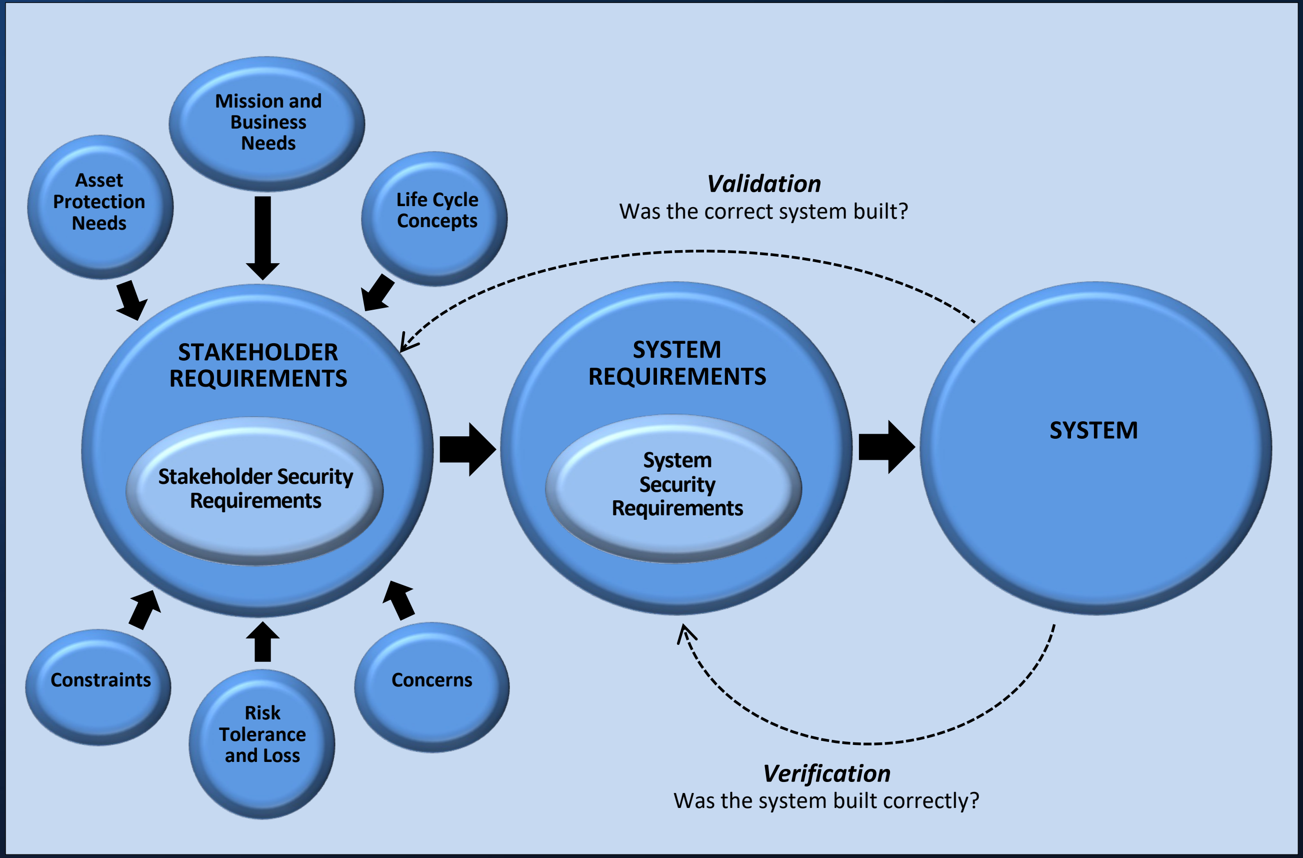
NASA Life-Cycle Phases		Approval for Formulation	FORMULATION	Approval for Implementation	IMPLEMENTATION			
Project Life-Cycle Phases	Pre-Phase A: Concept Studies	Phase A: Concept and Technology Development	Phase B: Preliminary Design and Technology Completion	Phase C: Final Design and Fabrication	Phase D: System Assembly, Integration & Test, Launch & Checkout	Phase E: Operations and Sustainment	Phase F: Closeout

TECHNICAL PROCESSES

- Business or Mission Analysis (BA)
- Stakeholder Needs and Requirements Definition (SN)
- System Requirements Definition (SR)
- System Architecture Definition (SA)
- Design Definition (DE)
- System Analysis (SA)
- Implementation (IP)
- Integration (IN)
- Verification (VE)
- Transition (TR)
- Validation (VA)
- Operation (OP)
- Maintenance (MA)
- Disposal (DS)

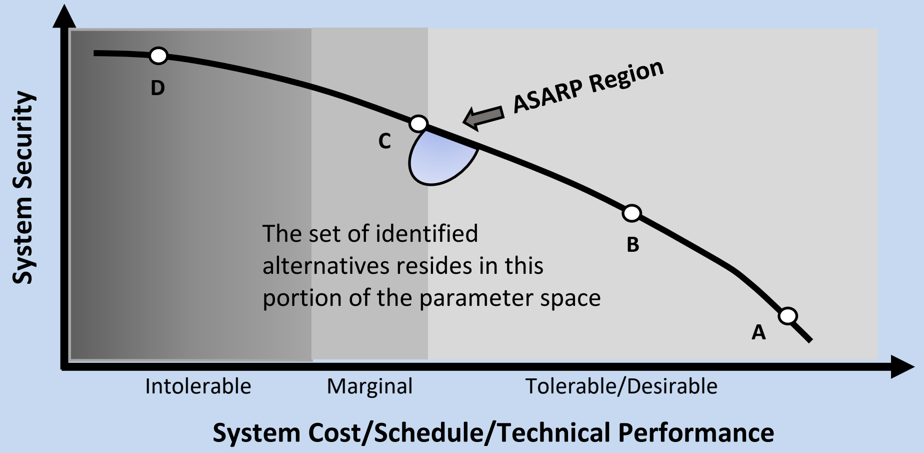
Requirements Engineering

Security requirements, a subset of system requirements, help to protect the mission…



Adequate Security

Means as secure as reasonably practicable…



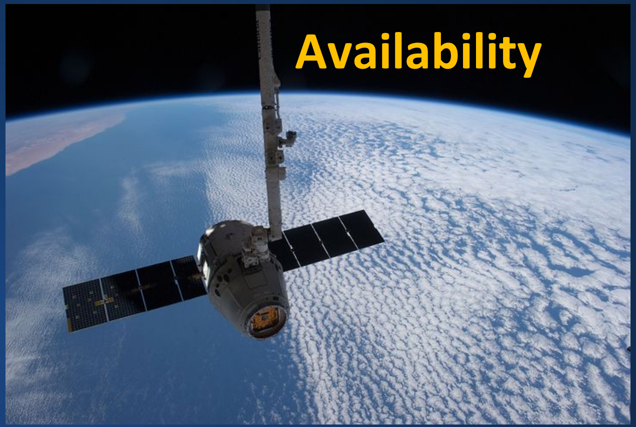
A: Large increases in system security can be achieved by addressing basic security issues. Little cost, schedule, or technical impact.

B: Basic security issues have been addressed but significant security can still be "bought" without failing to meet cost, schedule, or technical performance requirements.

C: Limit of ASARP regime has been reached but significant increases in security can be "bought" without exceeding tolerable limits of cost, schedule, or technical performance requirements.

D: Limit of achievable security has been met. Increased security cannot be "bought" at any cost.

Adapted from NASA.

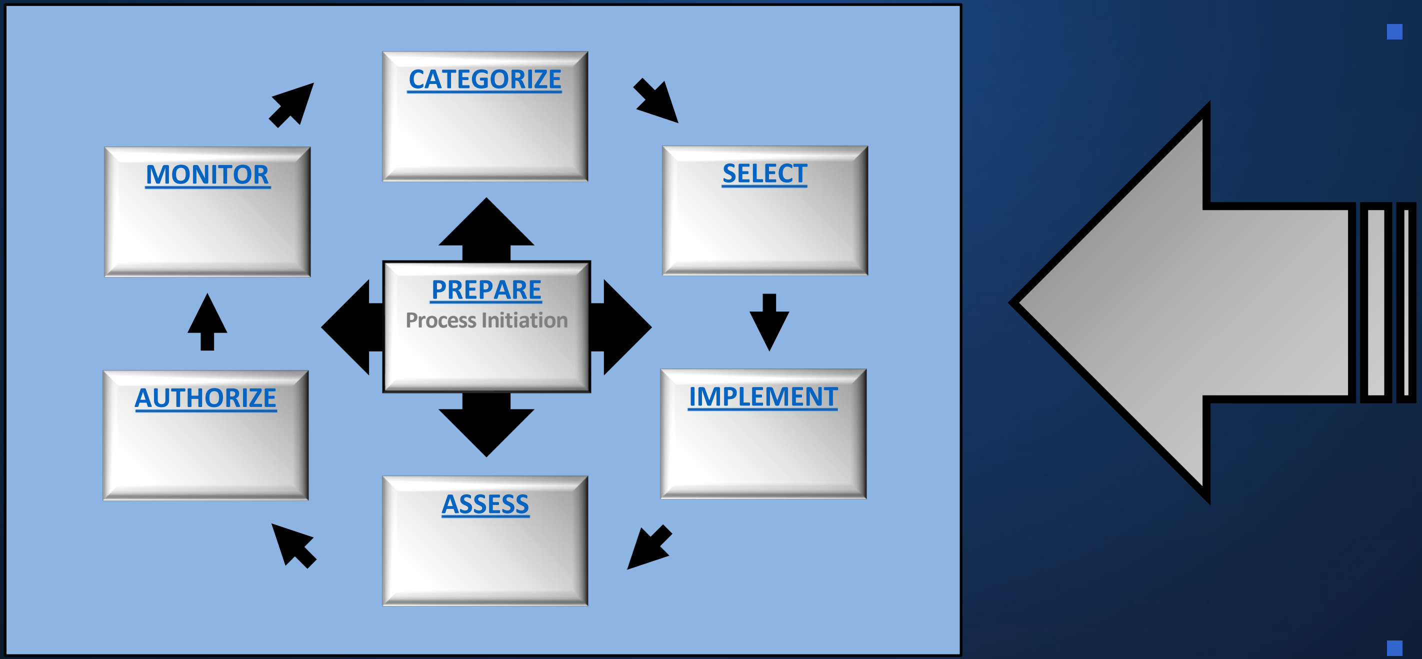


Systems security engineering relationships with other specialty engineering disciplines

A well-executed, engineering-driven life cycle process *can subsume* the steps in the RMF… producing trustworthy secure systems capable of protecting space missions

Systems Engineering Process

- Business or mission analysis
  - Stakeholder needs and requirements definition
    - System requirements definition
      - System architecture definition
        - Design definition
          - System analysis
            - Implementation
            - Integration
          - Verification
        - Transition
      - Validation
    - Operation
  - Maintenance
- Disposal



Risk Management Framework

NIST’s Role in the Space Systems Pilot Project

- Provide technical support to NASA and JPL systems engineering teams regarding the application of the principles and concepts in SP 800-160, Volume 1 to space systems and technologies
- Document the security-related systems engineering activities during the system lifecycle and lessons learned
- Develop a Special Publication (SP) that will serve as a case study for applying the security considerations in SP 800-160 to cyber-physical systems in different sectors (e.g., defense, transportation, energy)

Ron Ross

Email: **ron.ross@nist.gov**

Mobile: **301.651.5083**

Web: **http://csrc.nist.gov**

X: **https://x.com/ronrossecure**

LinkedIn: **https://linkedin.com/in/ronrossecure**