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

Protecting Cyber-Physical Space Systems

The SunRISE Engineering-Based Security Pilot Project

Ron Ross

Adversarial and Non-Adversarial

Threats to Space Systems

A Holistic Systems Engineering Perspective

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

Source: NIST SP 800-30

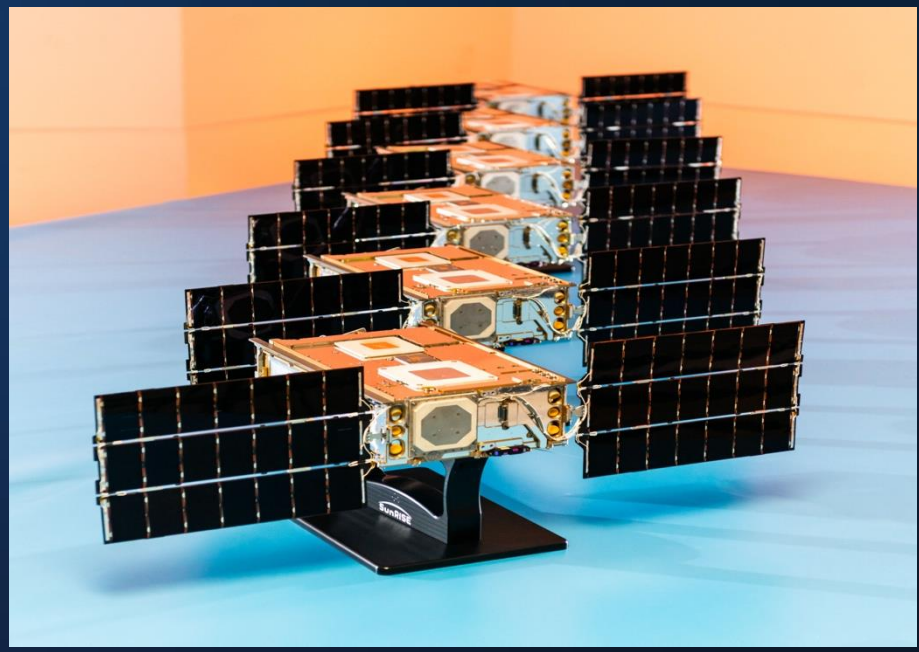
Engineering-Based Security Pilot Project

Interagency Partnership

NASA, Science Mission Directorate

National Institute of Standards and Technology

NASA Jet Propulsion Laboratory
California Institute of Technology



SunRISE
Sun Radio Interferometer Space Experiment

SunRISE Pilot Strategy

- Choose an existing NASA mission with a system Authorization to Operate (ATO) in Phase D / Phase E
- Select an appropriate subsystem
- Conduct baseline resilience and programmatic evaluation of subsystem
- Redesign and reimplement chosen subsystem using the systems engineering process defined in NIST SP 800-160 on a high-fidelity testbed
- Verify that the functionality of subsystem is unaffected after redesign
- Conduct resilience and programmatic evaluation of reimplemented subsystem
- Conduct comparative evaluation of data from both the original subsystem and the redesigned subsystem

System of Interest

- SunRISE is an array of six toaster-size CubeSats that will work together to study solar activity
- The mission will observe low radio frequency emissions so scientists can understand better how the Sun is able to generate intense space weather storms – known as solar particle storms – that can be hazardous to spacecraft and astronauts
- This research will help scientists forecast space weather, improve our understanding of how our Sun works, and may apply to studies of other stars – particularly those with planets

Ground Data System

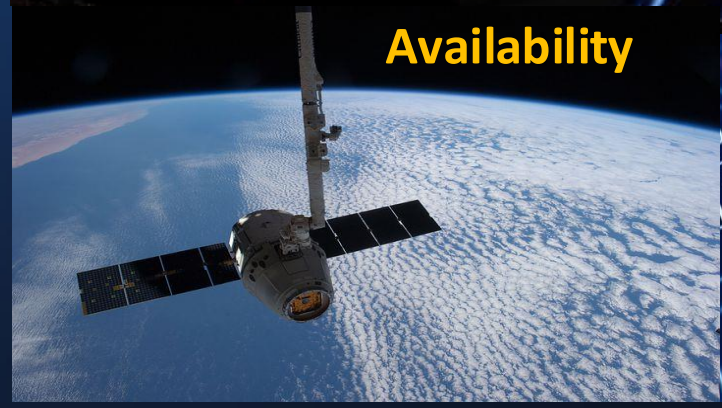
Sub-System of Interest

- A GDS is the *Ground Data System* that supports large-scale embedded systems by allowing operators to interact with the embedded system
- This system is typically used with spacecraft to facilitate control and monitoring of those systems' flight software

SunRISE Integrated Project Team

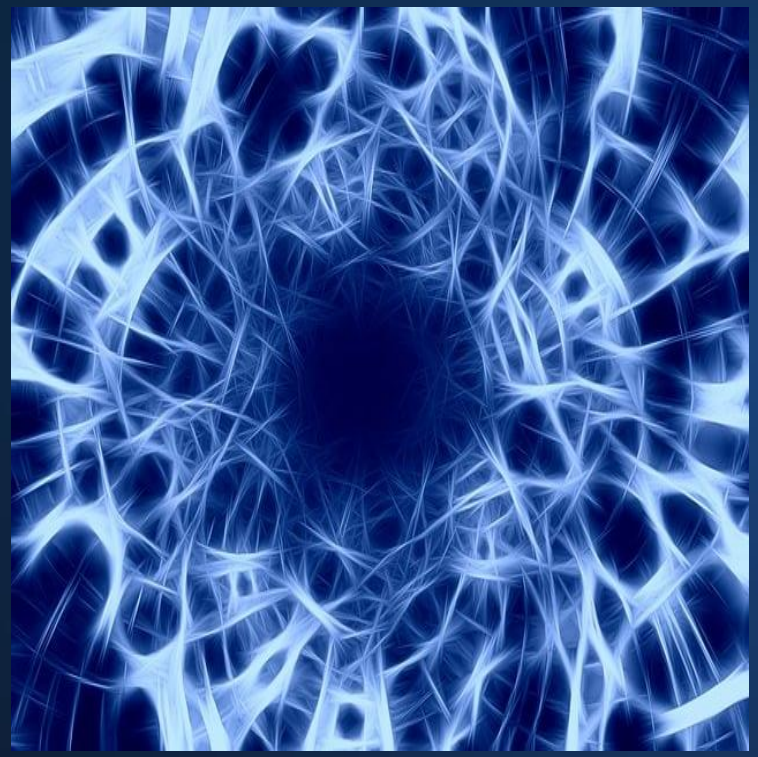
A blending of knowledge, skills, and abilities from the systems engineering and cybersecurity communities as well as other specialty disciplines…

- Project Managers
- Principle Investigators
- Systems (Mission) Engineers
- Systems Security Engineers
- Specialty Disciplines



Foundational Concepts

- Security is an emergent property of an engineered system similar to safety, reliability, and resilience
- Mission protection needs guide and inform security requirements (for functionality and assurance)
- Protection needs focus on:
  - Reducing the uncertainty associated with the system's capability (i.e., system behavior)
  - Controlling (reducing, limiting) asset loss due to adverse consequences
- Adequate security involves trade space decisions that translate to *as secure as reasonably practicable*



Traditional Cybersecurity Risk Management

- Lacks alignment with the systems (mission) engineering lifecycle, creating a disconnected process
- Does not adequately address risks involving cyber-physical assets (e.g., ASICs, FPGAs, PLCs, robotic actuators, sensors)
- Inadequate integration of cyber risks into the established framework for overall project risks (e.g., safety, reliability)
- Inadequate conversion of current threat intelligence into actionable items by mission and systems engineers
- Provides ambiguous ROI (e.g., unknown confidence or assurance against a range of specified threats)
- Provides inadequate visibility into the underlying system design (i.e., black box problem) resulting in insufficient assurance in the system capability

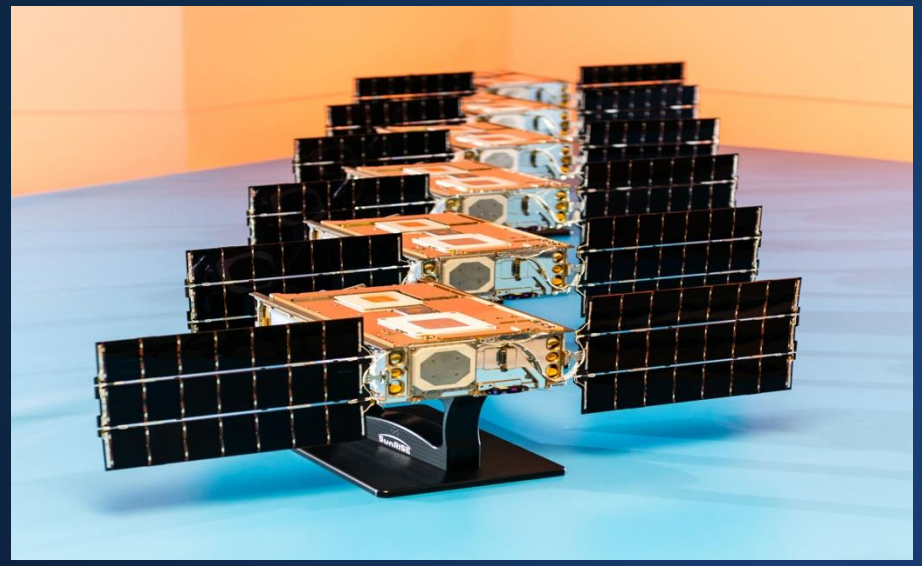
Cybersecurity v. Engineering-Based Security

	Cybersecurity Approach	Systems Engineering Approach
Mission	Mission agnostic	Mission centric
Focus	Catalog of safeguards and countermeasures	Security design principles, system resilience
Coverage	One system at a time, implicit, unprioritized	System-of-systems, explicit, prioritized
Timing	Lags in the system life cycle	Part of the entire system life cycle
Risk Mgt	Separate system authorization (ATO) process, compliance, vulnerability management	Part of mission risk processes, controlling asset loss, managing uncertainty, assurance
Innovation	Based on historical threats	Anticipates and mitigates future threats

Hypotheses

SunRISE Pilot Project

- A systems engineering approach using the design principles in NIST SP 800-160 produces a system that is more resilient and secure than a system that is only NIST SP 800-53 compliant
- A principled systems engineering process provides the necessary assurance evidence to satisfy the requirements for a system authorization to operate (ATO)
- A systems engineering approach to protecting critical space assets significantly reduces the level of effort, time, and resources required to achieve an ATO



SunRISE Pilot Objectives

- Demonstrate a working use case of applying the security design principles in NIST SP 800-160 to an actual flight project
- Identify potential protection gaps in traditional cybersecurity approaches versus engineering-based security approaches
- Identify potential security-related system design and implementation changes
- Document the cost and effectiveness of engineering-based security

SunRISE Pilot Outcomes

- Understand the application of the security design principles in NIST SP 800-160 to space systems
- Acquire critical information that can be used to make security-related modifications to the current SunRISE system (GDS)
- Obtain sufficient information to assess the cost, schedule, and performance implications for proposed protection measures
- Compare engineering-based security approach to current system authorization (ATO) process

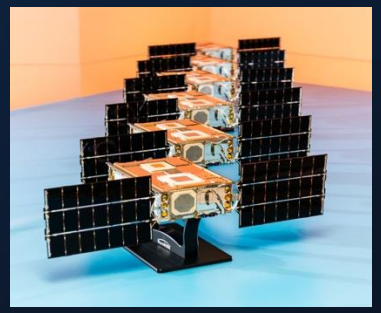
SunRise Pilot Project Approach

NASA Life Cycle Phases	Formulation		Implementation				
	Initiation		*Acquisition & Development*		*Implementation*	*Operation*	*Sunset*
Project Life Cycles	**Pre-Phase A Concept Studies**	**Phase A Concept & Technology Completion**	**Phase B Preliminary Design & Technology Completion**	**Phase C Final Design & Build**	**Phase D System Assembly Integration & Test**	**Phase E Deployment Operations Sustainment**	**Phase F Decommissioning**

ACTUAL — SunRISE System Life Cycle: Completed Phase D

SIMULATED — SunRISE Twin System Life Cycle

Applying NIST SP 800-160 Security Design Principles



SunRISE
Sun Radio Interferometer Space Experiment

SunRISE Pilot Data Sources

- **Security Design Principles (Top Level)**
  NIST SP 800-160, Volume 1 (Appendix E)
- **Resiliency Techniques, Approaches and Controls (Derivative)**
  NIST SP 800-160, Volume 2, NIST SP 800-53

NOTE: Resiliency techniques, approaches, and controls are derivative from and traceable to, top level security design principles.

Security Design Principles

The Foundation of Trustworthy Secure Systems

- Anomaly Detection
- Clear Abstractions
- Commensurate Protection
- Commensurate Response
- Commensurate Rigor
- Commensurate Trustworthiness
- Compositional Trustworthiness
- Continuous Protection
- Defense In Depth
- Distributed Privilege
- Diversity (Dynamicity)
- Domain Separation
- Hierarchical Protection
- Least Functionality
- Least Persistence
- Least Privilege
- Least Sharing
- Loss Margins
- Mediated Access
- Minimal Trusted Elements
- Minimize Detectability
- Protective Defaults
- Protective Failure
- Protective Recovery
- Reduced Complexity
- Redundancy
- Self-Reliant Trustworthiness
- Struct. Decomposition/Composition
- Substantiated Trustworthiness
- Trustworthy System Control

Security Design Principles

Selected for the SunRISE Pilot Project

- **Anomaly Detection**
- Clear Abstractions
- Commensurate Protection
- Commensurate Response
- Commensurate Rigor
- Commensurate Trustworthiness
- Compositional Trustworthiness
- Continuous Protection
- **Defense In Depth**
- Distributed Privilege
- Diversity (Dynamicity)
- Domain Separation
- Hierarchical Protection
- **Least Functionality**
- **Least Persistence**
- **Least Privilege**
- **Least Sharing**
- Loss Margins
- **Mediated Access**
- Minimal Trusted Elements
- Minimize Detectability
- Protective Defaults
- Protective Failure
- Protective Recovery
- **Reduced Complexity**
- Redundancy
- Self-Reliant Trustworthiness
- Struct. Decomposition/Composition
- Substantiated Trustworthiness
- Trustworthy System Control

Resiliency Techniques and Approaches

Selected for the SunRISE Pilot Project

- **Analytic Monitoring**
  - Monitoring and Damage Assessment
- **Non-Persistence**
  - Non-Persistent Information
  - Non-Persistent Connectivity
- **Coordinated Protection**
  - Calibrated Defense in Depth
- **Contextual Awareness**
  - Dynamic Resource Awareness
  - Dynamic Threat Awareness
  - Mission Dependency and Status Visualization
- **Adaptive Response**
  - Dynamic Resource Allocation
  - Dynamic Reconfiguration

Security Design Principle Traceability

- **Anomaly Detection (Security Design Principle)**
  NIST SP 800-160, Volume 1

- **Analytic Monitoring (Resiliency Technique)**
  NIST SP 800-160, Volume 2

- **Monitoring and Damage Assessment (Resiliency Approach)**
  NIST SP 800-160, Volume 2

System Performance Metrics

Design/Implementation Metrics

- Schedule
  - Number of days of additional schedule required to implement the security design principles
- Personnel Resources
  - Number of FTEs required to implement the security design principles
- Incidentals
  - Funds required for additional procurements needed to support the application of security design principles
- Cost of applying security design principles during the systems engineering lifecycle

System Performance Metrics

Operational Metrics

- Time required for recovery to full/acceptable operations
- Number of hours/days lost in the operational schedule due to security incidents
- Amount of science data lost due to incident
- Number of FTEs needed to restore the system to full or acceptable operations
- Funds required for additional procurements needed to support recovery operations
- Funds required to support the recovery of the system to full operations

Security Performance Metrics

- Mean Time to Inventory
  - The time it takes to identify appropriate assets, data flows, and mission workflows impacted by a vulnerability, once it is discovered
- Mean Time to Detect
  - The time the intrusion or incident manifests in the system logs and mission is alerted
- Mean Time to Acknowledgement
  - The time at which response or recovery operations start
- Mean Time to Recovery
  - The time at which the system is fully restored to its previous functional state before the incident

Evidence-Based Assurance

Essential for the development of trustworthy secure systems…

SYSTEM STACK

Transparency
Traceability
Visibility

Security Functions

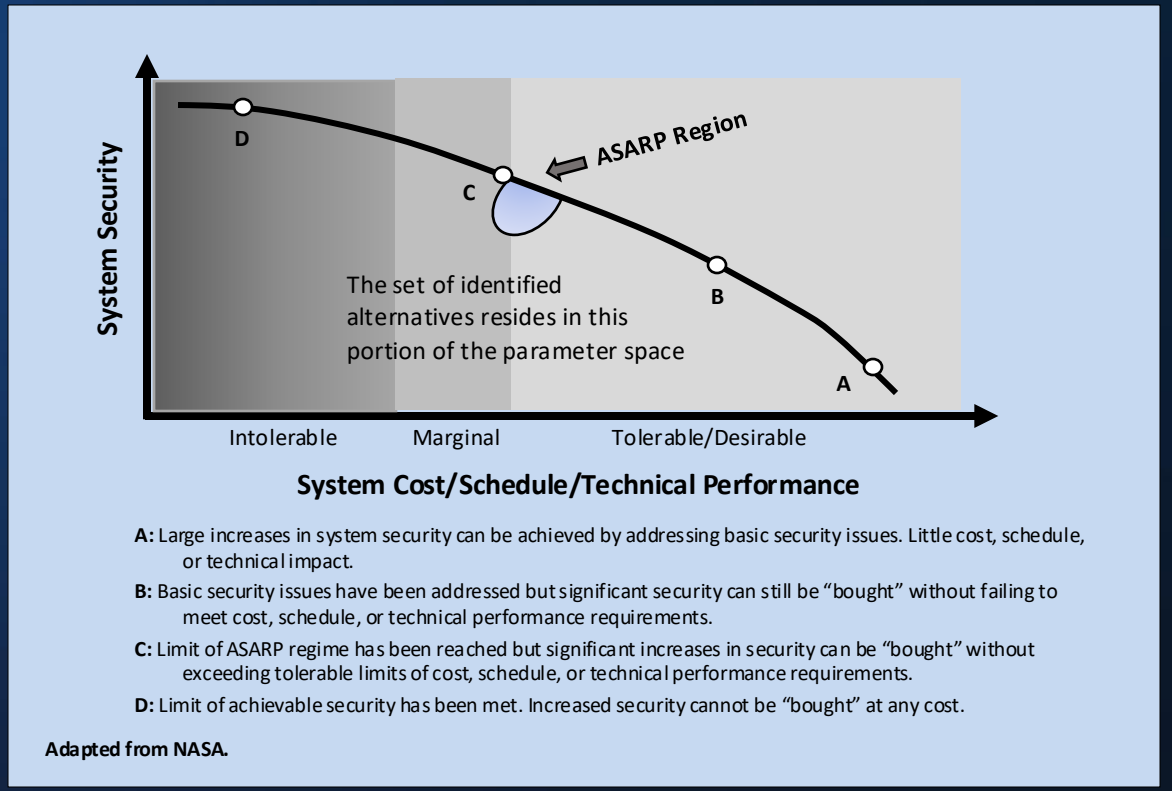
APPLICATIONS
MIDDLEWARE
OPERATING SYSTEMS
FIRMWARE
INTEGRATED CIRCUITS

NETWORK

Produced routinely during the systems engineering verification, validation, and system analyses processes…

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.

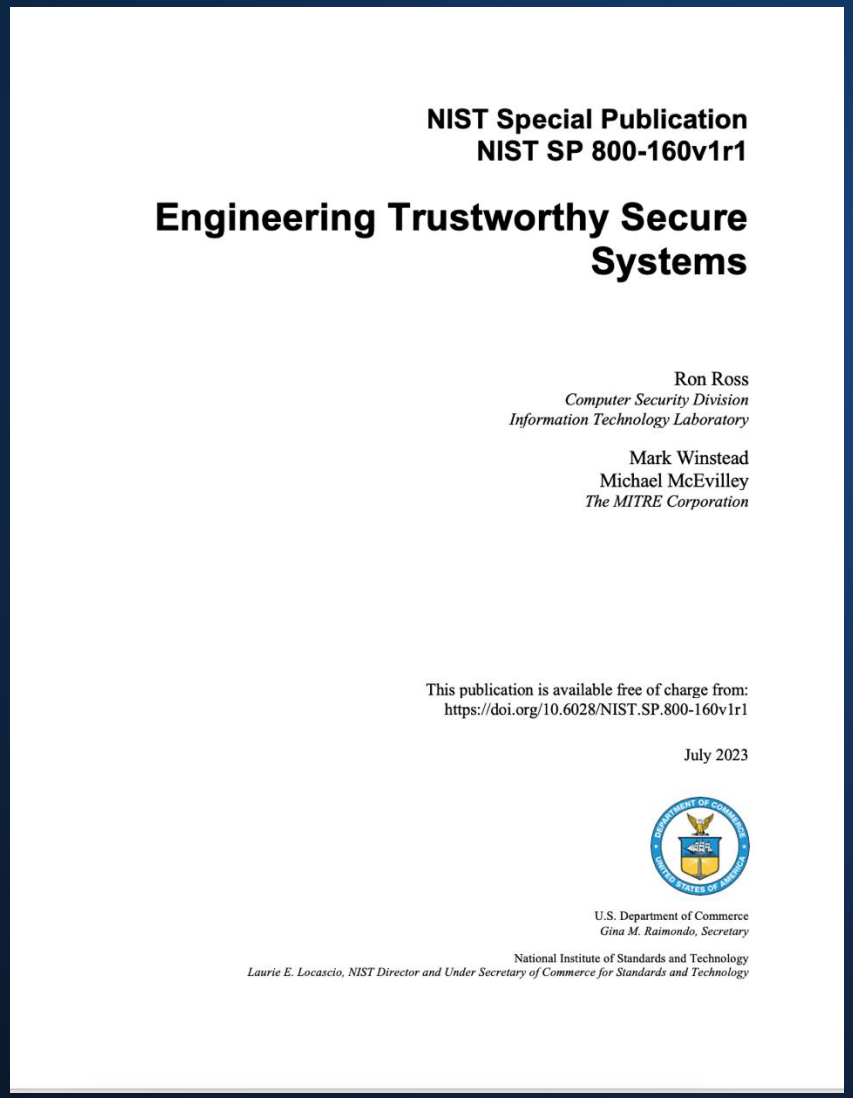
C: Limit of ASARP regime has been reached but significant increases in security can be "bought" without exceeding tolerable limits of cost, schedule, or technical performance requirements.

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

Adapted from NASA.

Future Pilot Options

- Expand the number of security design principles in SunRISE pilot
- Apply the current set of security design principles to new space platforms of increased size and complexity
- A combination of the above
- Extend to other organizations



Policy Mandate for Engineering Trustworthy Secure Systems

Implement the systems security engineering principles, concepts, techniques, and System Development/Engineering Lifecycle (SDLC/SELC) in NIST SP 800-160, Vol. 1, *Engineering Trustworthy Secure Systems* for all High Value Assets (HVA).

-- OMB Policy M-19-03

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

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

Systems Security Engineering Project

https://csrc.nist.gov/projects/systems-security-engineering-project

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE