Protecting Organizational 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."
Threats to Cyber-Physical 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
Critical interdependencies and relationships among internal system elements, systems within enterprise environments, and systems in external environments that affect security solutions.
Traditional Cybersecurity Risk Management—1

• Does not adequately address risks involving cyber-physical assets (Application Specific Integrated Circuits [ASIC], Programmable Logic Controllers [PLCs], Robotic Actuators, Field Programmable Gate Arrays [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/systems engineers

• Provides ambiguous ROI (e.g., unknown confidence against a specified spectrum of cyber-attacks)

• 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 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

SunRISE
Sun Radio Interferometer Space Experiment
Array of six toaster-size CubeSats that will work together to study solar activity.
### Pilot Project Goals and Objectives

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

- 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*

<table>
<thead>
<tr>
<th></th>
<th>Traditional Risk Management Approach</th>
<th>Systems Engineering Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td>A myriad of safeguards and countermeasures</td>
<td>Resilience and trustworthiness of engineered systems</td>
</tr>
<tr>
<td><strong>Mission</strong></td>
<td>Mission agnostic</td>
<td>Mission-centered context</td>
</tr>
<tr>
<td><strong>Coverage</strong></td>
<td>Implicit, unprioritized</td>
<td>Explicit, prioritized</td>
</tr>
<tr>
<td><strong>Timing</strong></td>
<td>After system is built</td>
<td>Throughout the system lifecycle</td>
</tr>
<tr>
<td><strong>Risk Mgt.</strong></td>
<td>Separate ATO process</td>
<td>Part of mission risk processes</td>
</tr>
<tr>
<td><strong>Leverage</strong></td>
<td>Creates siloed processes</td>
<td>Existing rigorous SE processes</td>
</tr>
<tr>
<td><strong>Innovation</strong></td>
<td>Based on historical attacks</td>
<td>Anticipates and mitigates future attacks</td>
</tr>
</tbody>
</table>
Security requirements, a subset of system requirements, help to protect the mission...
Means as secure as reasonably practicable...

Adequate Security

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

Risk Management Framework

- **CATEGORIZE**
- **AUTHORIZE**
- **ASSESS**
- **SELECT**
- **IMPLEMENT**
- **MONITOR**

**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
Systems security engineering relationships with other specialty engineering disciplines
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