SPARTA Countermeasure Utilization & Prioritization

Brandon Bailey

Cybersecurity and Advanced Platforms Subdivision (CAPS)

Approved for Public Release – Derived from OTR 2022-01250, OTR-2024-00933, OTR 2025-00882, & OTR-2026-00072

Presentation Scope Clarification

Getting on the Same Page

- This is not an overview of the full SPARTA framework, taxonomy, or toolset.
- **Assumption:** Audience is already familiar with SPARTA's structure, purpose, and value.
- All space programs can increase cybersecurity protections, within cost, and schedule constraints, if they can prioritize countermeasures effectively.
- The focus of this presentation is narrow and targeted on the following key topics to help programs prioritize the implementation of appropriate countermeasures:
  - SPARTA Evolution
  - What SPARTA means by Countermeasures
  - From Threat Intelligence to Countermeasures
  - Prioritizing Countermeasures through security controls tailoring
  - Transforming security controls into Countermeasures
  - Reference Implementation

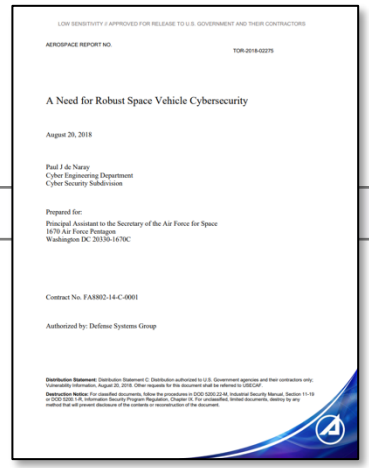
Moving from overwhelming list of controls to mission-relevant, risk-informed countermeasures

Strategic Evolution for Space Enterprise

Orchestrated with FFRDC Customers and Aerospace Support

Call to action

2018

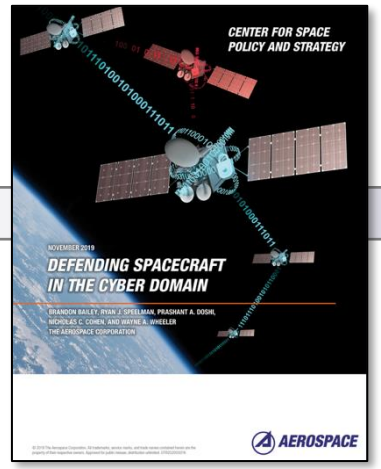


SAF/AQ Sponsored

TOR-2018-02275

Definition of threats

2019

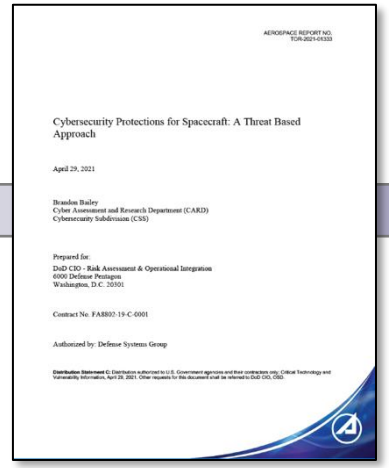


Center for Space Policy & Strategy

OTR-2020-00016

Defense-in-Depth, Linkage of threats to mitigations

2021

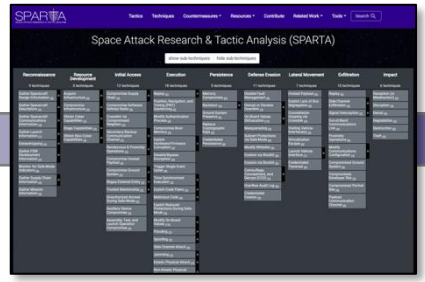


DoD CIO Sponsored

TOR-2021-01333 Rev A

Structured TTPs, Dissemination of Knowledge

2022



Aerospace Funded

TOR-2023-02161 Rev A

Space Segment Cybersecurity Profile for National Security Systems

2023

Space Platform Overlay for National Security Systems

2025

Knowledge base is now being recognized and leveraged

Understanding SPARTA Countermeasures

- **What Are They?**
  - SPARTA countermeasures are technical, operational, and procedural safeguards aligned to adversary TTPs that help engineers prevent, detect, or mitigate cyberattacks on spacecraft systems.
    - Each countermeasure is given a unique identifier (e.g., CM0032) and is described in terms of its purpose, implementation context, and the SPARTA techniques it helps address
    - Continuously updated to reflect new research and threats
- **Why They Matter**
  - **Mitigation Guidance:** They provide engineering and security teams with actions they can take to reduce the likelihood or impact of a technique being used successfully against their system.
  - **Secure-by-Design Alignment:** Many are aligned with secure design principles (e.g., least privilege, defense in depth).
  - **Mapping to Weaknesses:** Countermeasures are often linked to common software/hardware weaknesses (CWEs), helping developers understand how to prevent exploit paths at the design or implementation level.
- Grounded in NIST SP 800-53 Rev. 5 controls and Aerospace's Defense-in-Depth (DiD) model for space systems
  - Many to many relationship where one control maps to multiple countermeasure and vice versa
- Examples
  - CM0002: COMSEC, CM0034: Monitor Critical Telemetry Points, CM0032: On-board Intrusion Detection & Prevention
- Tailored & Evolving
  - Tailored per mission, threat model, and assurance level
  - Mapped to techniques and weaknesses (CWEs)
  - Supports both design-time security and long-term resilience

SPARTA countermeasures turn threat knowledge into engineering action bridging the gap between "what attackers do" and "how we detect/stop them."

SPARTA Countermeasures – Helping Translate (Rosetta Stone)

NASA's Space Security: Best Practices Guide (BPG)

The Space Security: Best Practices Guide (BPG) from NASA provides guidance on mission security implementation in the form of principles coupled with applicable controls that cover both the space vehicle and the ground segment. According to the BPG, "the principles are meant to be easily achievable regardless of mission, program, or project size, scope, or whether international, corporate, or university. The principles selected focus on a risk-based approach to mitigating vulnerabilities, that are impediments to mission success. These principles were identified as an initial starting point of critical implementations for NASA missions to consider. The underlying security principles and associated controls were identified through an iterative process to address today's cyber actors Tactics, Techniques, and Procedures (TTPs) used in attempts to compromise mission capabilities."

The BPG has security principles for the "Space Mission" in section 3.2 and "Ground" in section 3.3. Given SPARTA's focus on the space segment, there is substantial overlap in the principles identified in section 3.2 of the BPG and SPARTA's countermeasures. SPARTA's countermeasures are similar principles and/or best practices in their own right; therefore, a mapping of the 14 space segment related principles has been performed against SPARTA's countermeasures. In all cases there were multiple SPARTA countermeasures that aligned with the principles discussed in the BPG. The intention of this mapping is not to replace the BPG but augment the BPG principles with additional context and information to help system engineers implement the principles. Additionally, this mapping will provide implementers of the BPG a wealth of resources since the mapping will enable correlation to SPARTA techniques, their associated risk scores from the notional risk scoring tool, example requirements, additional cross correlations to NIST 800-53, ISO 27001, and D3FEND. Leveraging SPARTA in addition to the BPG as a source for threat-informed techniques offers benefits by providing a correlation between attacks with defense strategies.

The intent of mapping SPARTA countermeasures to the BPG and standards like NIST SP 800-53 and ISO 27001 is to provide SPARTA users with additional perspective of the security principle as well as how the SPARTA countermeasure aligns with compliance/regulatory/best practices published by such standards bodies.

ID	Name	Principle	Rationale	SPARTA Countermeasures
MI-ARCH-01	Mission Essential Data Flow Function	The mission should establish and maintain a current and accurate data flow diagram covering mission essential data flows, including those that pass through mission-external service providers.	A good data flow diagram provides understanding what data is needed by the system, and how that data flows across networks and communications links. In turn, this provides essential insight to understand where particular risk to the system may emerge, and where additional scrutiny or defenses may be warranted.	CM0001 | CM0002 | CM0020 | CM0022 | CM0070 | CM0071 | CM0073
MI-ARCH-02	Mission Least Privilege Function	The mission should employ the principles of domain separation and least privilege for the on-board architecture, communications, and control.	Least privilege designs will protect the main processor and core control functions of the vehicle from compromised assemblies by limiting the actions that can be executed on shared buses and onboard networks from recognized attack vectors. Segmentation and boundary control on the vehicle will mitigate supply chain attacks in procured or provided assemblies and in onboard software of varying provenance, as well as operational vulnerabilities when multiple command paths are available (e.g., an instrument with its own command link). Fault management systems should be employed to power off or block non-safety-critical assemblies that exhibit behavior that suggests compromise or failure.	CM0022 | CM0031 | CM0032 | CM0037 | CM0038 | CM0039 | CM0040 | CM0050 | CM0065 | CM0067

D3-CI	Configuration Inventory	Configuration inventory identifies and records the configuration of software and hardware and their components throughout the organization.
D3-DI	Data Inventory	Data inventorying identifies and records the schemas, formats, volumes, and locations of data stored and used on the organization's architecture.
D3-SWI	Software Inventory	Software inventorying identifies and records the software items in the organization's architecture.
D3-AVE	Asset Vulnerability Enumeration	Asset vulnerability enumeration enriches inventory items with knowledge identifying their vulnerabilities.
D3-NNI	Network Node Inventory	Network node inventorying identifies and records all the network nodes (hosts, routers, switches, firewalls, etc.) in the organization's architecture.
D3-HCI	Hardware Component	Hardware component inventorying identifies and records the hardware items in the organization's architecture.

NIST References

The following references have been used in SPARTA Countermeasures and/or Defense-in-Depth Space Threats. While this is not a full list of the relevent NIST controls, these are the ones our subject matter experts found most relevent.

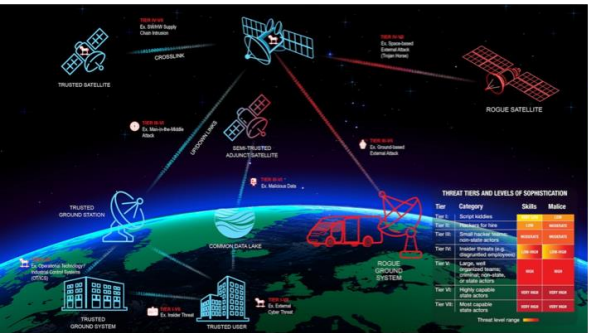
ID	Name	Description	SPARTA Countermeasures	ISO 27001
AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage	CM0005	5.2 | 5.3 | 7.5.1 | 7.5.2 | 7.5.3 | A.5.1 | A.5.2 | A.5.4 | A.5.15 |

View ISO 27001 Requirements | View ISO 27001 Controls

ID	Name	SPARTA Countermeasures	NIST Rev 5
A.5	Organizational controls	None	None
A.5.1	Policies for information security	CM0005 | CM0022 | CM0024 | CM0026 | CM0027 | CM0028 | CM0004	AC-1 | AT-1 | AU-1 | CA-1 | CM-1 | CP-1 | IA-1 | IR-1 | MA-1 | MP-1 | PE-1 | PL-1 | PM-1 | PS-1 | RA-1 | SA-1 | SC-1 | SI-1 | SR-1
A.5.2	Information security roles and responsibilities	CM0005 | CM0020 | CM0022 | CM0041 | CM0052 | CM0054 | CM0074 | CM0075 | CM0076 | CM0079 | CM0081 | CM0087 | CM0070 | CM0006 | CM0042 | CM0044 | CM0043 | CM0045 | CM0048 | CM0001 | CM0009 | CM0024 | CM0025 | CM0026 | CM0027 | CM0028 | CM0030 | CM0031 | CM0050 | CM0004 | CM0010 | CM0011 | CM0012 | CM0013 | CM0015 | CM0017 | CM0018 | CM0019 | CM0023 | CM0039 | CM0046 | CM0047 | CM0055 | CM0035 | CM0053 | CM0056 | CM0051 | CM0037 | CM0038 | CM0057 | CM0021	AC-1 | AT-1 | AU-1 | CA-1 | CM-1 | CM-9 | CP-1 | CP-2 | IA-1 | IR-1 | MA-1 | MP-1 | PE-1 | PL-1 | PM-1 | PM-2 | PM-10 | PM-29 | PS-1 | PS-7 | PS-9 | RA-1 | SA-1 | SA-3 | SA-9 | SC-1 | SI-1 | SR-1
A.5.3	Segregation of duties	None	AC-5
A.5.4	Management responsibilities	CM0005 | CM0024 | CM0025 | CM0026 | CM0027 | CM0028 | CM0041 | CM0004 | CM0010 | CM0012 | CM0013 | CM0015 | CM0021 | CM0048 | CM0022	AC-1 | AT-1 | AU-1 | CA-1 | CM-1 | CP-1 | IA-1 | IR-1 | MA-1 | MP-1 | PE-1 | PL-1 |

Intel or Attacker Driven Countermeasure / Control / Requirement Derivation

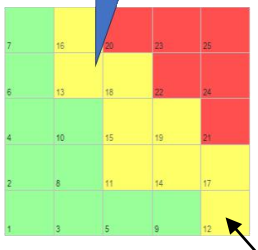
Threat Intel → SPARTA Techniques → SPARTA Countermeasures → NIST SP 800-53 Controls



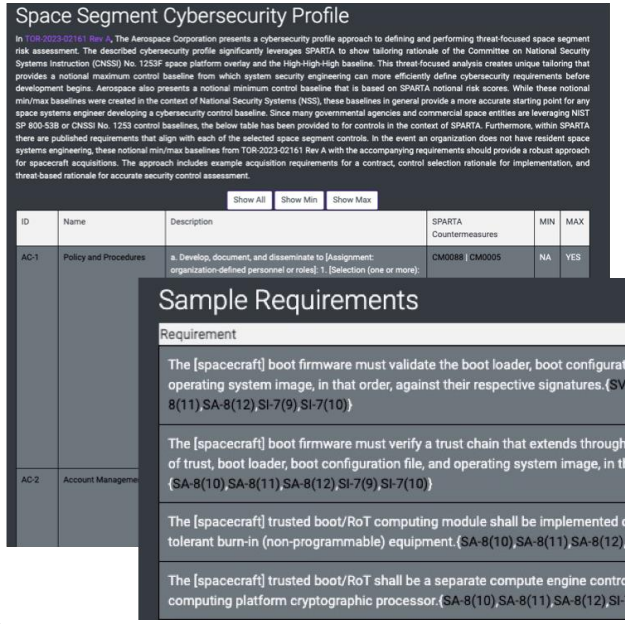
Decomposing Threats

Mitigating Countermeasures

Controls &/or Requirements



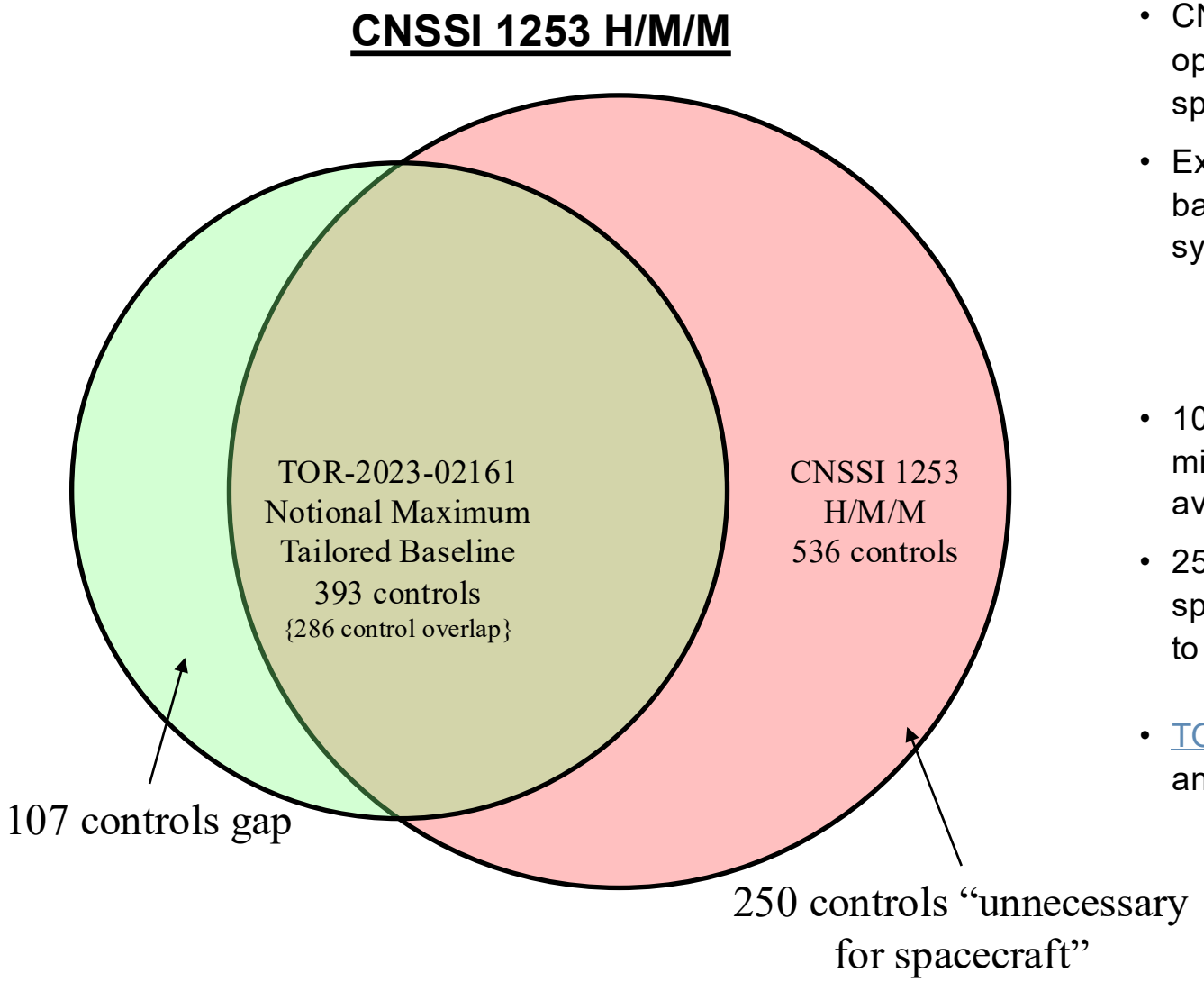
Impact + Likelihood → Impact, Vulnerabilities, Threats → Risk



informs

https://sparta.aerospace.org/notional-risk-scores

Cybersecurity Control Tailoring



- CNSSI 1253 H/M/M include 536 controls, many of which are optimized for terrestrial systems and not directly applicable to spacecraft.
- Ex: TOR-2023-02161 proposes a tailored spacecraft-specific baseline of 393 controls, derived from threat-informed analysis and system constraints.
  - The tailored baseline matches 286 controls with CNSSI 1253, demonstrating alignment with core federal security expectations while remaining mission-relevant.
- 107 CNSSI controls were omitted from CNSS H/M/M due to misalignment with spacecraft, threat surface, or operational realities avoiding over-engineering and system bloat.
- 250 controls from CNSSI 1253 were deemed unnecessary for spacecraft, illustrating the risk of blindly applying terrestrial baselines to orbital platforms.
  - **Needs tailored** on implementation side for spacecraft
- TOR-2023-02161 solidifies the need for mission-specific, efficient, and sufficient cybersecurity protections, not maximalist checklists.
  - New Space Overlay will include space platform guidance and justification for selection

Cybersecurity is not about checking every box; it's about mitigating actual threats. For spacecraft, that means customizing the baseline to fit the environment, mission, and threat profile.

Examples of the 107 – Not in the CNSS HMM Baseline

From Upcoming Space Overlay

(U) AC-3(2), Access Enforcement | Dual Authorization

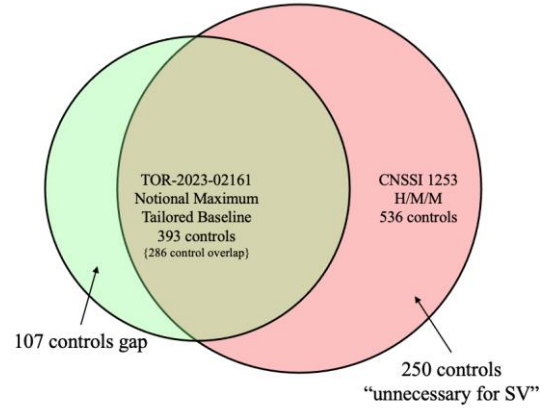
(U) Justification to Select:

(U) Relevant threats outlined in https://sparta.aerospace.org/countermeasures/references/AC-3/2

(U) Space Platform Guidance:

(U) When spacecraft missions require dual authorization to reduce the risk of single-person misuse, the ground segment typically handles the two-operator aspect. However, incorporating indicators of dual concurrence within the command stream can be crucial for on-orbit verification. For instance, multiple cryptographic signatures, or a specific "arm–execute" handshake, can be enforced to ensure no single console operator can unilaterally activate mission-critical functions like propulsion changes or cryptographic key rotation. Even if the flight software does not confirm dual operator presence, it can validate that all commands carry the expected signatures or security tokens. Space programs can also maintain an onboard audit log reflecting dual-authorization events, providing evidence that two authorized parties concurred post-facto. Any high-stakes command requiring unanimous ground approval might only be accepted upon detecting these dual credentials if the vehicle's design includes limited autonomy. Autonomy preserves mission integrity and safeguards against internal threat actors or compromised ground stations. Ultimately, dual authorization fosters a "checks-and-balances" mentality for all critical uplinks—especially given that a single flawed or malicious command could jeopardize an irreplaceable national asset in orbit.

		actors can also utilize compromised ground stations t a viable attack vector and the appropriate/equivalent s
IA-0007	Compromise Ground System	Threat actors may initially compromise the ground sys compromising encryption keys, and compromising aut topology, missions ran out of said ground station, birds
IA-0007.01	Compromise On-Orbit Update	Threat actors may manipulate and modify on-orbit upd table/memory values, or replacing compiled versions v
IA-0007.02	Malicious Commanding via Valid GS	Threat actors may compromise target owned ground s components have already been configured for commu including Execution and Exfiltration.
IA-0008	Rogue External Entity	Threat actors may gain access to a victim spacecraft t
IA-0008.01	Rogue Ground Station	Threat actors may gain access to a victim spacecraft t
IA-0008.02	Rogue Spacecraft	Threat actors may gain access to a target spacecraft u of the commercial and military assets in space are trac of the larger attenuation that would otherwise affect th
IA-0009	Trusted Relationship	Access through trusted third-party relationship exploits actors as these interconnections typically lack stringen
IA-0009.02	Vendor	Threat actors may target the trust between vendors an be intended to be limited to the infrastructure being ma resources or network locations. In the spacecraft cont



(U) SR-11(3), Component Authenticity | Anti-Counterfeit Scanning

(U) Justification to Select:

(U) Relevant threats outlined in https://sparta.aerospace.org/countermeasures/references/SR-11/3

(U) Space Platform Guidance:

(U) Anti-counterfeit scanning is particularly crucial in the aerospace industry, where an inauthentic microcontroller or sensor could jeopardize millions in launch costs or result in total mission failure. Techniques include optical inspections to detect mismatched markings, x-ray or ultrasound scans for hidden defects and advanced electrical testing to verify the expected performance envelope. On the software side, thorough code-signing validation or compile-time reproducibility checks can unmask trojans within binaries. Implementing these scans at multiple checkpoints—upon receipt from suppliers, during integration, and before final storage—provides layered assurance. If suspicious anomalies are detected, further forensic analysis can confirm whether the part is safe to fly. By investing in rigorous anti-counterfeit measures, mission teams safeguard not only hardware functionality but the mission's credibility and security posture as well.

(U) SC-40(1), Wireless Link Protection | Electromagnetic Interference

(U) Justification to Select:

(U) Relevant threats outlined in https://sparta.aerospace.org/countermeasures/references/SC-40/1

(U) Space Platform Guidance:

(U) Electromagnetic interference (EMI) and jamming threaten continuous communication with space platforms, particularly in tactical or high-conflict scenarios. Programs must assess the potential for benign interference—like solar activity or crowded spectral environments—and deliberate enemy jamming. Designers often employ spread-spectrum techniques such as frequency hopping or direct-sequence spreads, combined with NSA-approved cryptographic keys, to maintain a robust link even under hostile conditions. This ensures that an adversary cannot quickly zero in on the exact frequency a spacecraft is using; for small satellites with limited transmitter power, narrow-beam antennas, or cross-links between multiple vehicles can bolster resilience. By methodically planning anti-jam capabilities before the Preliminary Design Review, teams minimize late-cycle design upheavals and deliver a better platform to weather both natural and adversarial disruptions.

EX-0013	Flooding	Threat actors use flo various outcomes. A devastating results t
EX-0013.01	Valid Commands	Threat actors may u layer with valid com
EX-0013.02	Erroneous Input	Threat actors inject signals/commands/
EX-0014	Spoofing	Threat actors may a important informati processed erroneou
EX-0016	Jamming	Jamming is an elect completely reversibl wrong satellite can j potentially impact s
EX-0016.01	Uplink Jamming	An uplink jammer is operators from send command station o
EX-0016.02	Downlink Jamming	Downlink jammers t field of view of the r above the terminal i cover a wider area a ground.* *https://ae
EX-0016.03	Position, Navigation, and Timing (PNT) Jamming	Threat actors may a
PER-0005	Credentialed	Threat actors may a

Translating Into Mission-Ready Protections

Control implementation SHOULD be coordinated set of technical security capabilities (e.g., SPARTA Countermeasure) to achieve real security outcomes in spacecraft

- Ex: SI-7 (“Software, Firmware, and Information Integrity”) provides a broad guidelines for protecting the integrity of code and data but does not prescribe specific technologies or mechanisms to achieve that goal.
- In practice, fully implementing SI-7 in spacecraft requires a coordinated set of security capabilities, that could include:
  - Secure boot, Software Bill of Materials (SBOM), static and dynamic code analysis, dependency and supply chain validation, cryptographic signatures for firmware updates, development environment hardening, onboard anomaly detection or IDS, etc.
- Compliance with SI-7 is not achieved through a single action, but through a layered and integrated defense strategy that touches development, supply chain, runtime verification, and update processes.
- From an engineering perspective, SI-7 does not translate to a single requirement or test case instead, it must be interpreted and decomposed into multiple testable, traceable requirements aligned to the system architecture.
- SPARTA shows, robust implementation of a control like SI-7 spans multiple lifecycle stages, including:
  - Early design threat modeling (to inform which parts of FSW need integrity protection) {CM0020}
  - Development-time assurance (e.g., static analysis, SBOM) {CM0019, CM0012}
  - Deployment protections (e.g., secure boot, digital signature enforcement) {CM0014, CM0021}
  - On-orbit detection and response (e.g., monitoring unexpected process behavior or memory tampering) {CM0032}
- The takeaway: A control like SI-7 must be translated into specific security countermeasures, and these countermeasures must be implemented collectively to provide real, mission-relevant and mission-specific protections (i.e., mission tailoring).
  - Simply stating “we comply with SI-7” is insufficient unless it’s tied to concrete evidence of these layered protections.

It’s not just the “right controls” – but the interpretation matters!!!!

Many to Many Goes the Other Way

One Countermeasure to Several Controls

- Previous slide shows SI-7 can be interpreted / translated to numerous countermeasures in SPARTA
  - Same applies where one countermeasure encompasses several controls
- SPARTA Countermeasures represent security principles such as *Least Privilege*, *Secure Boot*, etc.
  - These are not 1-to-1 mappings to NIST controls; they represent goals that span multiple lifecycle phases and require composite implementation.
- Ex: CM0039: Least Privilege
  - Typically thought of as only AC-6
- In reality, CM0039 spans a wide range of controls, including:
  - Account control and access restrictions (AC-2, AC-3 variants, AC-6)
  - Execution and domain separation (SC-2(2), SC-32(1), SC-49, SC-50)
  - Minimized system complexity and functionality (CM-7, CM-7(5), CM-7(8))
  - Architectural enforcement and layering (PL-8, SA-8 series)
  - Security-driven development practices (SA-3, SA-4(9), SA-17(7))
  - If you just implement one NIST control (e.g., AC-6), you might technically meet the letter of a checklist, but you've missed the intent and full protective posture.
- You cannot implement "Least Privilege" meaningfully by turning on just one control as it requires **cross-cutting design, enforcement, and verification** mechanisms.

NIST Rev5 Controls

- AC-2 - Account Management
- AC-3(13) - Access Enforcement | Attribute-based Access Control
- AC-3(15) - Access Enforcement | Discretionary and Mandatory Access Control
- AC-4(2) - Information Flow Enforcement | Processing Domains
- AC-6 - Least Privilege
- CA-3(6) - Information Exchange | Transfer Authorizations
- CM-7 - Least Functionality
- CM-7(5) - Least Functionality | Authorized Software
- CM-7(8) - Least Functionality | Binary or Machine Executable Code
- PL-8 - Security and Privacy Architectures
- PL-8(1) - Security and Privacy Architectures | Defense in Depth
- SA-3 - System Development Life Cycle
- SA-4(9) - Acquisition Process | Functions, Ports, Protocols, and Services in Use
- SA-8 - Security and Privacy Engineering Principles
- SA-8(3) - Security and Privacy Engineering Principles | Modularity and Layering
- SA-8(4) - Security and Privacy Engineering Principles | Partially Ordered Dependencies
- SA-8(9) - Security and Privacy Engineering Principles | Trusted Components
- SA-8(13) - Security and Privacy Engineering Principles | Minimized Security Elements
- SA-8(14) - Security and Privacy Engineering Principles | Least Privilege
- SA-8(15) - Security and Privacy Engineering Principles | Predicate Permission
- SA-8(19) - Security and Privacy Engineering Principles | Continuous Protection
- SA-17(7) - Developer Security and Privacy Architecture and Design | Structure for Least Privilege
- SC-2(2) - Separation of System and User Functionality | Disassociability
- SC-7(29) - Boundary Protection | Separate Subnets to Isolate Functions
- SC-32(1) - System Partitioning | Separate Physical Domains for Privileged Functions
- SC-49 - Hardware-enforced Separation and Policy Enforcement
- SC-50 - Software-enforced Separation and Policy Enforcement

SPARTA Countermeasures Have Application Across the Spacecraft Architecture and Lifecycle

Applying Least Privilege across Spacecraft Architecture

- **Flight Software (FSW) / Command & Data Handling (C&DH)**
  - Only allow processes/modules to access the memory, telemetry points, and device interfaces they explicitly require.
  - **Example (*execution and domain separation*)**
    - The thermal control module cannot issue propulsion commands.
    - The payload application can only access its own data buffer and not system logs or bus telemetry.
  - **Sample Controls:** AC-6, CM-7, SC-2(2), SA-8(14)

- **Communications Subsystem (COMM)**
  - Restrict which processes can send/receive commands or telemetry through uplinks/downlinks.
  - **Example (*account control and access restrictions*)**
    - Only the secure command validation module can forward uplinked commands to the C&DH.
    - Downlink interfaces are isolated from command processing to prevent spoofed echo injection.
  - **Sample Controls:** SC-7(10), AC-3, SC-16(2), CM-7(8)

- **Attitude Determination and Control System (ADCS)**
  - Restrict command access to attitude actuators to authorized modes and subsystems.
  - **Example (*minimized system complexity and functionality*)**
    - Safe-mode software cannot execute precision maneuver commands.
    - Only ground-validated command sequences can change the inertial reference frame.
  - **Sample Controls:** AC-3(13), SA-17(7), SA-8(15)

- **Cryptographic Subsystem / Key Management**
  - Access to stored keys or key-handling routines is limited to cryptographic modules.
  - **Example (*architectural enforcement and layering*)**
    - Command validation routines can access keys, but telemetry generation software cannot.
    - Key update functions are write-only to FSW and verified via digital signature.
  - **Sample Controls:** AC-4(2), SC-12, SC-13, SA-8(9), SA-8(23)

- **Bootloader / Firmware**
  - Ensure only authorized processes can trigger reboots or upload firmware.
  - **Example (*security-driven development practices*)**
    - The update daemon must validate cryptographic signatures before applying firmware.
    - The bootloader prevents any process from modifying its own memory region after execution begins.
  - **Sample Controls:** SI-7(8), CM-7(5), PL-8(1), SA-8(19)

Interpretation matters!!!!

This is a large gap when applying controls or RMF in general to spacecraft.

Example on Most Missions

Where Control Interpretation Matters….

- SPARTA CM: On-board Intrusion Detection & Prevention
  - 62 controls mapped to this CM in SPARTA
    - 47 of which are on in the H/M/M baseline
    - Using/combining only those 47 controls “should” result in an IDS/IPS being deployed on the spacecraft
      - But yet, it doesn’t? Why?
- Hard pressed to find a different interpretation of the items in green to not mean IDS/IPS on the spacecraft
  - Logging, recovery/reconstitution, Self-analysis, denial-of-service protection, malicious code protection, system monitoring, system-wide IDS, indicators of compromise, memory protection, etc.
- It is important to understand countermeasures (i.e., security capabilities) that are required to mitigate certain attacker techniques and leverage resources and guidance from NIST/CNSSI where appropriate to influence implementation/interpretation

ID	Name
AU-2	Event Logging
AU-3	Content of Audit Records
AU-3(1)	Content of Audit Records | Additional Audit Information
AU-4	Audit Log Storage Capacity
AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage
AU-5	Response to Audit Logging Process Failures
AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration
AU-6(4)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-9(2)	Protection of Audit Information | Store on Separate Physical Systems or Components
AU-14	Session Audit
CA-7(6)	Continuous Monitoring | Automation Support for Monitoring
CP-10	System Recovery and Reconstitution
IR-4	Incident Handling
IR-4(11)	Incident Handling | Integrated Incident Response Team
IR-4(12)	Incident Handling | Malicious Code and Forensic Analysis
IR-4(14)	Incident Handling | Security Operations Center
IR-5	Incident Monitoring
IR-5(1)	Incident Monitoring | Automated Tracking, Data Collection, and Analysis
PL-8	Security and Privacy Architectures
PL-8(1)	Security and Privacy Architectures | Defense in Depth
RA-10	Threat Hunting
SA-8(21)	Security and Privacy Engineering Principles | Self-analysis
SA-8(22)	Security and Privacy Engineering Principles | Accountability and Traceability
SA-8(23)	Security and Privacy Engineering Principles | Secure Defaults
SC-5	Denial-of-service Protection
SC-5(3)	Denial-of-service Protection | Detection and Monitoring
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic
SC-7(10)	Boundary Protection | Prevent Exfiltration
SC-16(2)	Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms
SI-3	Malicious Code Protection
SI-3(10)	Malicious Code Protection | Malicious Code Analysis
SI-4	System Monitoring
SI-4(1)	System Monitoring | System-wide Intrusion Detection System
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-time Analysis
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic
SI-4(5)	System Monitoring | System-generated Alerts
SI-4(10)	System Monitoring | Visibility of Encrypted Communications
SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies
SI-4(16)	System Monitoring | Correlate Monitoring Information
SI-4(23)	System Monitoring | Host-based Devices
SI-4(24)	System Monitoring | Indicators of Compromise
SI-4(25)	System Monitoring | Optimize Network Traffic Analysis
SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability for Significant Events
SI-10(6)	Information Input Validation | Injection Prevention
SI-16	Memory Protection

Asking AI to Interpret the 47 Controls

Using the below 47 controls from NIST 800-53, could you give me your interpretation of what that would translate to on the spacecraft? Give me 2 different interpretations of what technology, security capability, countermeasure, etc.

Grok

- Onboard System Security: Implementing the NIST 800-53 controls directly within the spacecraft's onboard systems, emphasizing autonomous security, real-time monitoring, and protection of critical hardware and software components.
- Mission Resilience and Recovery: Spacecraft's ability to withstand and recover from attacks or failures, focusing on redundancy, recovery mechanisms, and proactive threat mitigation to ensure mission continuity.

ChatGPT

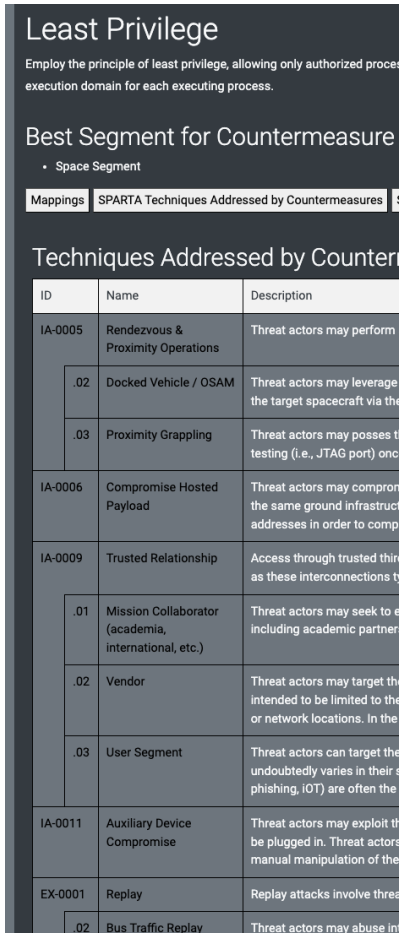
- Mission-Aware Cyber Monitoring and Detection: These controls demand the ability to monitor, detect, and alert on anomalous activity across the spacecraft.
- Space-Adapted Incident Response and Forensics: This set of controls supports the ability to detect, analyze, and respond to cyber incidents across all mission phases.

Enter SPARTA countermeasures….space focused, lifecycle application, driven by attacker techniques

- Some programs **do not follow** the RMF process correctly
  - Spacecraft implementation of CNSSI 1253 HMM baseline **should include** an on-board IDS, because the baseline calls for it as shown in previous 2 slide, and the threat landscape justifies it
    - But why do our current systems not have them?
      - Bad interpretation of controls and lack of threat awareness, if security analysis concludes that one is not needed then training on effective tailoring, as defined in CNSSI 1253, is what can remedy this
        - SPARTA countermeasures recommendations for a spacecraft illustrate effective tailoring
      - Improper allocation of resources when recommended but not within cost/schedule constraints
- Regardless of how you do RMF, SPARTA has the features to recommend a list of specific countermeasures any modern NSS spacecraft should implement if it is to address threats common to all spacecraft.
  - By necessity, the list is large
    - However, SPARTA has and will improve features to help program focus on the subset that is most likely to deliver value to a specific program

Security is a Many-to-Many Problem

- Attacker techniques don't exploit just one gap/one control deficiency
  - They exploit the absence of multiple controls.
    - Example: A privilege escalation attack may exploit weak account management (AC-2), lack of access enforcement (AC-3), and missing process isolation (SC-32).
- A single NIST control only addresses part of a technique, and often only in one lifecycle phase (e.g., AC-6 may define least privilege, but it doesn't enforce it in software design or execution domains).
- SPARTA Countermeasures represent defense-in-depth strategies.
  - Each one maps to multiple NIST controls, implemented across development, architecture, runtime, and policy.
  - Each one also mitigates multiple techniques, not just one.
    - Implement the CM in the context of the technique it is addressing
      - Memory injection is different than lateral movement from payload
        - EX-0012.03: Modify On-Board Values: Memory Write/Loads
        - LM-0001: Hosted Payload
      - Memory injection could be related to FSW, Operating System
      - Hosted payload could be more bus level access control



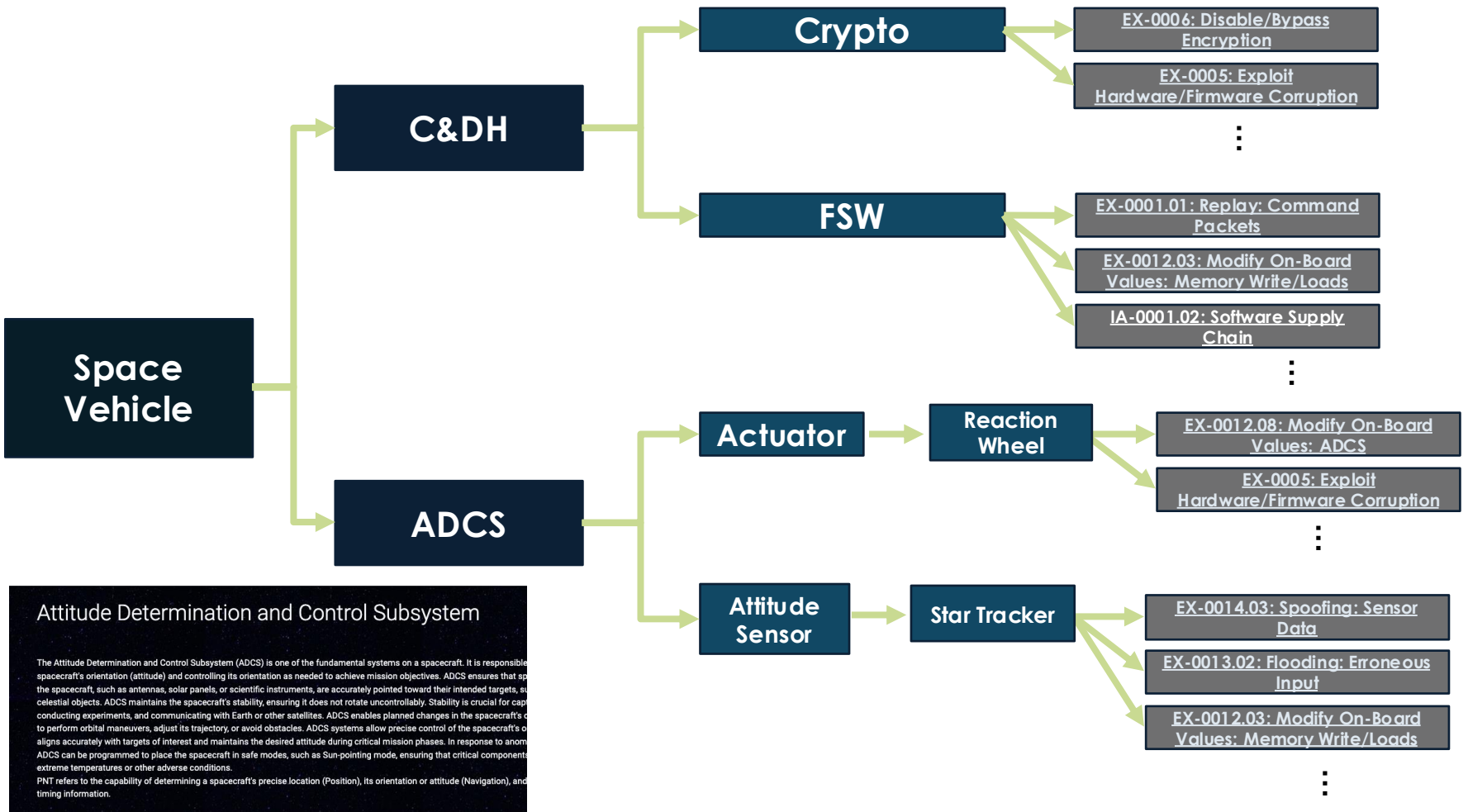
Same as Std. IT and ATT&CK

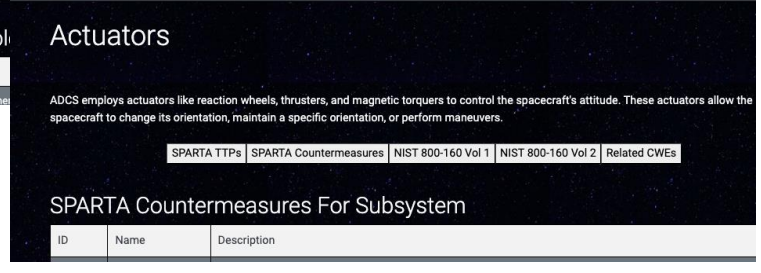
ntrol	Control Name	Mapping Type	Technique ID	Technique Name
AC-6	Least Privilege	mitigates	T1547.013	XDG Autostart Entries
AC-6	Least Privilege	mitigates	T1547.004	Winlogon Helper DLL
AC-6	Least Privilege	mitigates	T1543.003	Windows Service
AC-6	Least Privilege	mitigates	T1021.006	Windows Remote Management
AC-6	Least Privilege	mitigates	T1546.003	Windows Management Instrumentatio
AC-6	Least Privilege	mitigates	T1047	Windows Management Instrumentatio
AC-6	Least Privilege	mitigates	T1222.001	Windows File and Directory Permissions
AC-6	Least Privilege	mitigates	T1059.003	Windows Command Shell
AC-6	Least Privilege	mitigates	T1505.003	Web Shell
AC-6	Least Privilege	mitigates	T1056.003	Web Portal Capture
AC-6	Least Privilege	mitigates	T1606.001	Web Cookies
AC-6	Least Privilege	mitigates	T1021.005	VNC
AC-6	Least Privilege	mitigates	T1059.005	Visual Basic
AC-6	Least Privilege	mitigates	T1055.014	VDSO Hijacking
AC-6	Least Privilege	mitigates	T1078	Valid Accounts
AC-6	Least Privilege	mitigates	T1550	Use Alternate Authentication Material
AC-6	Least Privilege	mitigates	T1552	Unsecured Credentials

NIST Rev5 Controls

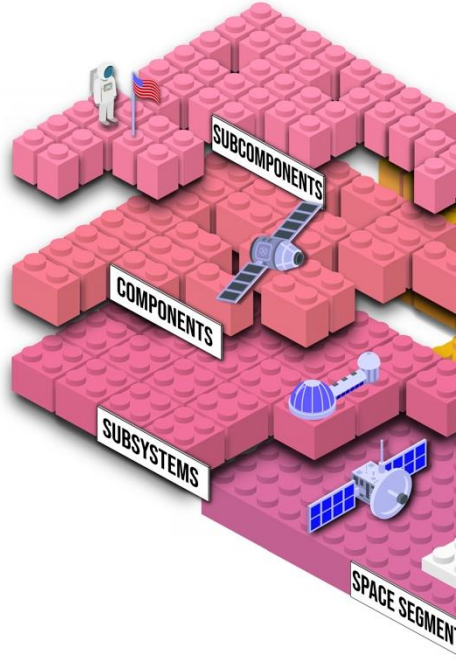
- AC-2 - Account Management
- AC-3(13) - Access Enforcement | Attribute-based Access Control
- AC-3(15) - Access Enforcement | Discretionary and Mandatory Access Control
- AC-4(2) - Information Flow Enforcement | Processing Domains
- AC-6 - Least Privilege
- CA-3(6) - Information Exchange | Transfer Authorizations
- CM-7 - Least Functionality
- CM-7(5) - Least Functionality | Authorized Software
- CM-7(8) - Least Functionality | Binary or Machine Executable Code
- PL-8 - Security and Privacy Architectures
- PL-8(1) - Security and Privacy Architectures | Defense in Depth
- SA-3 - System Development Life Cycle
- SA-4(9) - Acquisition Process | Functions, Ports, Protocols, and Services in Use
- SA-8 - Security and Privacy Engineering Principles
- SA-8(3) - Security and Privacy Engineering Principles | Modularity and Layering
- SA-8(4) - Security and Privacy Engineering Principles | Partially Ordered Dependencies
- SA-8(9) - Security and Privacy Engineering Principles | Trusted Components
- SA-8(13) - Security and Privacy Engineering Principles | Minimized Security Elements
- SA-8(14) - Security and Privacy Engineering Principles | Least Privilege
- SA-8(15) - Security and Privacy Engineering Principles | Predicate Permission
- SA-8(19) - Security and Privacy Engineering Principles | Continuous Protection
- SA-17(7) - Developer Security and Privacy Architecture and Design | Structure for Least Privilege
- SC-2(2) - Separation of System and User Functionality | Disassociability
- SC-7(29) - Boundary Protection | Separate Subnets to Isolate Functions
- SC-32(1) - System Partitioning | Separate Physical Domains for Privileged Functions
- SC-49 - Hardware-enforced Separation and Policy Enforcement
- SC-50 - Software-enforced Separation and Policy Enforcement

Spacecraft Decomposition Tool - https://sparta.aerospace.org/sc-decomp





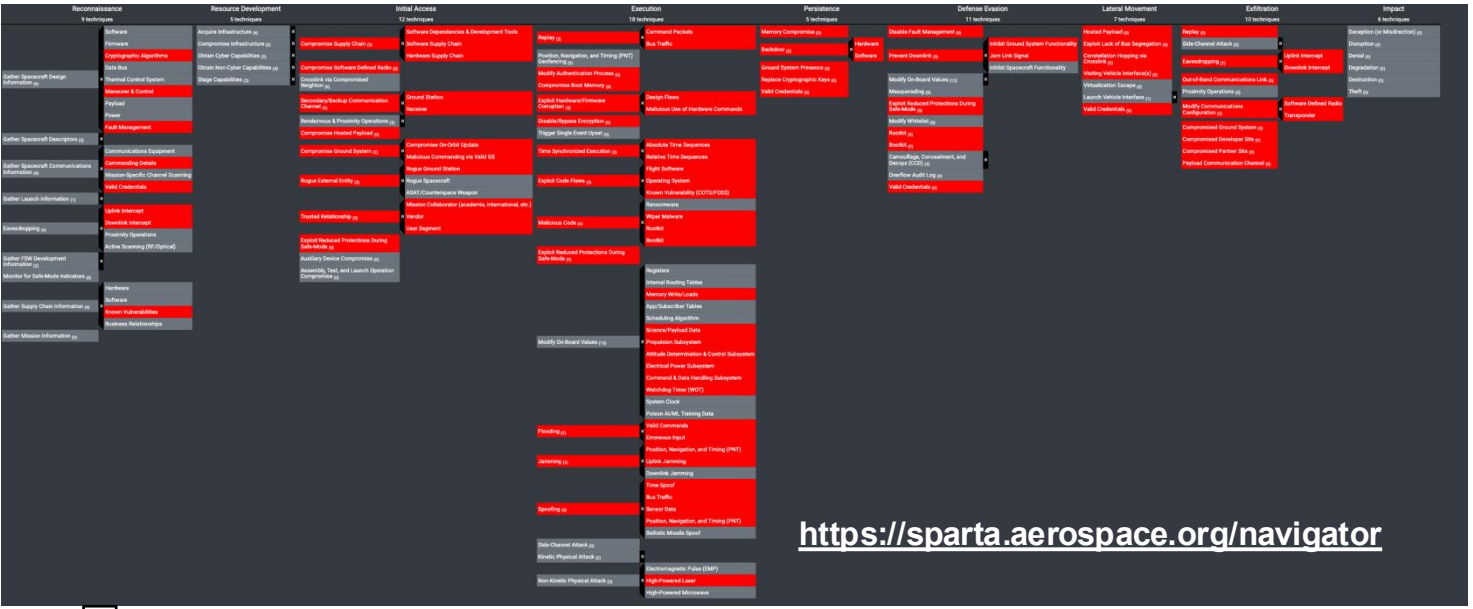
Another way to approach countermeasures Components vice System Level



Countermeasures, NIST 800-160 Vol 1 / Vol 2, & CWE classes to mitigate when designing the subsystem/component

Narrowing Down Countermeasures @ Spacecraft (system level)

Notional Risk Score Between 21-25



Potential Countermeasures

Potential Requirements via Excel Export

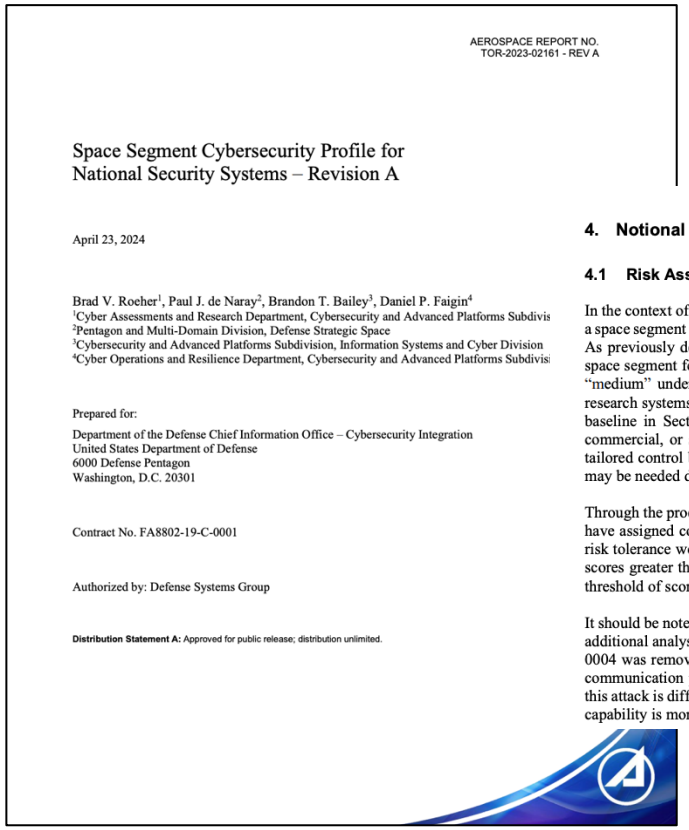
Or via NIST control

	Family	ID	Name	Discussion	Control	Techniques	TOR Threats	ISO IEC 27001	TOR 2023-02161 Min	02161 Max	Low Level Requirements
3	Access Control	AC-2(11)	Account Management | Usage Conditions	Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].	REC-0001.01,REC-0001.02,REC-0001.03,REC-0001.04,REC-0001.05,REC-0001.06,REC-0001.07,REC-0001.08,REC-0001.09,REC-0002.01,REC-0002.02,REC-0002.03,REC-0003.01,REC-0003.02,REC-	SV-AC-1,SV-MA-7	None	NA	NA	The [spacecraft] shall provide the capability to restrict command lock based on geographic location of ground stations.
6	Access Control	AC-3	Access Enforcement	Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	REC-0001,REC-0002,REC-0003,REC-0004,REC-0006,REC-0007,REC-0008,REC-0009,RD-0002,RD-0003,RD-0004,IA-0002,IA-0003,IA-0004,IA-0006,IA-0007,IA-0008,IA-0009,IA-0012,EX-0001,PER-0003,PER-0005,DE-0002,DE-0004,DE-0011,LM-0001,LM-0003,LM-0007,EXF-0001,EXF-0006,EXF-0007,EXF-0008,EXF-0009	SV-AC-3,SV-CF-2,SV-IT-2,SV-AV-4,SV-IT-5,SV-MA-3,SV-SP-3,SV-SP-6,SV-SP-9,SV-AC-6,SV-AC-8,SV-SP-11,SV-AV-5,SV-AC-1,SV-CF-1,SV-IT-1,SV-MA-7,SV-AC-4,SV-CF-3,SV-MA-4	A.5.15,A.5.33,A.8.3,A.8.4,A.8.18,A.8.20,A.8.2	NA	YES	The [organization] shall develop and document program-specific access control policies for controlling information flow and leakage on-board the spacecraft. [The [organization] shall develop and document program-specific identification and authentication policies for accessing the development environment and spacecraft. [The [organization] shall protect documentation and Controlled Unclassified Information (CUI) as required, in accordance with the risk management strategy. [The [organization] shall identify and properly classify mission sensitive design/operations information and access control shall be applied in accordance with classification guides and applicable federal laws, Executive Orders, directives, policies, regulations, and standards. [The [organization] shall protect the security plan from unauthorized disclosure and modification. [The [organization] shall ensure security requirements/configurations are placed in accordance with NIST 800-171 with enhancements in 800-172 on the development environments to prevent the compromise of source code from supply chain or information leakage perspective. [The [organization] shall identify the key system components or capabilities that require isolation through physical or logical means. [The

	A	
1	Design Con	Requirement
2	Design	The [spacecraft] shall implement a reference monitor mechanism that mediates access between subjects and objects based on a defined set of rules, tha
3	Design	The [spacecraft] shall ensure that sensitive information can only be accessed by personnel with appropriate roles and an explicit need for such informat
4	Design	The [spacecraft] shall enforce approved authorizations for controlling the flow of information within the platform and between interconnected system
5	Design	The [spacecraft] security implementation shall ensure that information should not be allowed to flow between partitioned applications unless explicit
6	Design	The [organization] shall state that information should not be allowed to flow between partitioned applications unless explicitly permitted by the Prog
7	Design	The [spacecraft] shall utilize automated mechanisms to protect sensitive information and detect and alert when sensitive information is accessed with
8	Design	The [organization] shall document and design a security architecture using a defense-in-depth approach that allocates the [organization]s defined safeg
9	Design	The [organization] shall ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.
10	Design	The [organization] shall implement a security architecture and design that provides the required security functionality, allocates security controls amo
11	Design	The [spacecraft] shall protect authenticator content from unauthorized disclosure and modification.
12	Design	The [spacecraft] encryption key handling shall be handled outside of the onboard software and protected using cryptography.
13	Design	The [spacecraft] encryption keys shall be restricted so that the onboard software is not able to access the information for key readout.
14	Design	The [spacecraft] encryption keys shall be restricted so that they cannot be read via any telecommands.
15	Design	The [spacecraft] shall authenticate the ground station (and all commands) and other spacecraft before establishing remote connections using bidirecti
16	Design	The [spacecraft] shall implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitat
17	Design	The [spacecraft] shall ensure that processes reusing a shared system resource (e.g., registers, main memory, secondary storage) do not have access to inf
18	Design	The [spacecraft] shall protect the confidentiality and integrity of the following information using cryptography while it is at rest: [all information].
19	Design	The [spacecraft] shall maintain the confidentiality and integrity of information during preparation for transmission and during reception.
20	Design	The [spacecraft] shall encrypt all telemetry on downlink regardless of operating mode to protect current state of spacecraft.
21	Design	The [spacecraft] shall not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode).
22	Design	The [spacecraft] shall, when transferring information between different security domains, implements the following security policy filters that require
23	Design	The [spacecraft] shall implement boundary protections to separate bus, communications, and payload components supporting their respective functi

An Application of Down Selecting Baseline Countermeasures

AEROSPACE REPORT NO. TOR-2023-02161 - REV A



AEROSPACE REPORT NO.
TOR-2023-02161 - REV A

Space Segment Cybersecurity Profile for
National Security Systems – Revision A

April 23, 2024

Brad V. Roeher[1], Paul J. de Naray[2], Brandon T. Bailey[3], Daniel P. Faigin[4]
[1]Cyber Assessments and Research Department, Cybersecurity and Advanced Platforms Subdivis
[2]Pentagon and Multi-Domain Division, Defense Strategic Space
[3]Cybersecurity and Advanced Platforms Subdivision, Information Systems and Cyber Division
[4]Cyber Operations and Resilience Department, Cybersecurity and Advanced Platforms Subdivisi

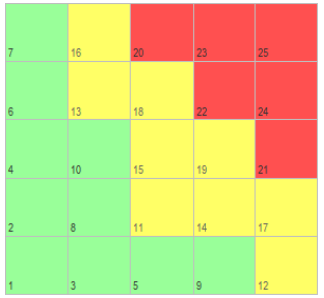
Prepared for:

Department of the Defense Chief Information Office – Cybersecurity Integration
United States Department of Defense
6000 Defense Pentagon
Washington, D.C. 20301

Contract No. FA8802-19-C-0001

Authorized by: Defense Systems Group

Distribution Statement A: Approved for public release; distribution unlimited.



4. Notional Minimum Tailored Control Baseline

4.1 Risk Assessment

In the context of NSS the definition of a minimum tailored control baseline still includes the importance of a space segment supporting NSS, but there will be considerations for lower impact and higher risk tolerance. As previously described in the process for risk scores, there is consideration for notional criticality of a space segment for NSS. The minimum impact of an NSS space segment would be a notional criticality of "medium" under the SPARTA risk score descriptions. A notional "low" criticality is for academic or research systems, while a notional "high" criticality correlates with the notional maximum tailored control baseline in Section 3. A notional medium criticality aligns with a strategy for civil, science/weather, commercial, or similar systems that are NSS or support NSS. While this approach provides a notional tailored control baseline to utilize as a minimum, it must be emphasized that additional countermeasures may be needed depending upon system-specific technologies, capabilities, or missions.

Through the process described in Section 2.3, the SPARTA notional risk scores in the 5x5 risk matrix cells have assigned colors as shown in Figure 6. For this notional minimum tailored control baseline, a higher risk tolerance would be a threshold that correlates with mitigating only risks that are red, which are those scores greater than 20 in the medium criticality category. The selection of techniques that match this risk threshold of scores greater than 20 are shown in Appendix D.

It should be noted that two techniques in the minimum tailored baseline techniques were removed based on additional analysis: EXF-0004 (Out-of-Band Communications Link) and EX-0001.02 (Bus Traffic). EXF-0004 was removed because the missions in the medium criticality do not likely utilize these out-of-band communication paths (e.g., cryptographic rekeying). EX-0001.02 was removed because an execution of this attack is difficult to accomplish on orbit as it requires direct access to the satellite bus interface and this capability is more complex of a compromise to execute.

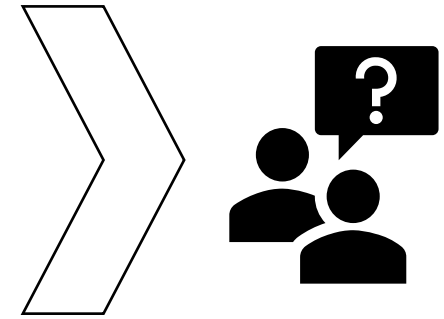
https://sparta.aerospace.org/resources/TOR-2023-02161-RevA%20Space%20Segment%20Cybersecurity%20Profile.pdf

Appendix E – Notional Minimum Tailored Baseline Countermeasures

Table 8 captures all unique SPARTA countermeasures associated with the techniques listed in Appendix D and with the removal of noted countermeasures in Table 3.

Table 8 - Notional Minimum Tailored Baseline Countermeasures

Countermeasure	Title
CM0002	COMSEC
CM0006	Cloaking Safe-mode
CM0007	Software Version Numbers
CM0008	Security Testing Results
CM0009	Threat Intelligence Program
CM0010	Update Software
CM0011	Vulnerability Scanning
CM0012	Software Bill of Materials
CM0013	Dependency Confusion
CM0014	Secure boot
CM0015	Software Source Control
CM0016	CWE List
CM0017	Coding Standard
CM0018	Dynamic Analysis
CM0019	Static Analysis
CM0020	Threat modeling



Maybe I can't afford all?
How do I prioritize?

SPARTA Tools Provide List of Countermeasures to Consider to Mitigate Techniques, but May Need to Prioritize

How Do I Prioritize Countermeasures?

Manually / SME

- In general threats/attacker techniques {SPARTA NRS or real intel} should drive countermeasure selection
  - Compliance is real and we must also adhere to CNSSI (e.g., HMM baseline). Why not have both? (CM <> Controls)
  - **Assumption:** Already established the threats/attacker techniques that are deemed important/detrimental to my mission

Concepts to consider when prioritizing:

- Mission Impact & Criticality
  - Is the countermeasure protecting a mission-critical function or high-assurance subsystem (e.g., C&DH, propulsion, ADCS)?
  - Would its absence lead to irreversible mission degradation?
- Technical Feasibility / Architecture Compatibility
  - Can it be implemented on your spacecraft given SWaP (Size, Weight, and Power) constraints?
  - Do I already have that countermeasure in my baseline? (e.g., COMSEC)
  - Does it require hardware redundancy or architectural features not present in your system?
- Technology Readiness Level (TRL)
  - Is the countermeasure spaceflight-proven, or is it low TRL and risky to implement on your timeline?
  - Has it been demonstrated in similar spacecraft or in your operational environment?
- Cost and Schedule Impact
  - What are the labor hours, hardware mods, or software changes required?
  - Does it require significant redesign, external coordination, or long-lead items?
- Defense-in-Depth Contribution
  - Does it complement other mitigations? Is it a single point of failure or part of a layered defense?
  - Can it reduce residual risk when paired with other controls?

How Do I Prioritize Countermeasures?

~~Manually / SME~~ → ***Generically at Scale***

- In general threats/attacker techniques {SPARTA NRS or real intel} should drive countermeasure selection
  - Compliance is real and we must also adhere to CNSSI (e.g., HMM baseline). Why not have both? (CM <> Controls)
  - **Assumption:** Already established the threats/attacker techniques that are deemed important/detrimental to my mission

Concepts to consider when prioritizing:

- Mission Impact & Criticality
  - Is the countermeasure protecting a mission-critical function or high-assurance subsystem (e.g., C&DH, propulsion, ADCS)?
  - Would its absence lead to irreversible mission degradation?
- Technical Feasibility / ~~Architecture Compat~~ibility
  - Can it be implemented on your spacecraft given SWaP (Size, Weight, and Power) constraints?
  - Does it require hardware redundancy or architectural features not present in your system?
- Technology Readiness Level (TRL)
  - Is the countermeasure spaceflight-proven, or is it low TRL and risky to implement on your timeline?
  - Has it been demonstrated in similar spacecraft or in your operational environment?
- Cost and Schedule Impact
  - What are the labor hours, hardware mods, or software changes required?
  - Does it require significant redesign, external coordination, or long-lead items?
- ~~Defense-in-Depth Contribution~~ → ***Grouped***
  - Does it complement other mitigations? Is it a single point of failure or part of a layered defense?
  - Can it reduce residual risk when paired with other controls?

13

EFFICACY

Generic COST
$,$$,$$$,$$$$

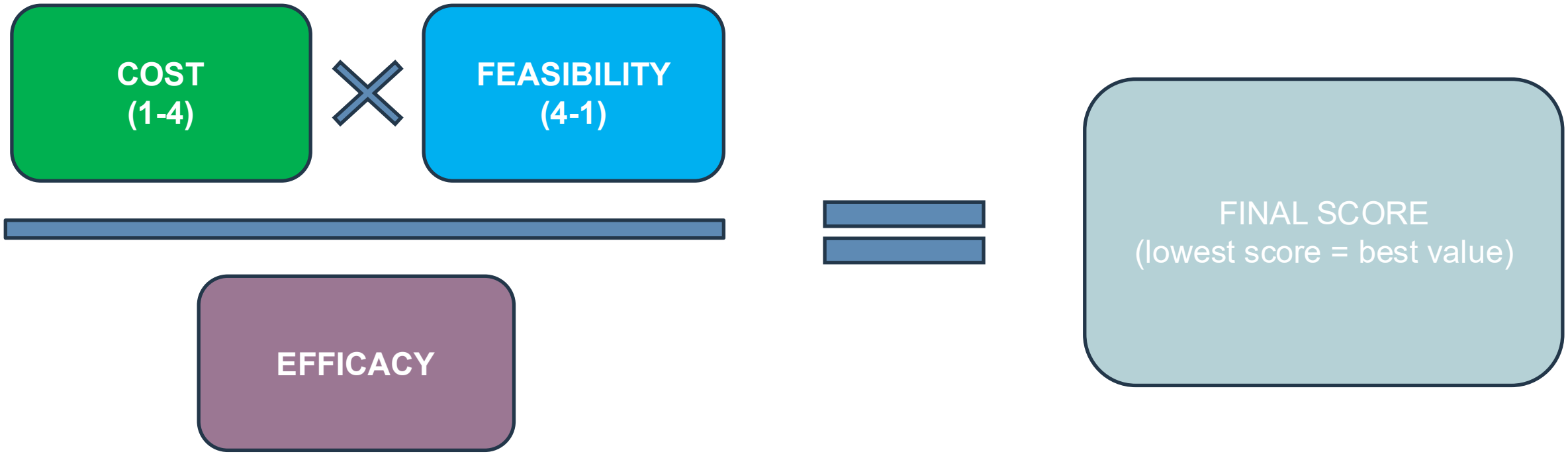
SPARTA 3.2

FEASABILITY

20

Alpha Version: SPARTA's NOTIONAL Countermeasure Prioritization

Attemping to Generically Prioritize SPARTA's Countermeasures



# of Techniques Mitigated

Average NRS of Techniques

E.g., 44 techniques mitigated translates to weight 1.44

NRS Average value sorted into 3 buckets based on score

Alpha Version: SPARTA's NOTIONAL Countermeasure Prioritization

SPARTA Countermeasure Tiering and Applicability

- **Objective:** Prioritize and categorize SPARTA cyber countermeasures based on cost, feasibility, and efficacy to guide implementation across space missions.

Three-Tier Prioritization Approach

- **Tier 1 CMs**:
  Most critical and feasible protections. Recommended for all missions to consider as the are foundational with high impact and lower implementation cost.
- **Tier 2 CMs**:
  Valuable protections but may involve moderate complexity, cost, or lower impact. Should be evaluated for mission-specific relevance.
- **Tier 3 CMs**:
  Advanced, emerging, or niche protections. Often high-cost or low-TRL; consider for highly capable or high-risk missions.

Platform-Based Applicability

- **Onboard Spacecraft CMs:** Protect in-flight assets and detect/respond to adversarial behavior on-orbit.
- **Process / Ground / Development CMs:** Address cybersecurity within design, development, testing, and mission control environments.

How to Use This Information

- Start with **Tier 1 CMs** relevant to both **onboard and ground/dev** domains.
- Assess **Tier 2 CMs** for mission risk, cost, and feasibility.
- Consider **Tier 3 CMs** for advanced threat environments or when TRL and budget permit.
- Use applicability (spacecraft vs. ground) to guide where and how each CM should be implemented.

Countermeasure	COST	FEASIBILITY	Techniques Mitigated Weight	NRS Avg Weight	EFFICACY	FINAL_SCORE (LOWE	CM Tiering	Onboard SV CM	Process/Ground/Dev CM
CM0019 Static Testing							Tier 1 CM		YES
CM0016 CWE List							Tier 1 CM		YES
CM0017 Coding Standard							Tier 1 CM		YES
CM0002 COMSEC							Tier 1 CM	YES	
CM0034 Monitor Critical Telemetry Points							Tier 1 CM	YES	YES
CM0015 Software Source Control							Tier 1 CM		YES
CM0031 Authentication							Tier 1 CM	YES	
CM0030 Crypto Key Management							Tier 1 CM	YES	YES
CM0004 Development Environment Security							Tier 1 CM		YES
CM0041 User Training							Tier 1 CM		YES
CM0011 Vulnerability Scanning							Tier 1 CM		YES
CM0012 Software Bill of Materials							Tier 1 CM		YES
CM0022 Criticality Analysis							Tier 1 CM		YES
CM0020 Threat modeling							Tier 1 CM		YES
CM0013 Dependency Confusion							Tier 1 CM		YES
CM0043 Backdoor Commands							Tier 1 CM	YES	
CM0008 Security Testing Results							Tier 1 CM		YES
CM0001 Protect Sensitive Information							Tier 1 CM		YES
CM0036 Session Termination							Tier 1 CM	YES	
CM0040 Shared Resource Leakage							Tier 1 CM	YES	
CM0047 Operating System Security							Tier 1 CM		YES
CM0072 Protocol Update / Refactoring							Tier 1 CM	YES	YES
CM0007 Software Version Numbers							Tier 1 CM		YES
CM0042 Robust Fault Management							Tier 1 CM	YES	
CM0006 Cloaking Safe Mode							Tier 1 CM	YES	
CM0054 Two-Person Rule							Tier 1 CM		YES
CM0032 On-board Intrusion Detection & Prevention							Tier 1 CM	YES	
CM0069 Process Whitelisting							Tier 1 CM	YES	
CM0035 Protect Authenticators							Tier 1 CM	YES	
CM0033 Relay Protection							Tier 1 CM	YES	
CM0010 Update Software							Tier 1 CM		YES
CM0070 Alternate Communications Paths							Tier 1 CM		YES
CM0048 Resilient Position, Navigation, and Timing							Tier 1 CM	YES	
CM0029 TRANSEC							Tier 1 CM	YES	
CM0039 Least Privilege							Tier 1 CM	YES	
CM0038 Segmentation							Tier 1 CM	YES	
CM0018 Dynamic Testing							Tier 1 CM		YES
CM0014 Secure boot							Tier 1 CM	YES	
CM0021 Software Digital Signature							Tier 1 CM	YES	
CM0055 Secure Command Mode(s)							Tier 2 CM	YES	
CM0023 Configuration Management							Tier 2 CM		YES
CM0050 On-board Message Encryption							Tier 2 CM	YES	
CM0053 Physical Security Controls							Tier 2 CM		YES
CM0052 Insider Threat Protection							Tier 2 CM	YES	YES
CM0056 Data Backup									

Applying Approach to Sample Mission

Using SPARTA's NOTIONAL Countermeasure Scores

- Start with the full list of recommended countermeasures from SPARTA that were derived from applicable SPARTA techniques
- Take the list of existing countermeasures already implemented/planned (e.g., COMSEC, Ground Security)
  - Perform gap analysis
    - Could leverage the HMM baseline as starting point, but …
      - Can lead to blind spot as the controls can be interpreted in many ways and often not interpreted across the lifecycle nor all the applicable systems, sub-systems, interfaces, component, etc.
      - As discussed, controls need to be interpreted multiple times over for the appropriate system, sub-system, interface, component, etc. >>> Countermeasures guidance in SPARTA contains guidance to assist
- Getting to that "top SPARTA countermeasures"
  - Top 5 for the Developer/Development {Not onboard the spacecraft}

CM0019 Static Testing
CM0016 CWE List
CM0017 Coding Standard
CM0015 Software Source Control
CM0004 Development Environment Security

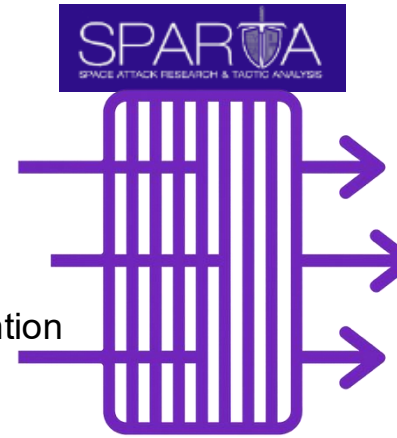
To prevent weak SW making its way onto the spacecraft likely already required via NIST RMF

Custom CWE list likely not required unless Application STIG compliance is required

Applying Approach Specifically to Sample Mission (cont.)

Getting to that Top SPARTA Countermeasures for Onboard Spacecraft

- CM0002 COMSEC
- CM0034 Monitor Critical Telemetry Points
- CM0031 Authentication
- CM0030 Crypto Key Management
- CM0043 Backdoor Commands
- CM0036 Session Termination
- CM0040 Shared Resource Leakage
- CM0072 Protocol Update / Refactoring
- CM0042 Robust Fault Management
- CM0006 Cloaking Safe Mode
- CM0032 On-board Intrusion Detection & Prevention
- CM0069 Process Whitelisting
- CM0035 Protect Authenticators
- CM0033 Relay Protection
- CM0048 Resilient Position, Navigation, and Timing
- CM0029 TRANSEC
- CM0039 Least Privilege
- CM0038 Segmentation
- CM0014 Secure boot
- CM0021 Software Digital Signature



Recommended Top Base on SPARTA's NOTIONAL CM Scores

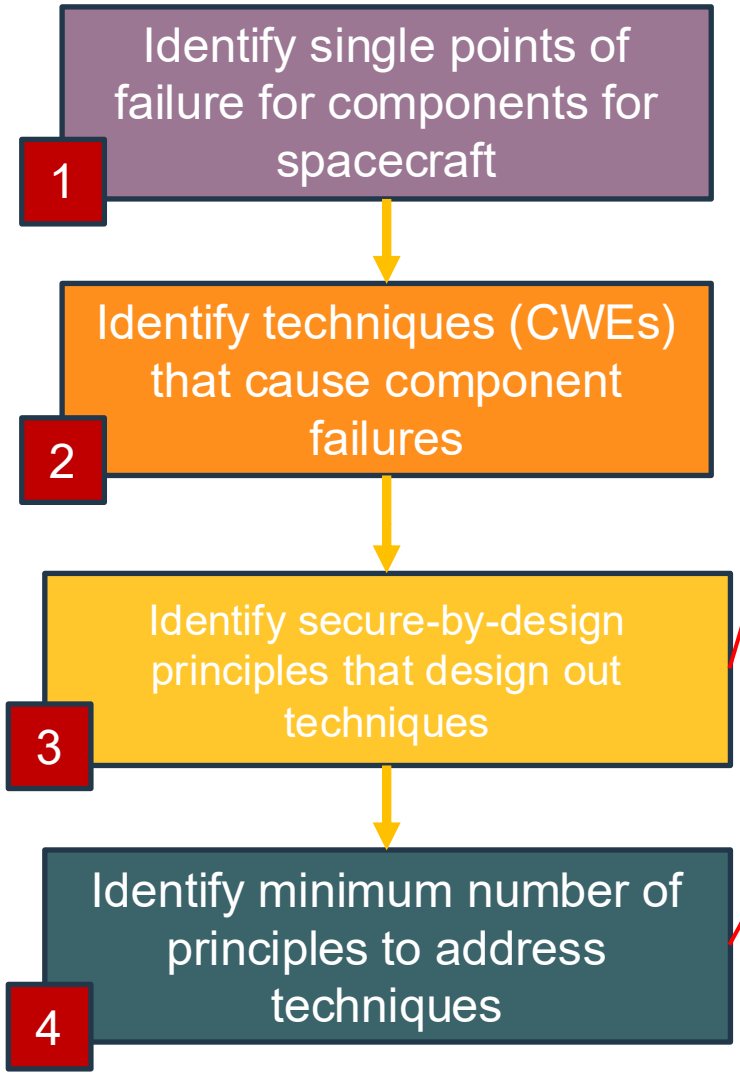
- CM0034 Monitor Critical Telemetry Points
- CM0043 Backdoor Commands
- CM0036 Session Termination
- CM0032 On-board Intrusion Detection & Prevention
- CM0039 Least Privilege
- CM0038 Segmentation
- CM0014 Secure boot & CM0021 Software Digital Signature

Already in Baseline/Plan

Let's Validate the Recommended Countermeasures with Another Information Source

Essential Spacecraft Security Capabilities - Derived from IEEE P3349/P3536 Std

https://www.researchgate.net/publication/382524612_Minimum_Requirements_for_Space_System_Cybersecurity_-Ensuring_Cyber_Access_to_Space



		800-160 vol 2	800-160 vol 1
CWE-1390	Weak Authentication	Attribute-based Usage Restriction	Least Privilege, Mediated Access, Domain Separation
CWE-20	Improper Input Validation	Behavioral Validation	Anomaly Detection, Commensurate Trustworthiness, Continuous Protection
CWE-285	Improper Authorization	Attribute-based Usage Restriction	Least Privilege, Mediated Access, Domain Separation
CWE-287	Improper Authentication	Attribute-based Usage Restriction	Least Privilege, Mediated Access, Domain Separation
CWE-300	Channel Accessible by Non-Endpoint	Behavioral Validation	Anomaly Detection, Commensurate Trustworthiness, Continuous Protection
CWE-346	Origin Validation Error	Dynamic Threat Awareness	Anomaly Detection, Continuous Protection
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	Consistency Analysis	Compositional Trustworthiness
CWE-665	Improper Initialization	Integrity Checks	Continuous Protection, Commensurate Trustworthiness
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Adaptive Management	Commensurate Protection, Commensurate Response
CWE-311	Missing Encryption of Sensitive Data	Dynamic Resource Awareness	Continuous Protection
CWE-923	Insecure Communication	Attribute-based Usage Restriction	Least Privilege, Mediated Access, Domain Separation

Some Key Principles: ***Least Privilege***, ***Domain Separation***, *Commensurate Protection, Commensurate Trustworthiness, Continuous Protection,* ***Integrity Checks***, *Compositional Trustworthiness, Substantiated Trustworthiness, Consistency Analysis, Adaptive Management,* ***Anomaly Detection***, *Least Sharing*

Top Four Design Principles from IEEE Analysis

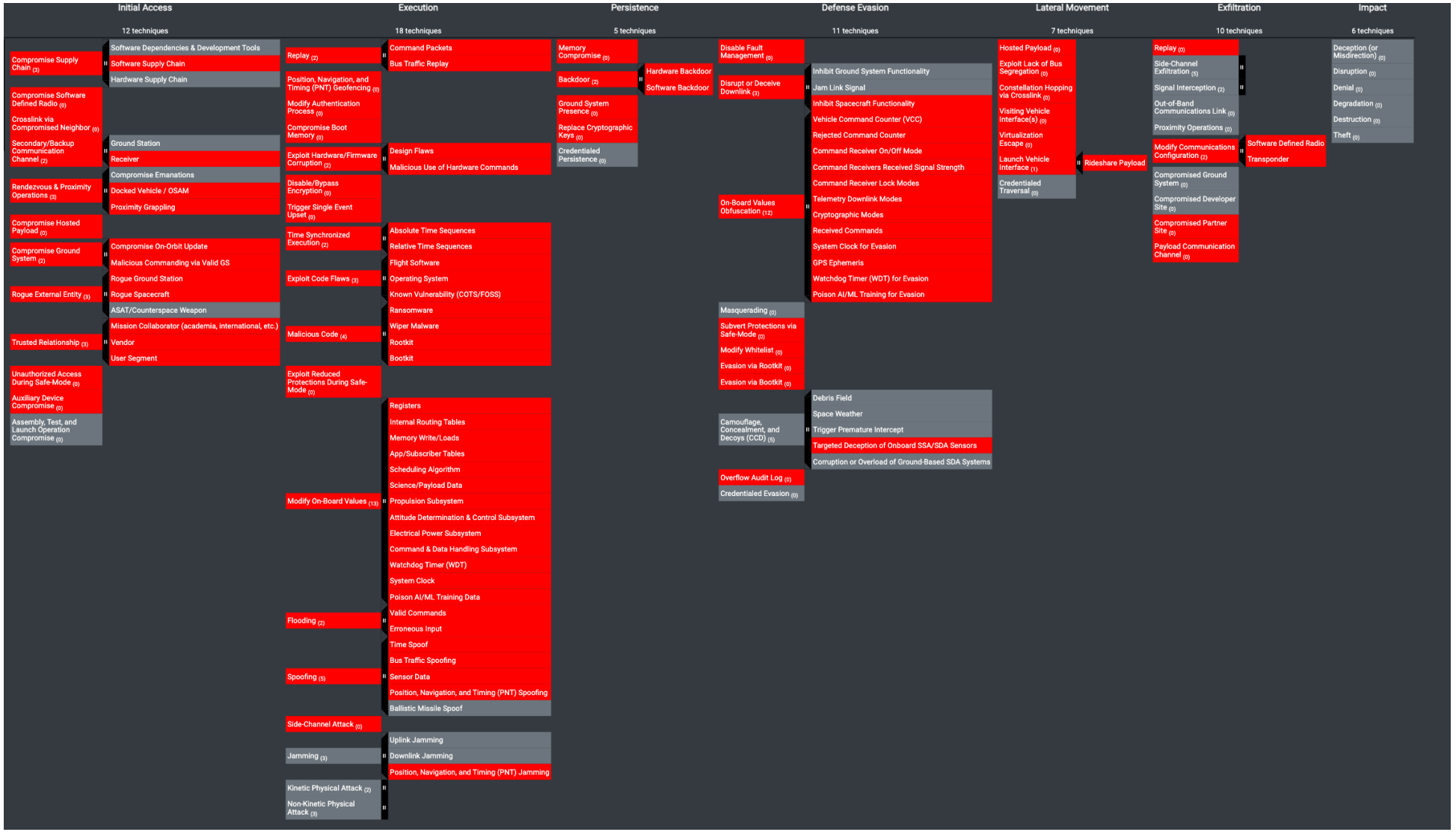
- **Least Privilege:** Each system element is allocated privileges that are necessary to accomplish its specified functions but no more
  - The application of the principle of least privilege means allocating to a system element only the privileges that are necessary to permit that element to perform the functions required of it. This could include a need to modify, delete, use, or configure a resource, or to authorize, start/enable, or stop/disable a process.
- **Domain Separation:** Domains with distinctly different protection needs are physically or logically separated
  - This is achieved through the control of information flow and data between domains as well as control over the use of a system capability between domains. This distinction may include separating critical functions from less critical functions, such as separating the flight control functions to the payload.
- **Anomaly Detection:** Any salient anomaly in the system or its environment is detected in a timely manner that enables effective response action.
  - The purpose of anomaly detection is to identify the need to take corrective action to address a loss condition that has occurred or that will occur if conditions that affect the system behavior are allowed to persist. Anomaly detection is critical to achieving loss control objectives to prevent and limit loss and its adverse effects. The “timely manner” aspect of anomaly detection reflects the urgency to detect emerging loss conditions as early as possible. Early detection increases response action options, such as graduated response options, and ensures that response actions have sufficient time to have an effect.
- **Integrity Checks:** Apply and validate checks of the integrity or quality of data, components (HW/SW), or services to guard against surreptitious modification.

**** From NIST 800-160 vol 1 & 2***

Helps Address Aspects of Many High-Risk Technique from SPARTA

Extending Beyond COMSEC & Ground Security Only

Least Privilege
Domain Separation
Anomaly Detection
Integrity Checks



Contextual Premise – Why Add?

Consensus Across NIST 800-160, 800-53, and SPARTA Countermeasure Prioritization

- Initial protections (COMSEC, AuthN, Key Mgmt) only guard *entry points* and not post-access or insider threats
  - Adversaries may exploit legitimate access, bypass command checks, or move laterally once onboard
  - Spacecraft are deterministic and resource-constrained so early anomaly detection is critical
  - Assume breach mindset requires onboard protections that detect, isolate, and contain malicious activity
- Justification for Additional SPARTA Countermeasures
  - **Monitor Critical Telemetry (CM0034):** Detects subsystem misuse, signal tampering, behavioral drift, or stealthy attacks
  - **Backdoor Commands (CM0043):** Prevents using valid but unauthorized hardware or maintenance commands
  - **Session Termination (CM0036):** Prevents session hijacking or abuse after mission access is granted
  - **Onboard IDS/IPS (CM0032):** Enables real-time detection & response without waiting for ground contact
  - **Least Privilege (CM0039):** Limits damage if credentials or processes are compromised
  - **Segmentation (CM0038):** Prevents adversaries from pivoting between processes or domains (e.g., payload → bus)
  - **Secure Boot & Signed Software (CM0014, CM0021):** Validates all code running on-board to prevent implants

Aligns with Key NIST 800-160 v1/v2 Secure-by-Design Principles that Support Resilience

Least Privilege: Reduces impact radius of malicious or misused access.
Domain Separation: Isolates critical subsystems to prevent cascading compromise.
Anomaly Detection: Finds threats without known signatures via behavioral deviations.
Integrity Checks: Ensures commands, configs, and software remain untampered.

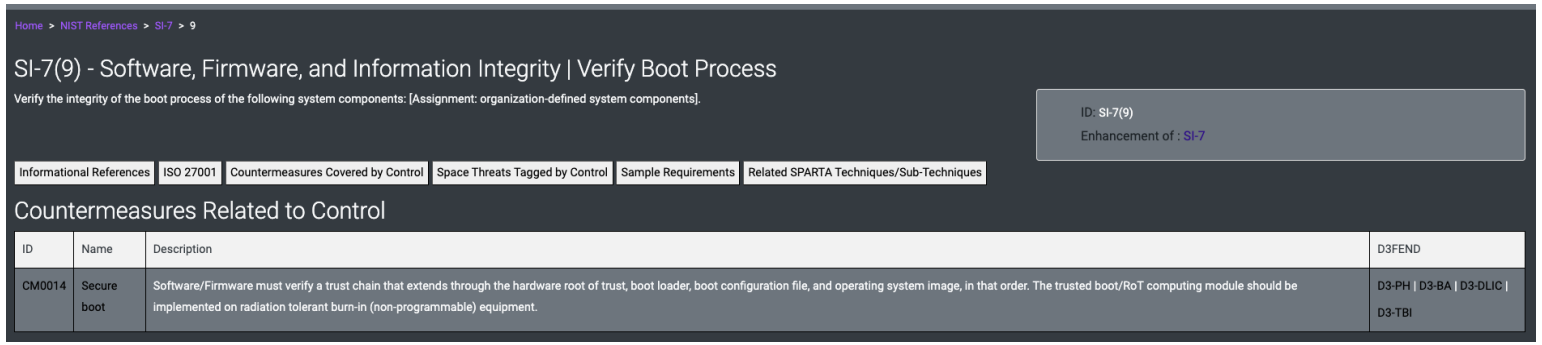
Not Good Enough … Need to Move to Requirements

Difference Between Controls & Requirements

- Justing saying “secure boot” likely not good enough

  or

- Levying CNSS Control SI-7(9)
  - Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].
  - Can translate to 16 design shalls
    - https://sparta.aerospace.org/countermeasures/references/SI-7/9

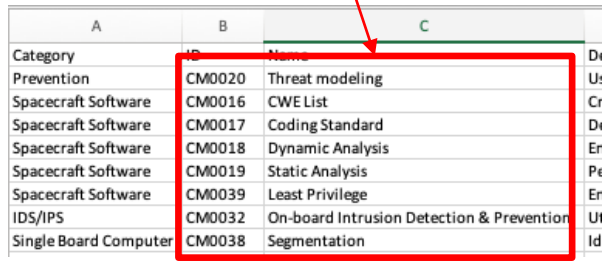


Requirements Linked to Countermeasures

Sample Requirements from SPARTA (not all encompassing)

- The [spacecraft] shall enforce approved authorizations for controlling the flow of information within the platform and between interconnected systems so that information does not leave the platform boundary unless it is encrypted. AC-3(3),AC-3(4),AC-4,AC-4(6),AC-4(21),CA-3,CA-3(6),CA-3(7),CA-9,IA-9,SA-8(19),SC-8(1),SC-16(3)
- The [spacecraft] security implementation shall ensure that information should not be allowed to flow between partitioned applications unless explicitly permitted by the system. AC-3(3),AC-3(4),AC-4,AC-4(6),AC-4(21),CA-9,IA-9,SA-8(3),SA-8(18),SA-8(19),SC-2(2),SC-7(29),SC-16,SC-32
- The [spacecraft] shall implement boundary protections to separate bus, communications, and payload components supporting their respective functions. AC-3(3),AC-3(4),CA-9,SA-8(3),SA-8(14),SA-8(18),SA-8(19),SA-17(7),SC-2,SC-2(2),SC-7(13),SC-7(21),SC-7(29),SC-16(3),SC-32,SI-3,SI-4(13),SI-4(25)
- The [spacecraft] shall maintain a separate execution domain for each executing process. SA-8(14),SA-8(19),SC-2(2),SC-7(21),SC-39,SI-3
- The [spacecraft] shall employ the principle of least privilege, allowing only authorized accesses processes which are necessary to accomplish assigned tasks in accordance with system functions. AC-3,AC-6,AC-6(9),CA-9,CM-5,CM-5(5),CM-5(6),SA-8(2),SA-8(5),SA-8(6),SA-8(14),SA-8(23),SA-17(7),SC-2,SC-7(29),SC-32,SC-32(1),SI-3
- The [spacecraft] shall isolate mission critical functionality from non-mission critical functionality by means of an isolation boundary (e.g. via partitions) that controls access to and protects the integrity of, the hardware, software, and firmware that provides that functionality. AC-3(3),AC-3(4),CA-9,SA-8(3),SA-8(19),SA-17(7),SC-2,SC-3,SC-3(4),SC-7(13),SC-7(29),SC-32,SC-32(1),SI-3,SI-7(10),SI-7(12)
- The [spacecraft] shall monitor and collect all onboard cyber-relevant data (from multiple system components), including identification of potential attacks and sufficient information about the attack for subsequent analysis. AC-6(9),AC-20,AC-20(1),AU-2,AU-12,IR-4,IR-4(1),RA-10,SI-3,SI-3(10),SI-4,SI-4(1),SI-4(2),SI-4(7),SI-4(24)
- The [spacecraft] shall generate cyber-relevant audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, and the outcome of the event. AU-3,AU-3(1),AU-12,IR-4,IR-4(1),RA-10,SI-3,SI-3(10),SI-4(7),SI-4(24)
- The [spacecraft] shall provide automated onboard mechanisms that integrate audit review, analysis, and reporting processes to support mission processes for investigation and response to suspicious activities to determine the attack class in the event of a cyber attack. AU-6(1),IR-4,IR-4(1),IR-4(12),IR-4(13),PM-16(1),RA-10,SA-8(21),SA-8(22),SC-5(3),SI-3,SI-3(10),SI-4(7),SI-4(24),SI-7(7)
- The [spacecraft] shall be designed and configured so that spacecraft memory can be monitored by the on-board intrusion detection/prevention capability. RA-10,SA-8(21),SI-3,SI-3(10),SI-4,SI-4(1),SI-4(24),SI-16
- The [spacecraft] shall have on-board intrusion detection/prevention system that monitors the mission critical components or systems. RA-10,SC-7,SI-3,SI-3(8),SI-4,SI-4(1),SI-4(7),SI-4(13),SI-4(24),SI-4(25),SI-10(6)

Countermeasures



	A	B	C	
	Category	ID	Name	De
	Prevention	CM0020	Threat modeling	Us
	Spacecraft Software	CM0016	CWE List	Cr
	Spacecraft Software	CM0017	Coding Standard	De
	Spacecraft Software	CM0018	Dynamic Analysis	En
	Spacecraft Software	CM0019	Static Analysis	Pe
	Spacecraft Software	CM0039	Least Privilege	En
	IDS/IPS	CM0032	On-board Intrusion Detection & Prevention	Ut
	Single Board Computer	CM0038	Segmentation	Id

"Shalls"

	A
1	Design Con equirement
2	Design he [spacecraft] shall enforce approved authorizations for controlling the flow of information within t platform and between interconnected systems
3	Design he [organization] shall define the security safeguards that are to be automatically employed when int rity violations are discovered.
4	Design he [organization] shall document and design a security architecture using a defense-in-depth approac that allocates the [organization]s defined safegu
5	Design he [organization] shall ensure that the allocated security safeguards operate in a coordinated and mu ally reinforcing manner.
6	Design he [organization] shall implement a security architecture and design that provides the required secur functionality, allocates security controls amor
7	Design he [organization] shall define acceptable secure communication protocols available for use within th mission in accordance with applicable federal la
8	Design he [spacecraft] shall only use [organization]-defined communication protocols within the mission.
9	Design he [spacecraft] shall only use communication protocols that support encryption within the mission.
10	Design he [spacecraft] shall be configured to provide only essential capabilities.
11	Design he [spacecraft] security implementation shall ensure that information should not be allowed to flow etween partitioned applications unless explicitl
12	Design he [spacecraft] shall implement boundary protections to separate bus, communications, and payloa components supporting their respective functio
13	Design he [spacecraft] data within partitioned applications shall not be read or modified by other applicatio s/partitions.
14	Design he [spacecraft] shall prevent unauthorized access to system resources by employing an efficient capab ity based object model that supports both confi
15	Design he [spacecraft] shall prevent unauthorized and unintended information transfer via shared system res urces.
16	Design he [spacecraft] shall maintain a separate execution domain for each executing process.
17	Design he [spacecraft] shall employ the principle of least privilege, allowing only authorized accesses process which are necessary to accomplish assigned tas
18	Design he [spacecraft] shall isolate mission critical functionality from non-mission critical functionality by m ans of an isolation boundary (e.g.via partitions)
19	Design he [spacecraft] shall ensure that processes reusing a shared system resource (e.g., registers, main mem ry, secondary storage) do not have access to info
20	Design he [spacecraft] shall monitor and collect all onboard cyber-relevant data (from multiple system com nents), including identification of potential atta
21	Design he [spacecraft] shall generate cyber-relevant audit records containing information that establishes wh t type of event occurred, when the event occurr
22	Design he [spacecraft] shall attribute cyber attacks and identify unauthorized use of the platform by downlin g onboard cyber information to the mission gr
23	Design he [spacecraft] shall alert in the event of the audit/logging processing failures.
24	Design he [spacecraft] shall provide the capability of a cyber "black-box" to capture necessary data for cyber ensics of threat signatures and anomaly resolut
25	Design he [spacecraft] shall provide automated onboard mechanisms that integrate audit review, analysis, a reporting processes to support mission process
26	Design he [spacecraft] shall integrate cyber related detection and responses with existing fault management apabilities to ensure tight integration between t
27	Design he [spacecraft] shall implement cryptographic mechanisms to protect the integrity of audit informat n and audit tools.
28	Design he [spacecraft] shall prevent the installation of Flight Software without verification that the compone t has been digitally signed using a certificate tha
29	Design he [organization] shall employ automated tools that provide notification to ground operators upon d scovering discrepancies during integrity verifica
30	Design he [spacecraft] shall provide automatic notification to ground operators upon discovering discrepan es during integrity verification.
31	Design he [spacecraft], upon detection of a potential integrity violation, shall provide the capability to [audi the event and alert ground operators].
32	Design he [spacecraft] shall perform an integrity check of software, firmware, and information at startup or d ring security-relevant events.
33	Design he [spacecraft] shall enter a cyber-safe mode when conditions that threaten the platform are detected enters a cyber-safe mode of operation with restr

Summary / Conclusion

The Tiered SPARTA Countermeasure Model

- Tiered SPARTA CM Model transforms SPARTA into a better decision-making tool
- Security becomes scalable, measurable, and mission-driven
  - Threat-informed prioritization
  - Commensurate security investment aligned to mission risk
  - Differentiation between foundational, enhanced, and advanced resilience controls
  - Sample acquisition language tied to threat coverage and mission impact
- How to Use It in Practice
  - Assess adversary capability, mission criticality, and operational environment.
  - Select CM Tier appropriate for mission
    - Tier 1: Foundational mission assurance
    - Tier 2: Elevated threat environment
    - Tier 3: Contested / high-value mission
  - Integrate into the Lifecycle during requirements definition, architecture design, trade studies, verification & validation
  - Reassess Over Time
    - Adjust tiers as threat posture, mission phase, or risk tolerance changes.

The tiered model enables structured, transparent, and risk-aligned cybersecurity decisions across the mission ensuring engineering effort is focused where it provides the greatest mission impact.