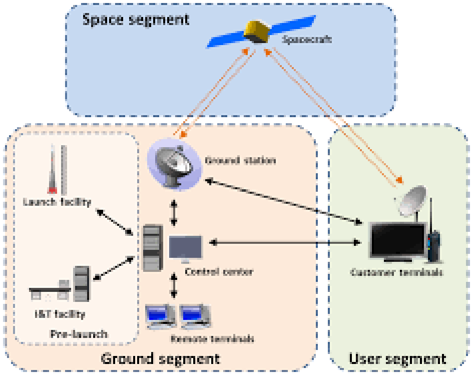
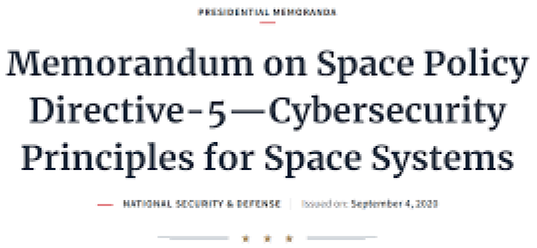
AI AIDED DESIGN AND DEVELOPMENT FOR SPACE SYSTEMS

Michael Orosz, PhD[1]
Alefiya Hussain, PhD[1]
Robert Lai, PhD[2]
[1]USC Information Sciences Institute
[2]Aerospace Corporation

What Are We Trying to Do and Why

- Over the last decade, the threat landscape has evolved and the space domain is being targeted by adversaries using cyber means
- There is a strong need to design and protect against cyber threats with space system design to determine minimizing risk areas and then adding cybersecurity requirements to reduce cyber risk
- Wide range of expertise involved in design and development of space systems (SV, payloads..)
- Various levels types of entities with diverse set of resources (e.g., commercial, government, university)
- Cybersecurity risk assessments and awareness needs to start from the early phases of system development.
- But it also spans the whole development lifecycle through operations and sustainment



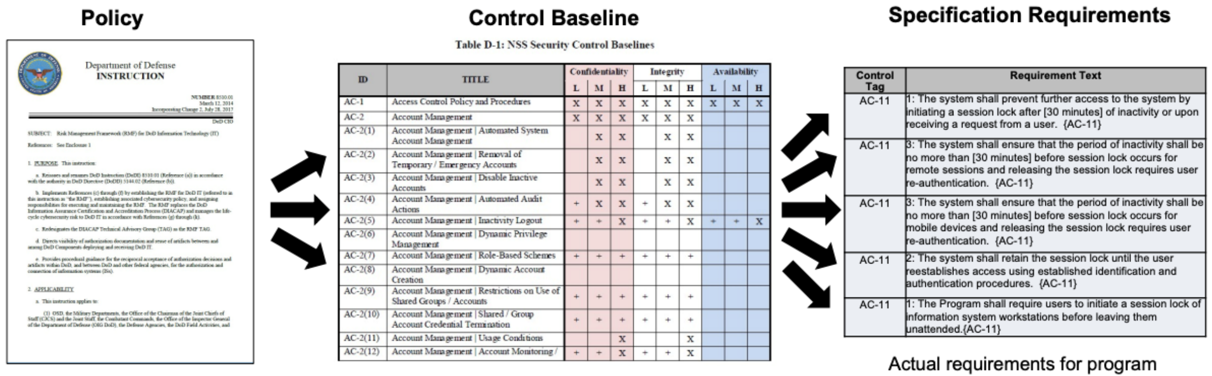


PRESIDENTIAL MEMORANDA

Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems

NATIONAL SECURITY & DEFENSE | Issued on: September 4, 2020

Compliance-Driven Spacecraft Development Initiatives



Policy

Department of Defense
INSTRUCTION

NUMBER 8510.01
March 12, 2014
Incorporating Change 2, July 28, 2017

DoD CIO

SUBJECT: Risk Management Framework (RMF) for DoD Information Technology (IT)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues and renames DoD Instruction (DoDI) 8510.01 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Implements References (c) through (f) by establishing the RMF for DoD IT (referred to in this instruction as "the RMF"), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT in accordance with References (g) through (k).

c. Redesignates the DIACAP Technical Advisory Group (TAG) as the RMF TAG.

d. Directs visibility of authorization documentation and reuse of artifacts between and among DoD Components deploying and receiving DoD IT.

e. Provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other federal agencies, for the authorization and connection of information systems (ISs).

2. APPLICABILITY

a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (OIG DoD), the Defense Agencies, the DoD Field Activities, and

"Program shall implement cybersecurity through RMF as directed in DoD 8510.01"

Control Baseline

Table D-1: NSS Security Control Baselines

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout	+	+	X	+	+	X	+	+	X
AC-2(6)	Account Management | Dynamic Privilege Management									
AC-2(7)	Account Management | Role-Based Schemes	+	+	+	+	+	+			
AC-2(8)	Account Management | Dynamic Account Creation									
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	+	+	+	+	+	+			
AC-2(10)	Account Management | Shared / Group Account Credential Termination	+	+	+	+	+	+			
AC-2(11)	Account Management | Usage Conditions			X			X			
AC-2(12)	Account Management | Account Monitoring /	+	+	X	+	+	X			

"Program shall implement CNSSI 1253 Moderate control baseline."

Specification Requirements

Control Tag	Requirement Text
AC-11	1: The system shall prevent further access to the system by initiating a session lock after [30 minutes] of inactivity or upon receiving a request from a user. {AC-11}
AC-11	3: The system shall ensure that the period of inactivity shall be no more than [30 minutes] before session lock occurs for remote sessions and releasing the session lock requires user re-authentication. {AC-11}
AC-11	3: The system shall ensure that the period of inactivity shall be no more than [30 minutes] before session lock occurs for mobile devices and releasing the session lock requires user re-authentication. {AC-11}
AC-11	2: The system shall retain the session lock until the user reestablishes access using established identification and authentication procedures. {AC-11}
AC-11	1: The Program shall require users to initiate a session lock of information system workstations before leaving them unattended.{AC-11}

Actual requirements for program design, development, and testing

https://aerospace.org/paper/cybersecurity-protections-spacecraft-threat-based-approach

- Step 1: A policy document (e.g., DODI 8510.01, NASA NPD 2810, NASA NPD 1000.0) which describes a high-level security strategy
- Step 2: Which then points to an overarching risk management framework (RMF) process (e.g., CNSSI 1253, NASA NPR 2810, NASA NPR 7150.2E) which specifies a "control baseline" using the Low-Moderate-High watermark approach.
  - The control baseline with high-level guidelines is usually where the guidance stops.
- Step 3: These baseline controls need to be translated by a system designer to decompose what the control baselines text means into implementable technical requirements.

A Diverse Team for Space System Design

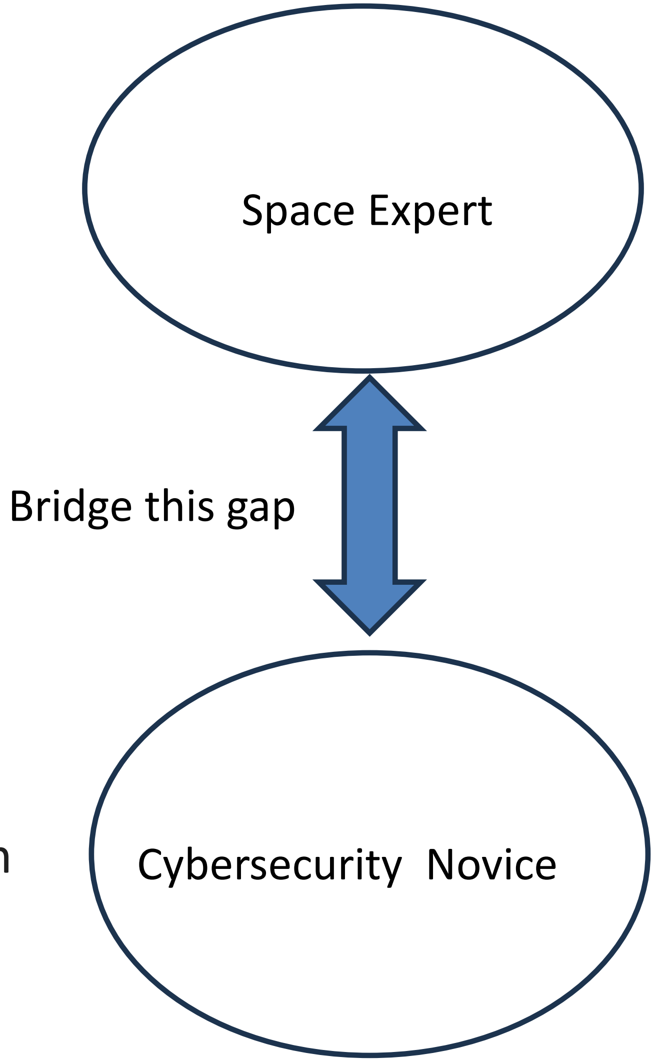
Designing a space system involves a collaborative effort from various professionals with specialized expertise.

- ***Engineers***
  - Systems Engineers, Aerospace Engineers, Electrical Engineers, Mechanical Engineers, Software Engineers
- ***Scientists***
  - Astrophysicists, Planetary Scientists, Computer Scientists
- ***Other Professionals***
  - Mission Managers, Project Managers, Safety Engineers, Procurement Specialists

The specific roles and responsibilities may vary depending on the nature of the space system and the organization involved. However, a successful space system design requires a multidisciplinary team

The Challenge: ***A cybersecurity expert is typically missing from the team***

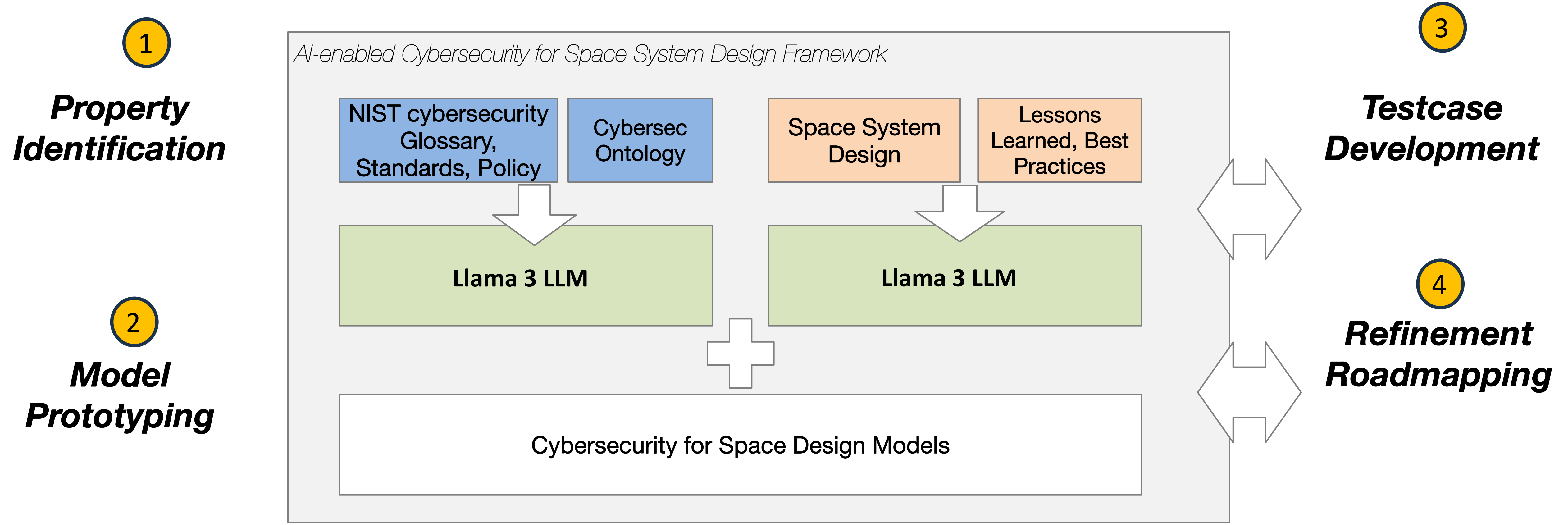
Second Challenge: *The cyber attack environment is dynamic*



Initial Research Effort

- Long-term goal is to create a system that addresses the complete space system design lifecycle.
- Initial step: Explore using AI to analyze different design options and suggest configurations that are inherently more secure and meet SPD-5 requirements.
  - Research question: Can an LLM be trained to identify if necessary cyber security controls are present in a space system design?
- Test Environment
  - We selected the Llama 3 LLM as this is a well understood LLM with extensive research support
  - Implemented on the USC/ISI GPU Éclair cluster.

Provided AI-based Guidance during the Space System Design



1
Property Identification
2
Model Prototyping
AI-enabled Cybersecurity for Space System Design Framework
NIST cybersecurity Glossary, Standards, Policy
Cybersec Ontology
Space System Design
Lessons Learned, Best Practices
Llama 3 LLM
Llama 3 LLM
Cybersecurity for Space Design Models
3
Testcase Development
4
Refinement Roadmapping

Cybersecurity for Space Design

- RAG (Retrieval-Augmented Generation) a specialized query tool that utilizes LLMs to retrieve information from a “knowledge” base.
- We will use RAG to query the trained LLM to ask the AI the following questions regarding an existing space system design.

Increasing level of cybersecurity and space SME expertise

Level 1: What does scanning mean?

Level 2: What are the relevant controls to prevent scanning (NIST 800-53 with space overlay, CNSSI 1253)
What are attacks related to scanning? (SPARTA Attacks)

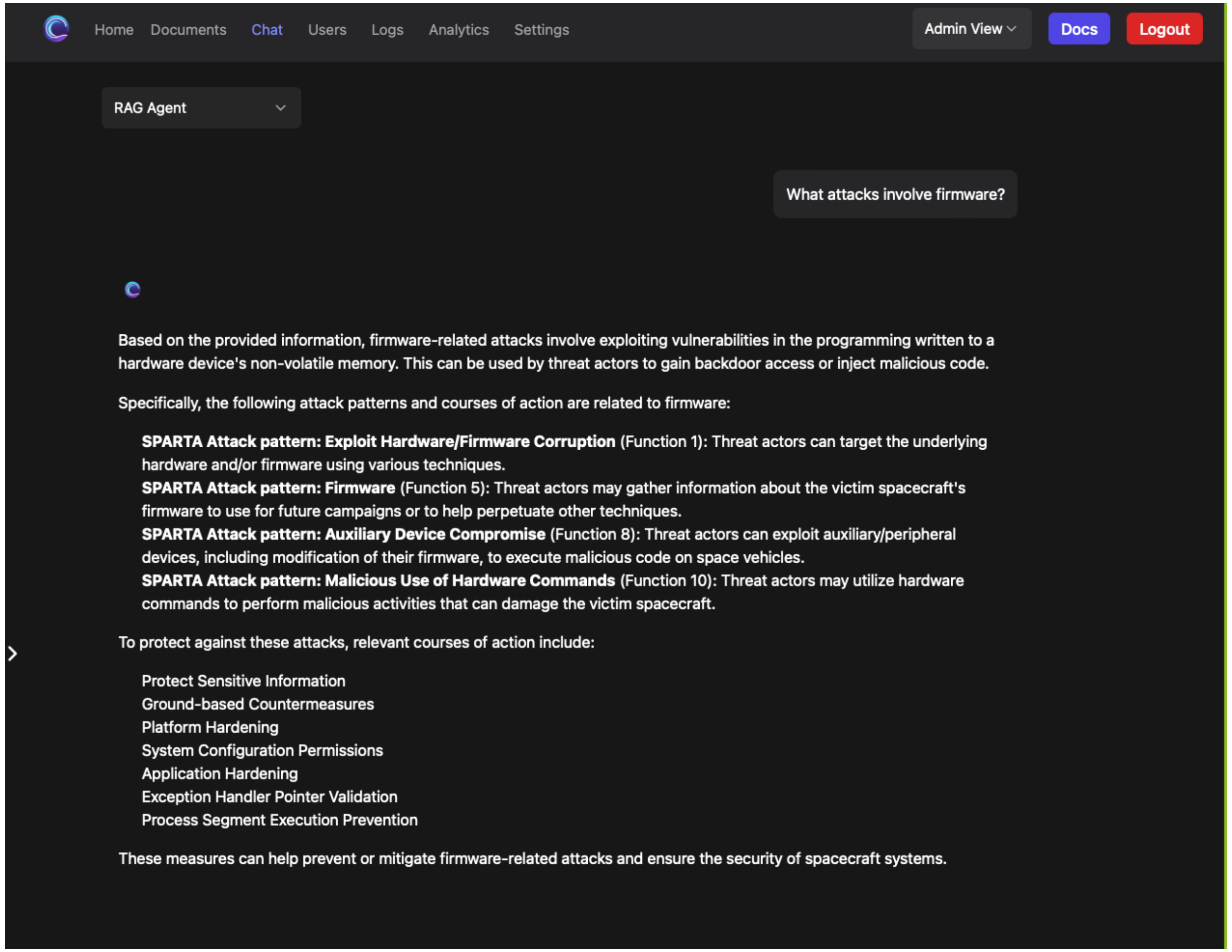
Level 3: Which controls are most relevant to the SPARTA exfiltration TTP?

Level 4: Is SC-5 applicable for this SV design?

Level 5: Which controls are needed to meet the cybersecurity requirements in this design?

Current Status

- Have trained the LLM to recognize/understand an initial set of cybersecurity policies and controls (e.g., SPARTA) and space systems design.
- Duplicates what we would expect to see from current state-of-the-art such as OpenAI/Google Gemini.
- For example, "What attacks involve firmware?"



What attacks involve firmware?

Based on the provided information, firmware-related attacks involve exploiting vulnerabilities in the programming written to a hardware device's non-volatile memory. This can be used by threat actors to gain backdoor access or inject malicious code.

Specifically, the following attack patterns and courses of action are related to firmware:

SPARTA Attack pattern: Exploit Hardware/Firmware Corruption (Function 1): Threat actors can target the underlying hardware and/or firmware using various techniques.
SPARTA Attack pattern: Firmware (Function 5): Threat actors may gather information about the victim spacecraft's firmware to use for future campaigns or to help perpetuate other techniques.
SPARTA Attack pattern: Auxiliary Device Compromise (Function 8): Threat actors can exploit auxiliary/peripheral devices, including modification of their firmware, to execute malicious code on space vehicles.
SPARTA Attack pattern: Malicious Use of Hardware Commands (Function 10): Threat actors may utilize hardware commands to perform malicious activities that can damage the victim spacecraft.

To protect against these attacks, relevant courses of action include:

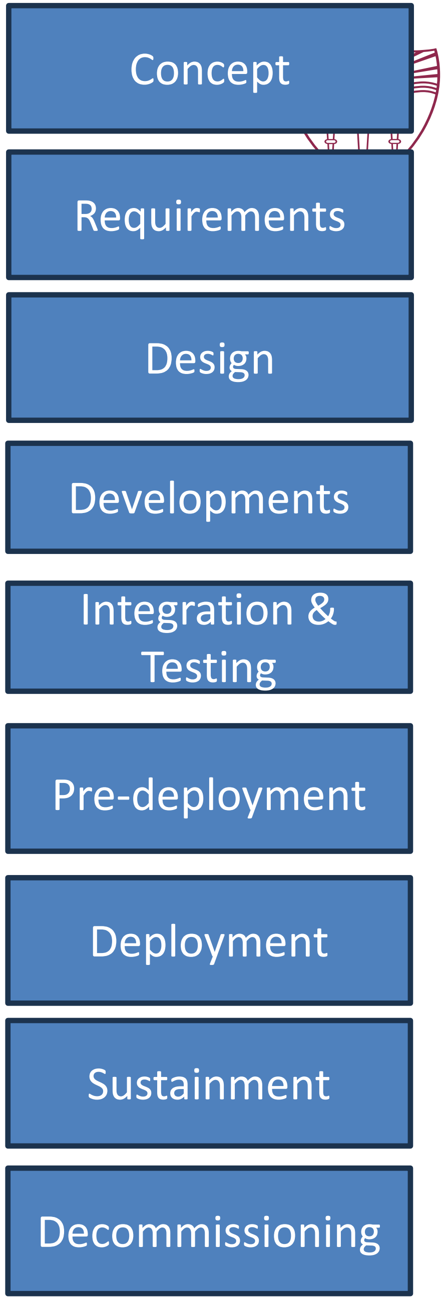
Protect Sensitive Information
Ground-based Countermeasures
Platform Hardening
System Configuration Permissions
Application Hardening
Exception Handler Pointer Validation
Process Segment Execution Prevention

These measures can help prevent or mitigate firmware-related attacks and ensure the security of spacecraft systems.

Cybersecurity in the Lifecycle of Space System Development

Compliance with policy and the risk management framework (RMF) at every stage of the system lifecycle

Current focus



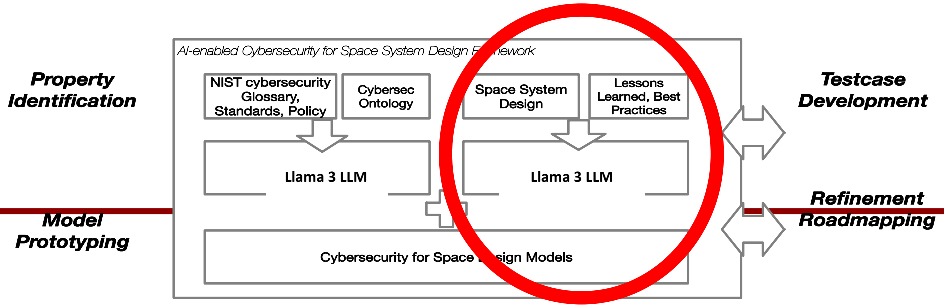
Steps applied at each step of the lifecycle process

Level 1: Implement testcases to evaluate scanning (what are we looking for?)
Level 2: Implement testcases to evaluate attacks related to scanning (SPARTA Attacks)
Level 3: Define tests to evaluate conformance for a set of controls
Level 4: Define conditions in which the system fails to meet the controls
Level 5: Analyze how the system complies to a set of cybersecurity control requirements

Waterfall, Agile/DevSecOps or Hybrid

Path Forward

- Complete training and testing of the prototype
- Demonstrate the technology to Aerospace Corporation leadership and interested parties with US Space Force (end of Sept 2024)
  - ***MVP to provide AI-muse to guide cybersecurity compliance at early stages of design.***
- With longer-term funding: Address the full lifecycle
  - Fine-tune based on increasingly complex space system designs
  - Apply to evaluations of systems; testing and evaluations, penetration testing
  - Specialize to different domains: cloud security, critical infrastructure


Property Identification
Model Prototyping
AI-enabled Cybersecurity for Space System Design F ework
NIST cybersecurity Glossary, Standards, Policy
Cybersec Ontology
Space System Design
Lessons Learned, Best Practices
Llama 3 LLM
Llama 3 LLM
Cybersecurity for Space sign Models
Testcase Development
Refinement Roadmapping

Thank You

Mike Orosz

mdorosz@isi.edu