An Introduction to Space Cyber

New Mexico Tech
2024 Space Cyber Resiliency Lecture Series

Joseph “Dan” Trujillo- AFRL

AFRL Space Cyber Resiliency(SCR) Tech Lead

Oct 2024

A bit about myself

Over 30 years working for Commercial and DoD

Air Force Research Labs (AFRL) Space Cyber Resiliency Lead

Microsoft, Disney, other commercial companies as a software developer, Lead, and Architect in DFW area

Hughes Aircraft, Lockheed Martin in Engineering roles

B.S. Science Aerospace Engineering University of Texas at Arlington

Presentation Format

- **Presenting**
- **Open to questions after each slide**
- **Audience discussion**

Overview

Space Cyber Resiliency (SCR) Tech Area, Goals & Challenges

Future Space Architecture and how it drives Cyber R&D

How is Space Cyber different than Terrestrial Cyber?

Vulnerability Assessments

Security & Resiliency Principles

Cyber Robustness

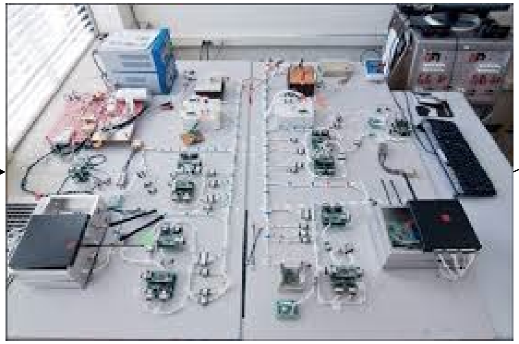
Space Cyber Resiliency (SCR) Tech Area

What is it that we do?

- **Future outlook**
- **Identify, develop, mature, test, evaluate, experiment, and demonstrate**
- **Day to Day**

Ideas, raw tech

Cyber Lab/Range/Testbeds



Flat-Sats

On-Orbit

SCR Goals

GOAL: Develop cyber-robust space systems

OBJECTIVES:

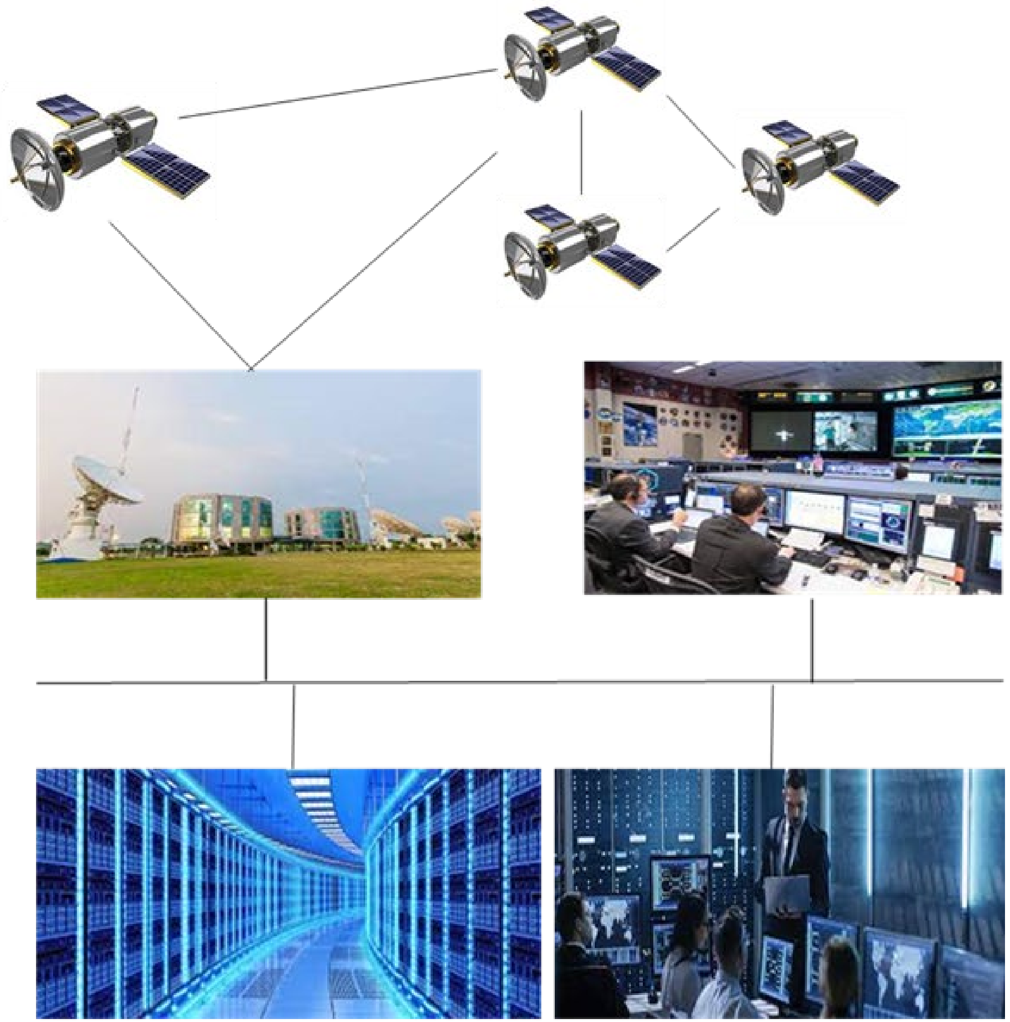
- Enable cyber-secure, resilient architectures & space data transport networks
- Provide expertise & support to Developmental Test & Evaluation and Operational Test & Evaluation operational units
- Inform cyber policy, requirements & champion adoption

What is the Space System?

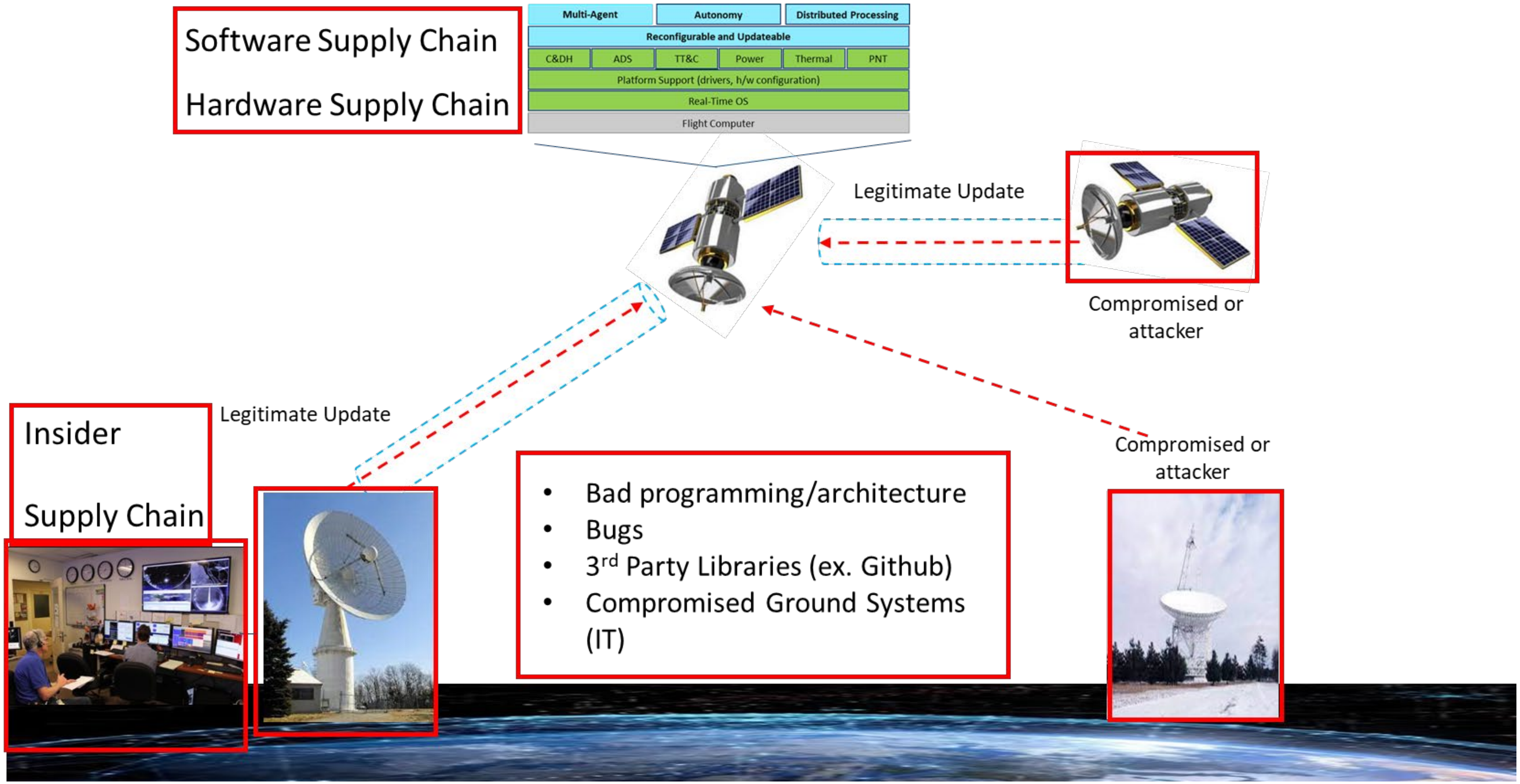
Space Segment
- Space Vehicle
- Constellations
- Networks

Command & Control Segment
- Command centers
- Tracking radar, antenna, optics
- Networks

User Segment
- Data fusion, processing, analytics
- Business
- Networks



Space System Access



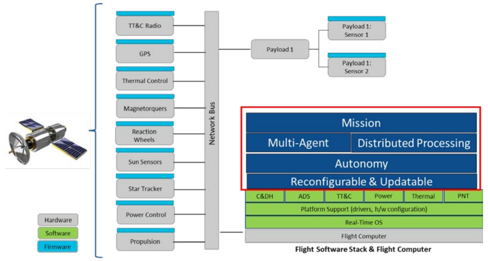
Future Space Architecture & Great Power Competition

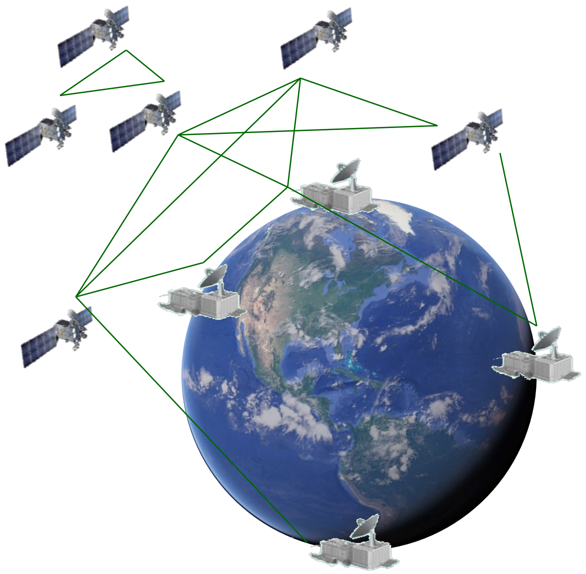
We want to keep our critical satellite systems, C2, and data secure, AND we want to greatly expand operational flexibility through integrated architectures

BUT, this will vastly increase cyber access…

Future Capabilities:

- **Integrated ground & space**
- **Autonomous systems**
- **Multi-Agent/Cooperative missions**
- **Constellations/Networked/Hybrid**
- **Edge processing**
- **Fully reconfigurable missions**
- **Cyber security & resilience**
- **Software-centric**
- **Updatable**





Future

Drivers for Advanced Communication and Sensor-Data Processing Electronics in Future Space Systems

Huge growth in sensor data rates coupled with limited communication bandwidth to ground

DATA RATE (Mb/s) No Compression

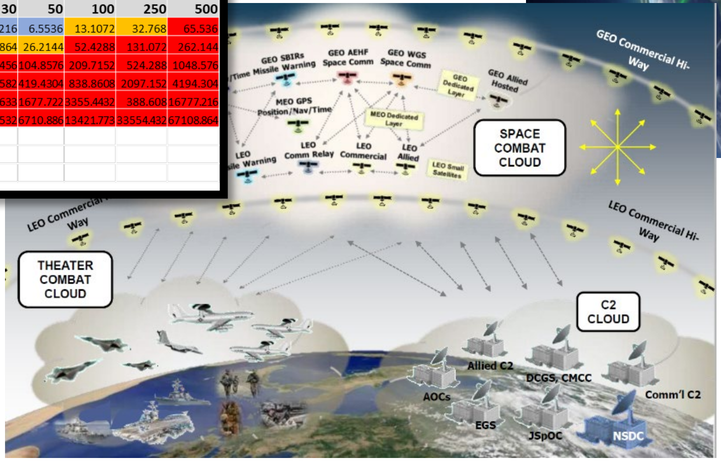
FPA Dimensions (Unit^2)	FRAMES RATE (Frames/s)										
	1	5	10	15	20	25	30	50	100	250	500
256	1.048576	5.24288	10.48576	15.7286	20.97152	26.2144	31.45728	52.4288	104.8576	262.144	524.288
512	4.194304	20.97152	41.94304	62.9145	83.88608	104.8576	125.8291	209.7152	419.4304	1048.576	2097.152
1024	16.777216	83.88608	167.77216	251.65824	335.5443	419.4304	503.3165	838.8608	1677.7216	4194.304	8388.608
2048	67.108864	335.54432	671.08864	1006.63296	1342.177	1677.722	2013.266	3355.443	6710.8864	16777.216	33554.432
4096	268.435456	1342.17728	2684.35456	4026.53184	5368.709	6710.886	8053.064	13421.77	26843.546	67108.864	134217.73
8192	1073.741824	5368.70912	10737.41824	16106.12736	21474.84	26843.55	32212.25	53687.09	107374.18	268435.46	536870.91

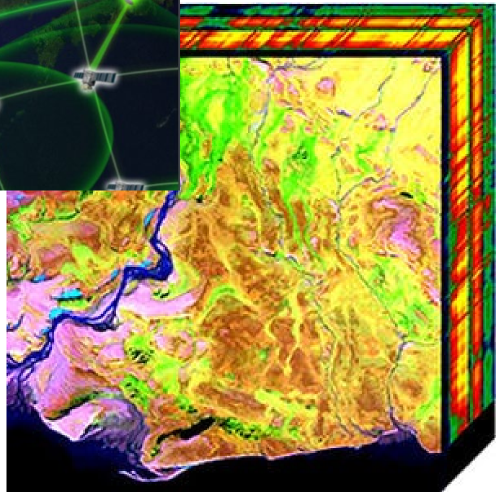
DATA RATE (Mb/s) 8:1 Compression

FPA Dimensions (Unit^2)	FRAMES RATE (Frames/s)										
	1	5	10	15	20	25	30	50	100	250	500
256	0.131072	0.65536	1.31072	1.96608	2.62144	3.2768	3.93216	6.5536	13.1072	32.768	65.536
512	0.524288	2.62144	5.24288	7.86432	10.48576	13.1072	15.72864	26.2144	52.4288	131.072	262.144
1024	2.097152	10.48576	20.97152	31.4572	41.94304	52.4288	62.91456	104.8576	209.7152	524.288	1048.576
2048	8.388608	41.94304	83.88608	125.82912	167.7722	209.7152	251.6582	419.4304	838.8608	2097.152	4194.304
4096	33.554432	167.77216	335.54432	503.31648	671.0886	838.8608	1006.633	1677.722	3355.4432	388.608	16777.216
8192	134.217728	671.08864	1342.17728	2013.26592	2684.355	3355.443	4026.532	6710.886	13421.773	33554.432	67108.864

Bit Depth	16

Proliferated "mega-constellations" at Low Earth Orbit & the pivot to autonomous operations





Space Enterprise Vision driving new tech objectives: Short duration missions with rapid tech refresh, & Multi-domain Combat Cloud

Opportunities to leverage Advanced Data Processing techniques

Audience Discussion

What can you envision Space will look like in the future?

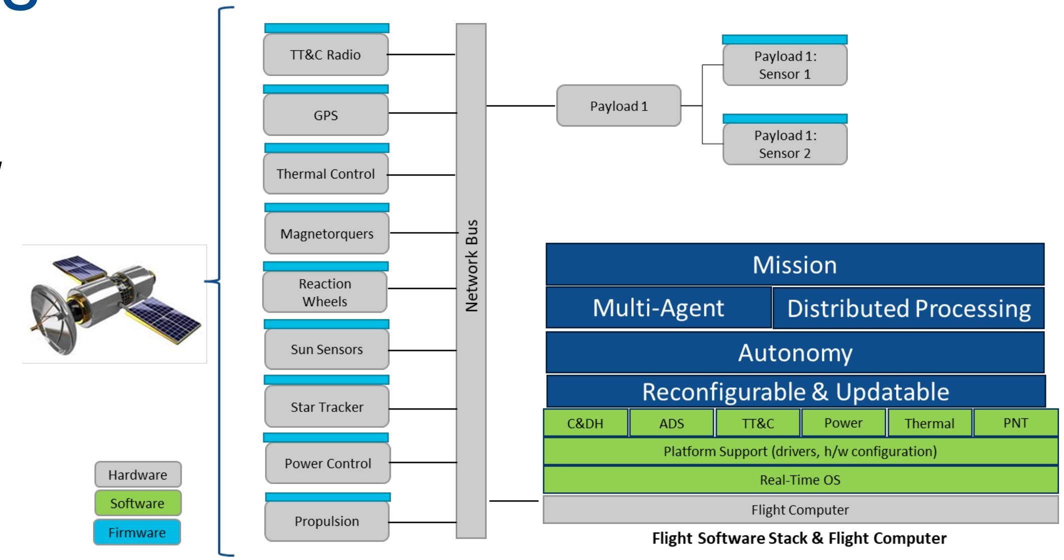
What do you think is different about how cyber effects Space vs Terrestrial Systems?

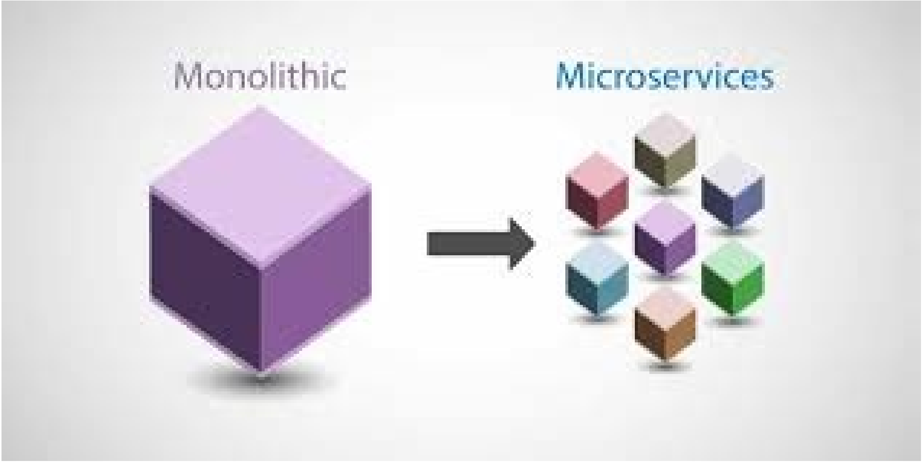
Systems in Space Considerations

- **Space Environment – radiation effects to both hardware and software**
- **Space Vehicle must be self-reliant**
- **Operates in a disconnected state (help desk scenario)**
- **Space Vehicles cannot be taken offline or fixed directly by humans**
- **Space Vehicles serve critical missions but are scarce in numbers. Redundancy for coverage but not cyber**
- **Space domain generally lags behind current industry standards and innovations**

Flight Software for Space Systems

- **FSW is expensive to develop and maintain**
- **Each Space Vehicle bus vendor has unique FSW**
- **SWaP-constrained**
- **Bespoke**
- **Tightly-coupled**
- **Monolithic**
- **Lacking designed-in Cybersecurity**



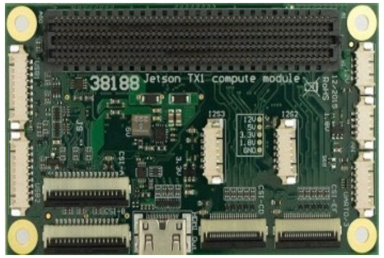


Flight Computers

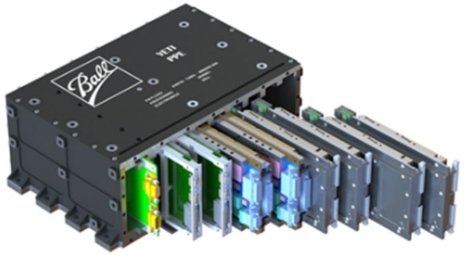
- Space Environment
  - Orbit Regimes (LEO, MEO, GEO, xGEO, deep space)
  - RAD-HARD vs RAD-Tolerant requirements
- Avionics vs Payloads processors
- Options:
  - Harden or shield modern processors
  - Schemas and architectures for resiliency
    - Hardened Avionics/Rad-Tolerant Payloads
    - RAD-HARD watchdogs monitoring, state, and reset Rad-Tolerant (high level functions like Autonomy and cyber detection for example)

RAD 750

RAD 5545



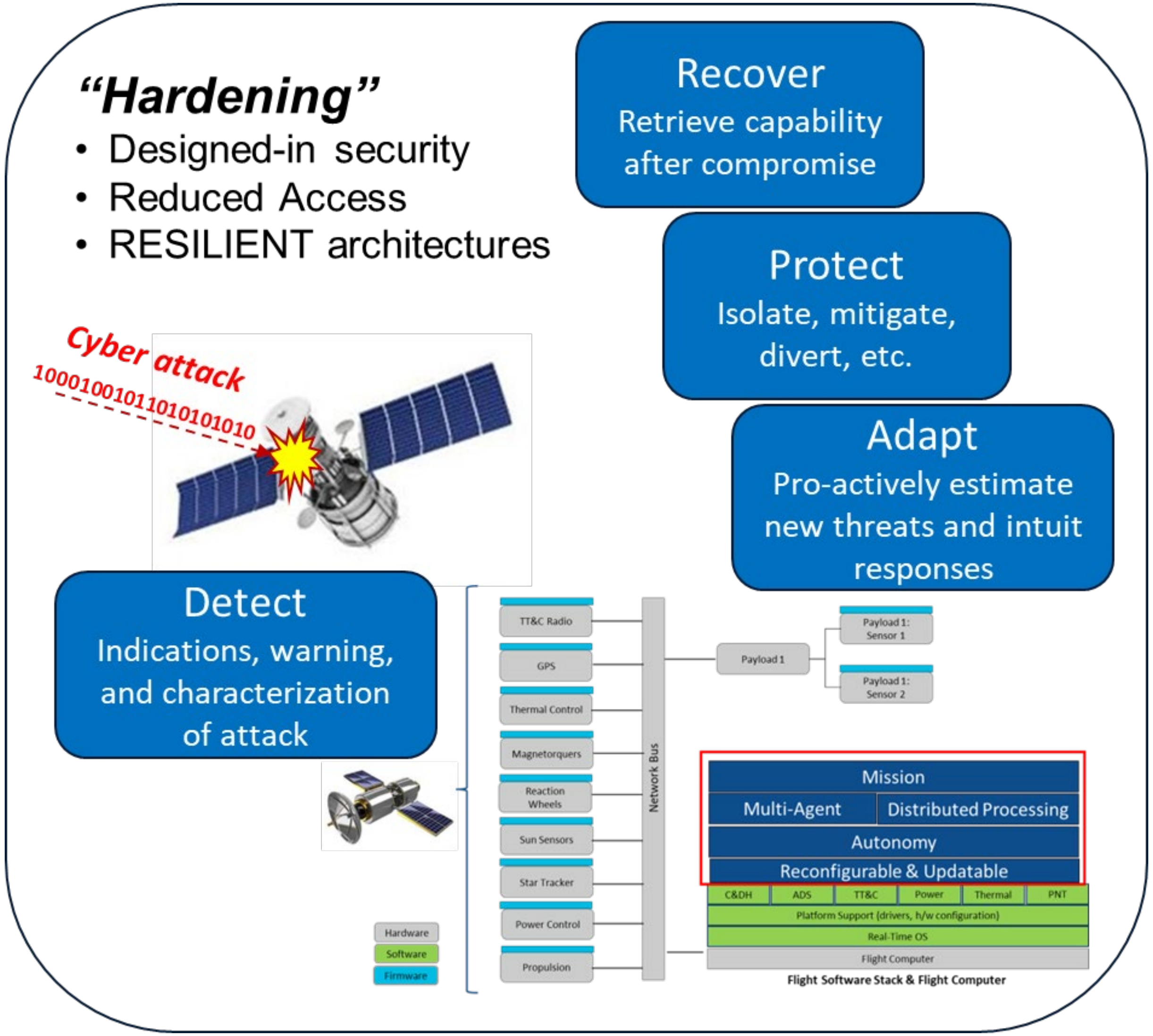
ARM, RISC-V



AFRL -> Heterogeneous On-Orbit Processing Engine (HOPE)

Cyber Robustness

- Hardening
- Detection
- Protection
- Recovery
- Adaptability



Cyber Security vs Resiliency

Security:

Goal -> Hardening -> Reduce access surface, vulnerabilities, and impact

Designed-in -> Detection, Protection, Recovery, and Adaptability

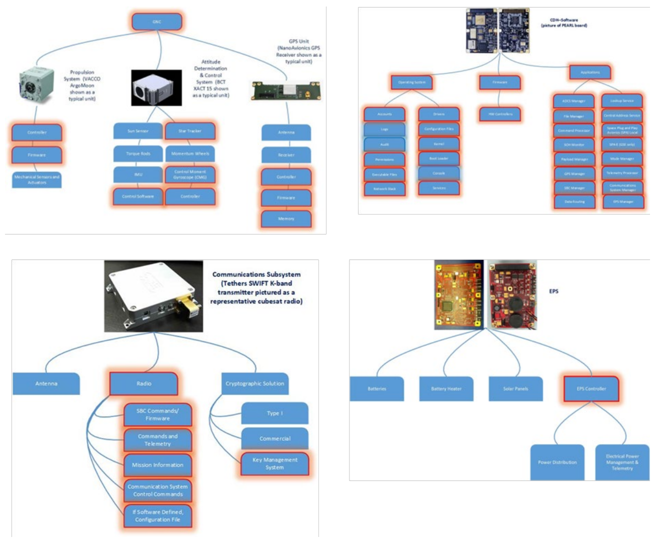
Resiliency:

Goal -> Capacity to recover from comprise

Real-time mechanisms -> Detection, Protection, Recovery, and Adapability

Assume Compromise

Cyber Vulnerability Assessments of Space Systems



- Understand the System
  - Mission, MEFs, Implementation of mission in the form of software, hardware, data, and processes
- Conduct CVA's to understand access points to the system, understand effects of a cyber intrusion and/or attack, understand susceptibilities
- CVA informs -> cyber hardening, detection, protection, recovery, and adaptability mechanisms
- Conduct CVA's on multiple systems to understand common and unique susceptibilities

Chaos Engineering

- Allows not having to address access
- Allows not having to address specific cyber-attacks
- Component by component effects
- Identifies the effects to mission, system, sub-systems, and external systems
  - What damage can the attacker inflict?
  - Where can the attacker pivot?
- Informs on how to address resiliency
  - Detection
  - Protection
  - Recovery
  - Adaptability

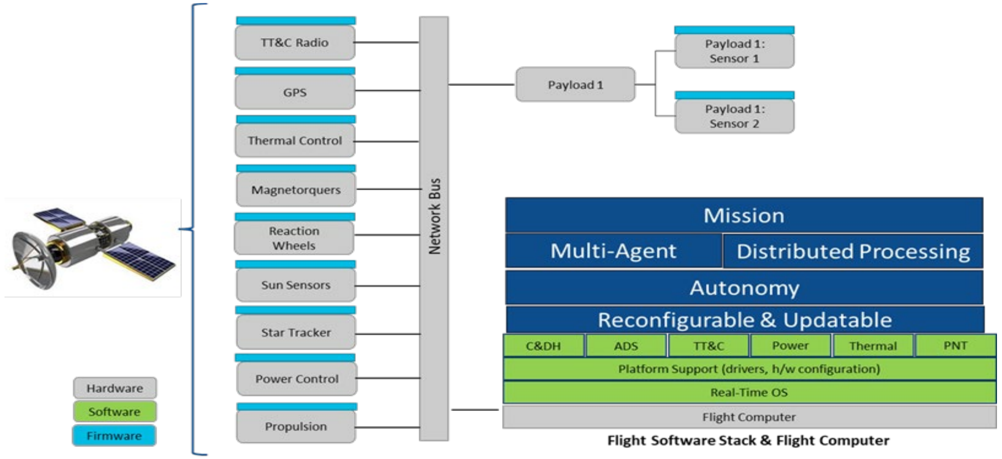
Netflix uses a variety of tools to intentionally cause failures and test their systems' resilience. This includes Chaos Kong, which simulates region outages, Chaos Gorilla, which simulates availability zone failures, and Chaos Monkey, which randomly shuts down servers. These tools help Netflix identify and fix weaknesses in their systems before they become critical problems

Hardening

Goal: Reduce access points (hard for attacker to gain foothold), reduce pivot, reduce vulnerabilities

Implement: Defense-in-Depth, Zero-Trust, and Least Privilege

- Secure layered architectures
- Modular
- Process Isolation
- Authentication and Authorization



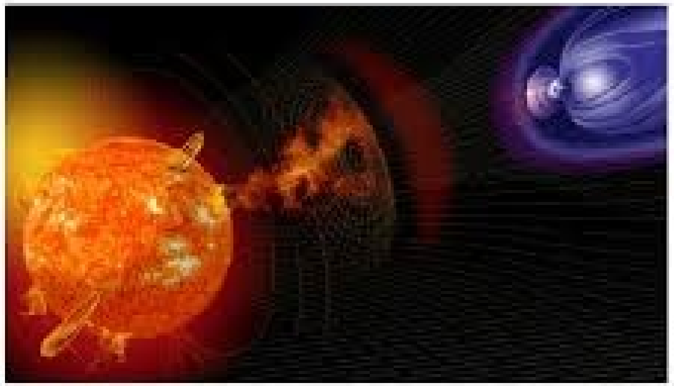
Detection

Goal: Know that system is under cyber-attack

Importance: Informs response

- Off-nominal
- Characterization

- Space weather effects can look like a cyber-attack
  - Sun emissions
- Faults can look like a cyber-attack
  - Normal wear and tear
  - Space environment



Protection

Goal: To stop or reduce the impact of a cyber-attack

Importance: Mission capability available in a cyber-contested environment

- Stop pivot
- Fool the attacker
- Diversification (homogenous vs heterogenous)
- Sensor – trip wires

Recovery

Goal: Meet mission requirements and timelines

Importance: Mission capability when needed

- Step-by-Step process (human, autonomous, both?)
- Identifying compromised component
- Updating a compromised component
- Restarting component
- Determine timelines for mission recovery

Adaptability

Goal: Proactively predict the next set of cyber-attacks

Importance: System secure and resilient to future cyber-attacks

- Cyber attacks constantly changing
- Possible to learn from previous cyber-attacks?
- Possible to update system (detect, protect, recover, and adapt)?
- Model human immune system?

Audience Discussion

Considering on-orbit space vehicles, how can those systems stay ahead of the ever changing cyber threat?

Next Time: Introduction to Space Vehicle Constellation Cyber Security