JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Critical Challenges in the Cyber Domain

DigiMariner 11/18/2020

Zachary Birnbaum, PhD
Chief Scientist – Resilient Military Systems Group
Johns Hopkins University Applied Physical Laboratory
Zachary.Birnbaum@jhuapl.edu
240-228-6067

Outline

- Organization introduction
  - Johns Hopkins University Applied Physics Laboratory
  - Resilient Military Systems Group
- Our Cyber Problem
- Approach to solving our cyber problem
  - Engineering Methods
  - Quantitative Analysis
  - Gap Identification and Solutions Development

JHU/APL in Brief

What are we?

Division of Johns Hopkins University

University Affiliated Research Center

Who are we?

Technically skilled and operationally oriented

Objective and independent

Who are our sponsors?

DoD, NASA, DHS, IC

What is our purpose?

Critical contributions to critical challenges

Laboratory Statistics: ~6,000 staff employed, ~$1.3B in revenues

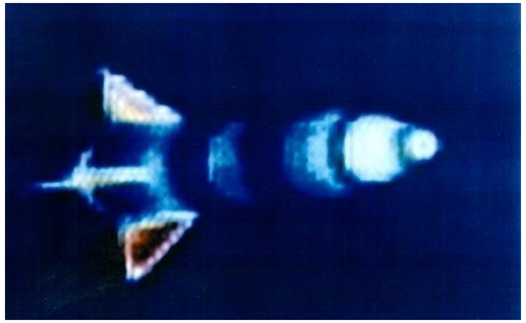
Core Competencies

Strategic Systems Test
& Evaluation

Submarine Security
& Survivability

Space Science
& Engineering

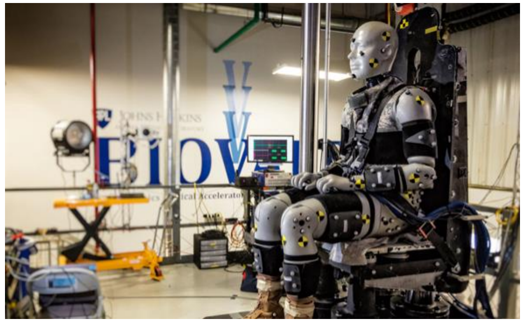
Combat Systems
& Guided Missiles



Theater Air Defense
& Power Projection

Information Technology
(C4ISR/IO)

Simulation, Modeling,
& Operations Analysis



Mission-Related Research
& Development

Group Identity

WE DESIGN CAPABILITIES FOR MILITARY SYSTEMS' ROBUSTNESS AND MISSION RESILIENCE IN HOSTILE CYBER ENVIRONMENTS

RESILIENT MILITARY SYSTEMS GROUP

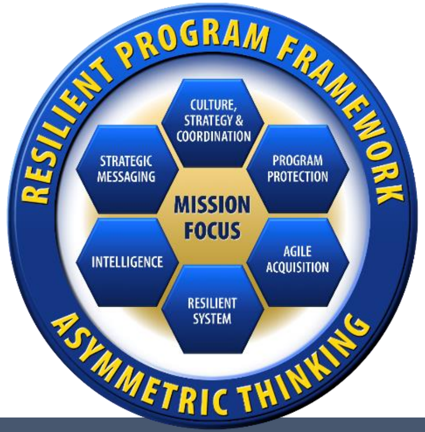
- Core Capabilities

__Cyber solutions__ prototyped and matured for operations upon __representative__ weapon systems development __environments__

__Aggressive experimentation__ on complex hardware and software systems with __emergent behavior__

Next-gen Operational Solutions

Resilient Architectures



RESILIENT PROGRAM FRAMEWORK

CULTURE, STRATEGY & COORDINATION

STRATEGIC MESSAGING

PROGRAM PROTECTION

MISSION FOCUS

INTELLIGENCE

AGILE ACQUISITION

RESILIENT SYSTEM

ASYMMETRIC THINKING

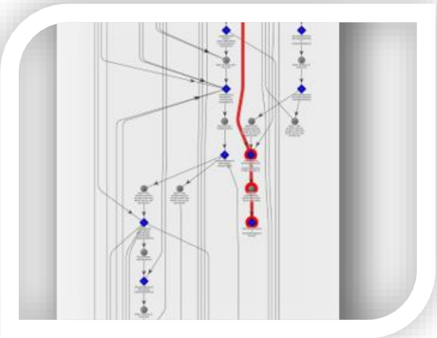
Fault-tolerant __design patterns and capabilities__ for full-lifecycle resilience—for the __program__ and the __system__

__Architecture & design analyses__ cutting across missions, programs, and systems

Simulation & Analytics

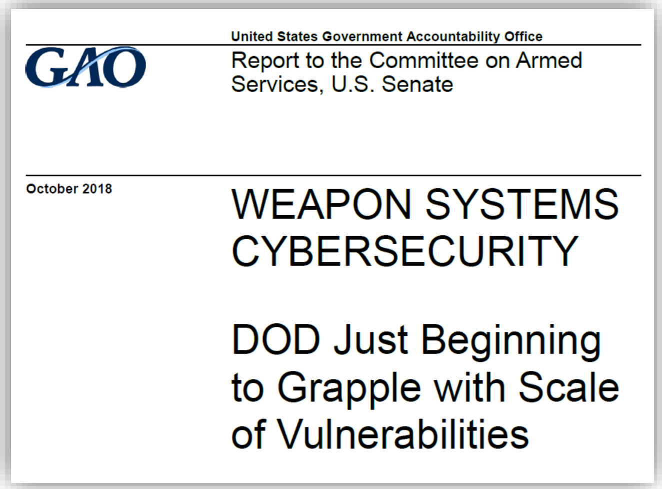
__Quantitative__ cyber analytic __toolkit__ with innovative methods, analytics, and algorithms to enable model-based engineering

Cutting-edge analytics for evaluations throughout __engineering__, __acquisitions__, and __operations__



ENGINEERING FOR SYSTEM ROBUSTNESS AND MISSION RESILIENCE

Our Critical Challenge



GAO

United States Government Accountability Office

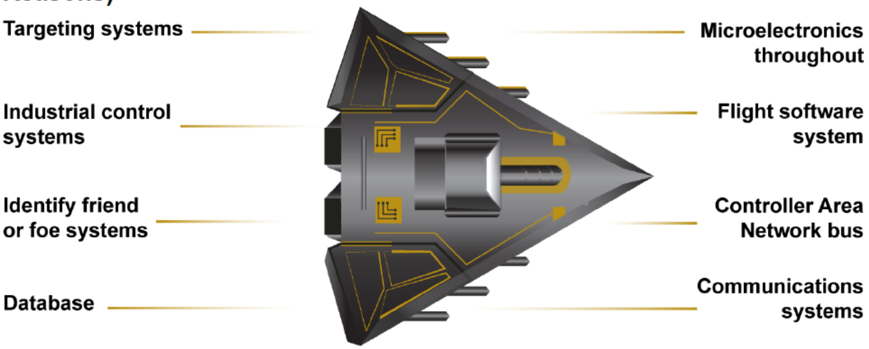
Report to the Committee on Armed Services, U.S. Senate

October 2018

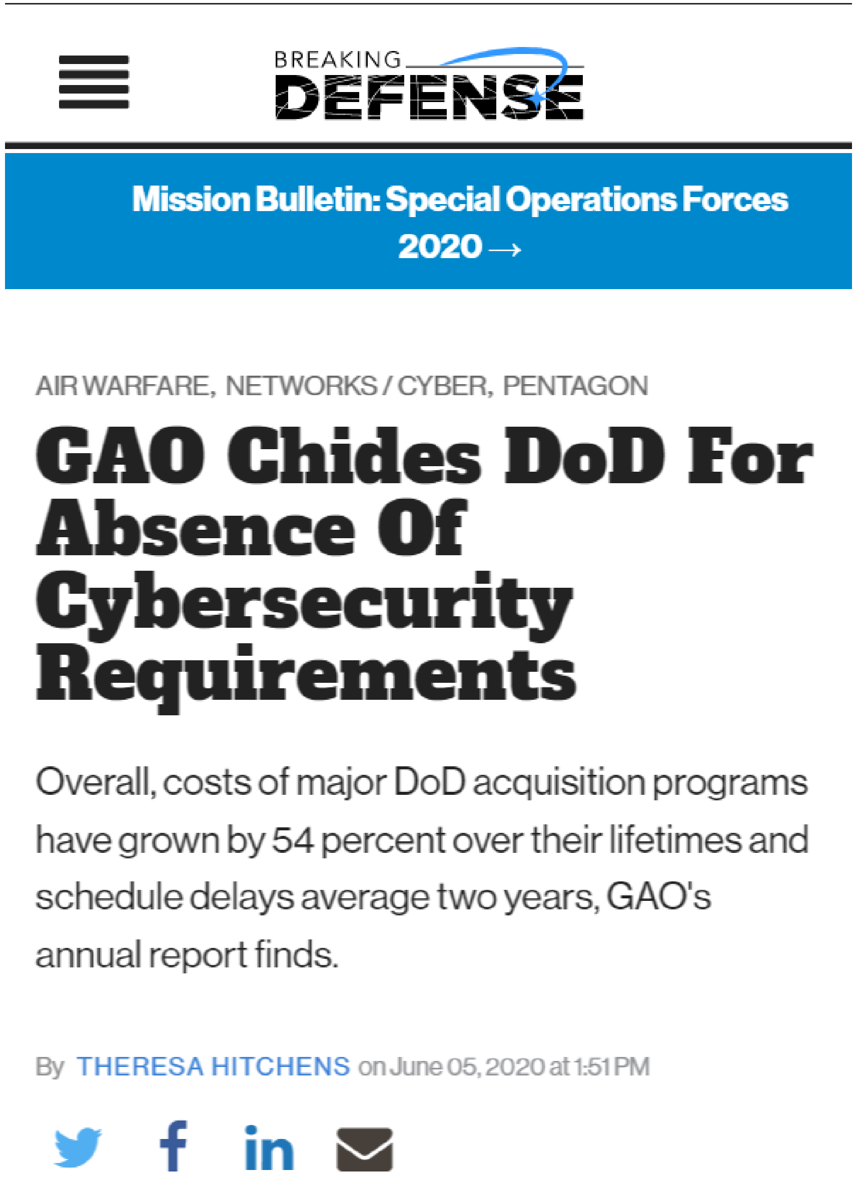
WEAPON SYSTEMS CYBERSECURITY

DOD Just Beginning to Grapple with Scale of Vulnerabilities

Embedded Software and Information Technology Systems Are Pervasive in Weapon Systems (Represented via Fictitious Weapon System for Classification Reasons)


Targeting systems
Industrial control systems
Identify friend or foe systems
Database
Microelectronics throughout
Flight software system
Controller Area Network bus
Communications systems

Source: GAO analysis of Department of Defense information. | GAO-19-128



BREAKING DEFENSE

Mission Bulletin: Special Operations Forces 2020 →

AIR WARFARE, NETWORKS / CYBER, PENTAGON

GAO Chides DoD For Absence Of Cybersecurity Requirements

Overall, costs of major DoD acquisition programs have grown by 54 percent over their lifetimes and schedule delays average two years, GAO's annual report finds.

By THERESA HITCHENS on June 05, 2020 at 1:51 PM

Defense Science Board Adversary Threat Tiers

Tier	Description
I	Practitioners who rely on other to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).
II	Practitioners with a greater depth of experience, with the ability to develop their own tools (from publicly known vulnerabilities).
III	Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
IV	Criminal or state actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits.
V	State actors who create vulnerabilities through an active program to “influence” commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
VI	States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.

Our Cyber Problem – Tier 6 Adversary Defeat

- To defeat the Tier VI adversary we must build systems that are resilient to unknown adversary capabilities against yet unknown cyberspace susceptibilities in the system
- Tier VI adversaries have technical talent, freedom of action, domain control, unlimited budget, guided by national interests
- Current Cybersecurity Requirements are insufficient
  - FISMA – PUBLIC LAW 107–347—DEC. 17 2002 , SEC. 301.
  - FIPS 200 - **Minimum Security Requirements**
  - NIST SP 800-37 – Risk Management Framework
    - “Controls are selected and implemented by the organization in order to satisfy the system requirements.” – pg. 19

Novel Cyber Engineering Method

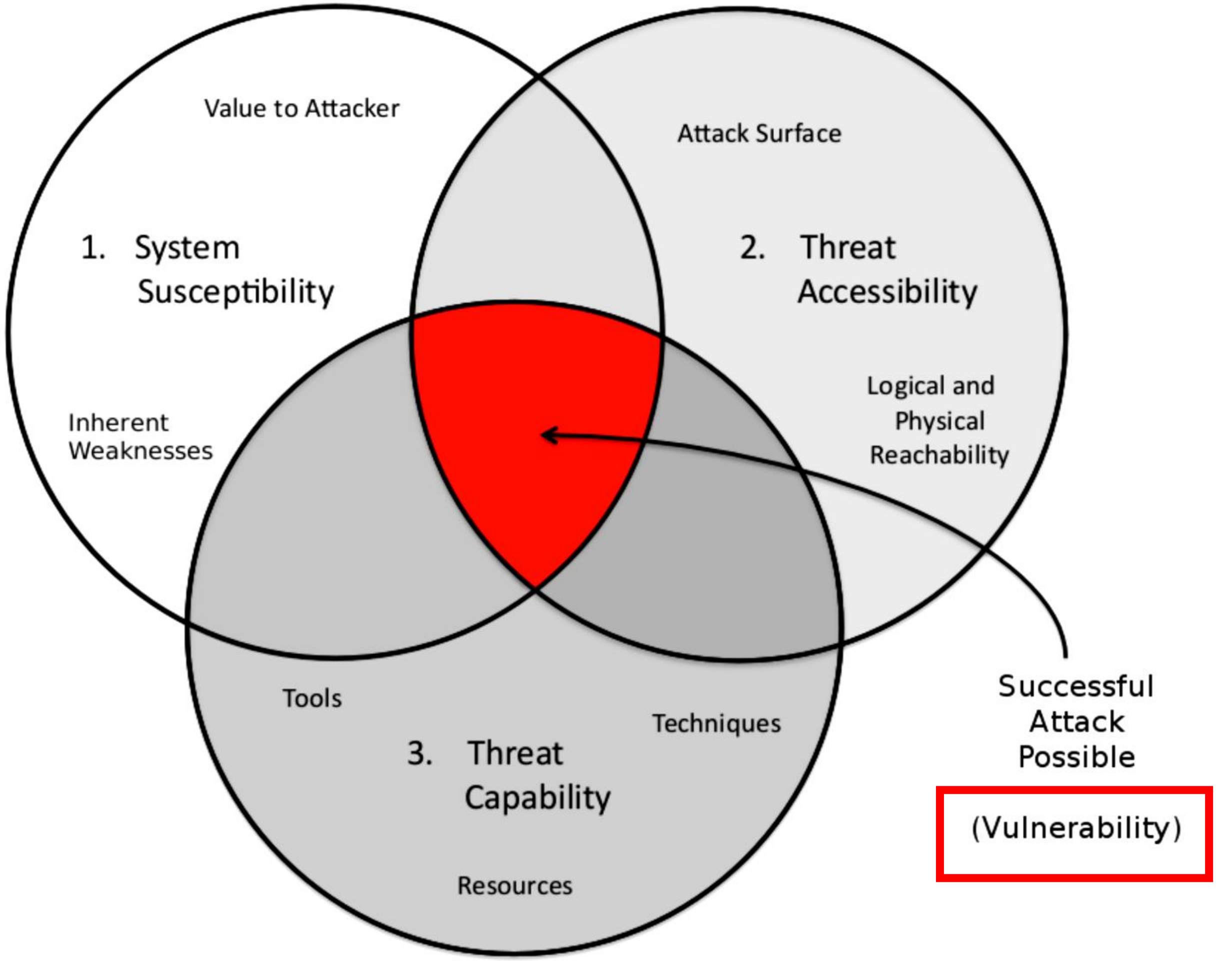
- Focus on mission success (not cybersecurity success)
- Focus on weak link in adversary cyber kill chain
- Goal - threat capability and system susceptibility independent for resilience against 0-day attacks
  - Increase adversary cost

- Threat definition > Requirements derivation > Sound systems engineering process
  - “Resilient to what?”

- Three Tenets for Secure Cyber-Physical System Design and Assessment - Jeff Hughes, George Cybenko, 2005
  - Basis for DoD Anti-Tamper program; Applicable to Cybersecurity
- **Risk model – all three elements must co-exist for a successful attack:**
  - Threat Capability
  - System Susceptibility
  - **Threat Accessibility**

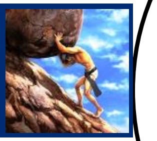
According to CNSSI No. 4009 a vulnerability is a: “Weakness in an information system, system security procedures, internal controls, or implementation **that could be exploited by a threat source.”**

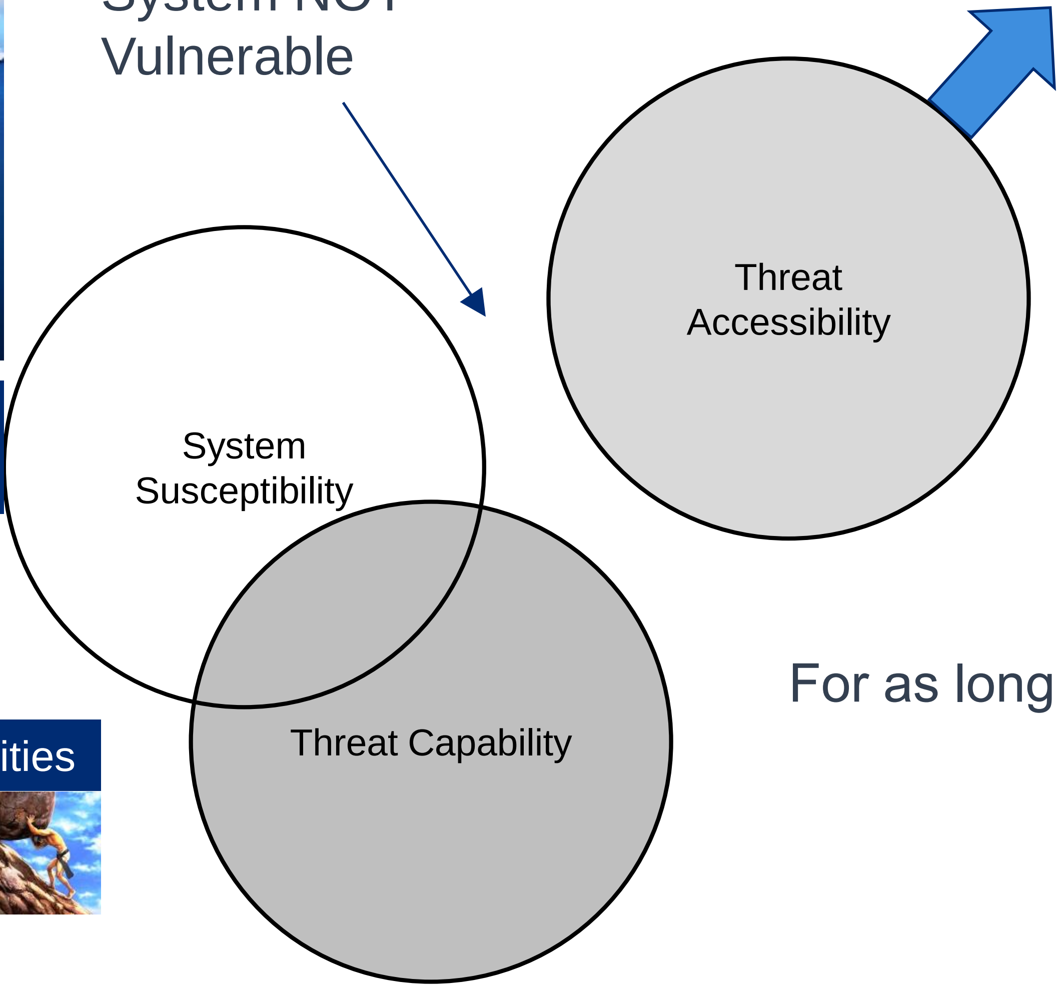
For a **threat source** to be able **to exploit** a weakness in an information system (susceptibility), **they must have** a capability **and access**.



A vulnerability only exists when these three elements are concurrently true

Endless cycle of system susceptibility discovery





System NOT Vulnerable

Can control access by design

For as long as the condition holds…

Cannot control threat capabilities

Tactical Systems have tremendous home field advantage…

Increasing Adversary Cost

Supply Chain

- Software
- Hardware

Data connection

- Networked connection
- RF
- Removable media
- Side / covert channel

Direct Access

- Insider Threat
- Burglar

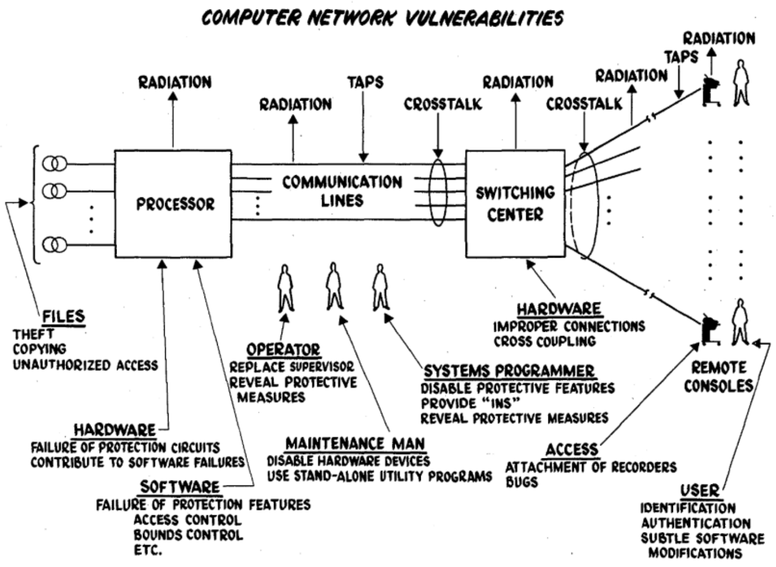


Figure 3

Security Controls for Computer Systems (U)
Report of Defense Science Board
Task Force on Computer Security
11 February 1970

Force the Tier VI adversary to pursue costly, time consuming vectors

Drive Adversaries from here… …to here

Data Connection — Supply Chain (Lot) — Supply Chain (Single Item) — Direct Access

Bad for the defender… …better for the defender

Tools and Analytics

- Methods, processes, and tools used to determine satisfiability of requirements providing answers to cyber centric analytic questions
- Historically, cyber analysis (e.g., risk) approaches have been
  - Labor intensive
  - Highly qualitative
  - Compliance-oriented
  - As much art as science
- Challenges
  - Repeatability, reproducibility
  - Coverage / completeness
  - Resource intensity (people, cost / time)
  - Data availability
  - Validation

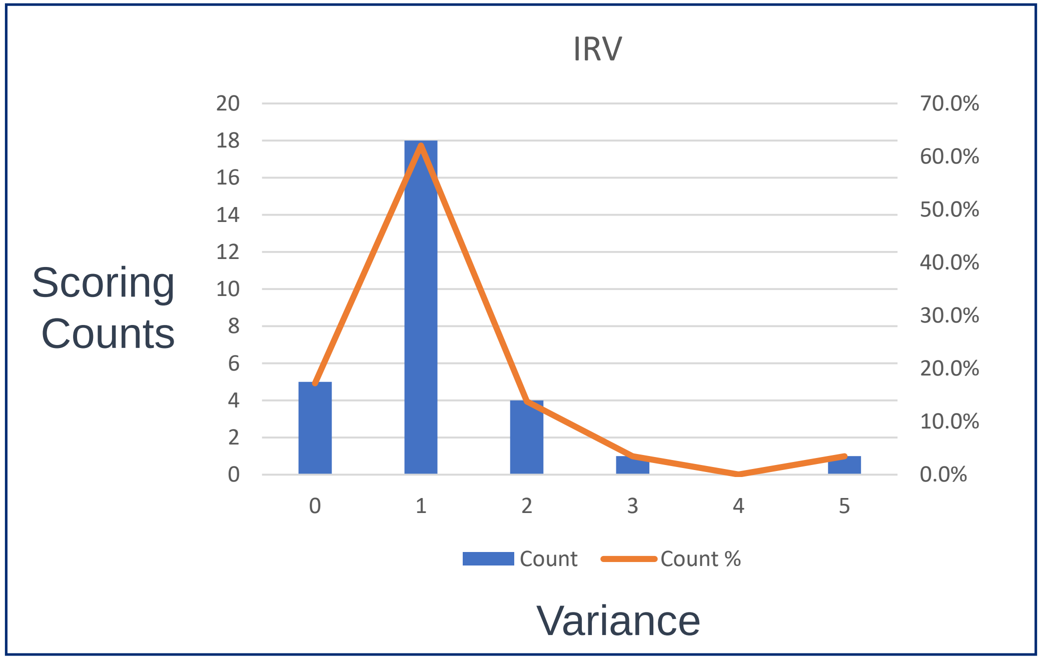
Challenge: Repeatability / Reproducibility

> *“The results indicate that the consensus of the raters is too low for the assessment results to provide a sound basis for decisions. In conclusion, better support is needed for assessing information security risks in order to reach the necessary consensus levels.”*

Hallberg, J., et al., “The Significance of Information Security Risk Assessments – Exploring the Consensus of Raters’ Perceptions of Probability and Severity,” *Int'l Conf. Security and Management, 2017*

Case Study @ APL

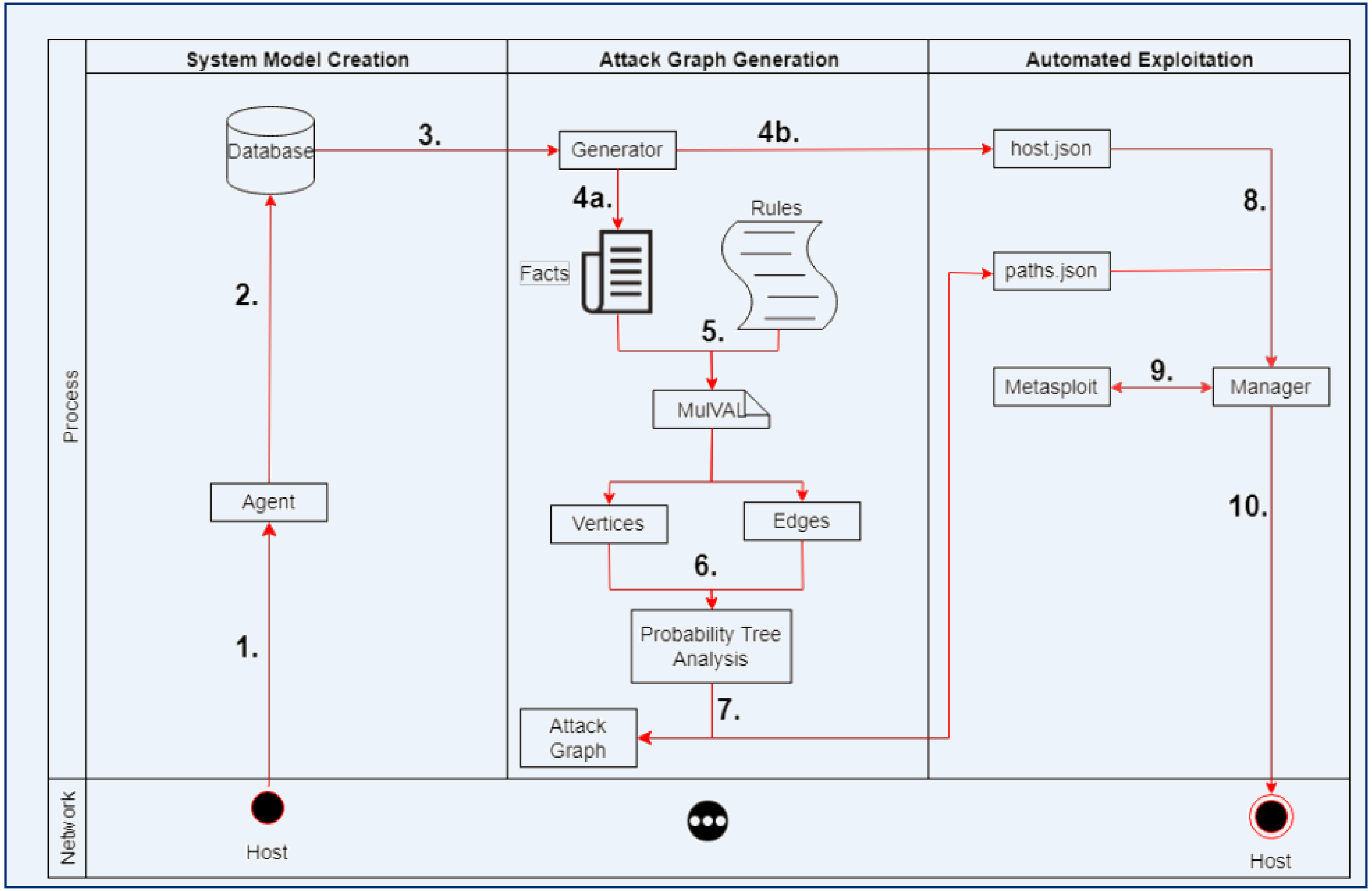
- August 2017
- Two separate teams scoring the same target system for cyber risk
- 5-pt Likert scale
- Results
    - 82% disagreement
    - 20% disagreement > 2 values off



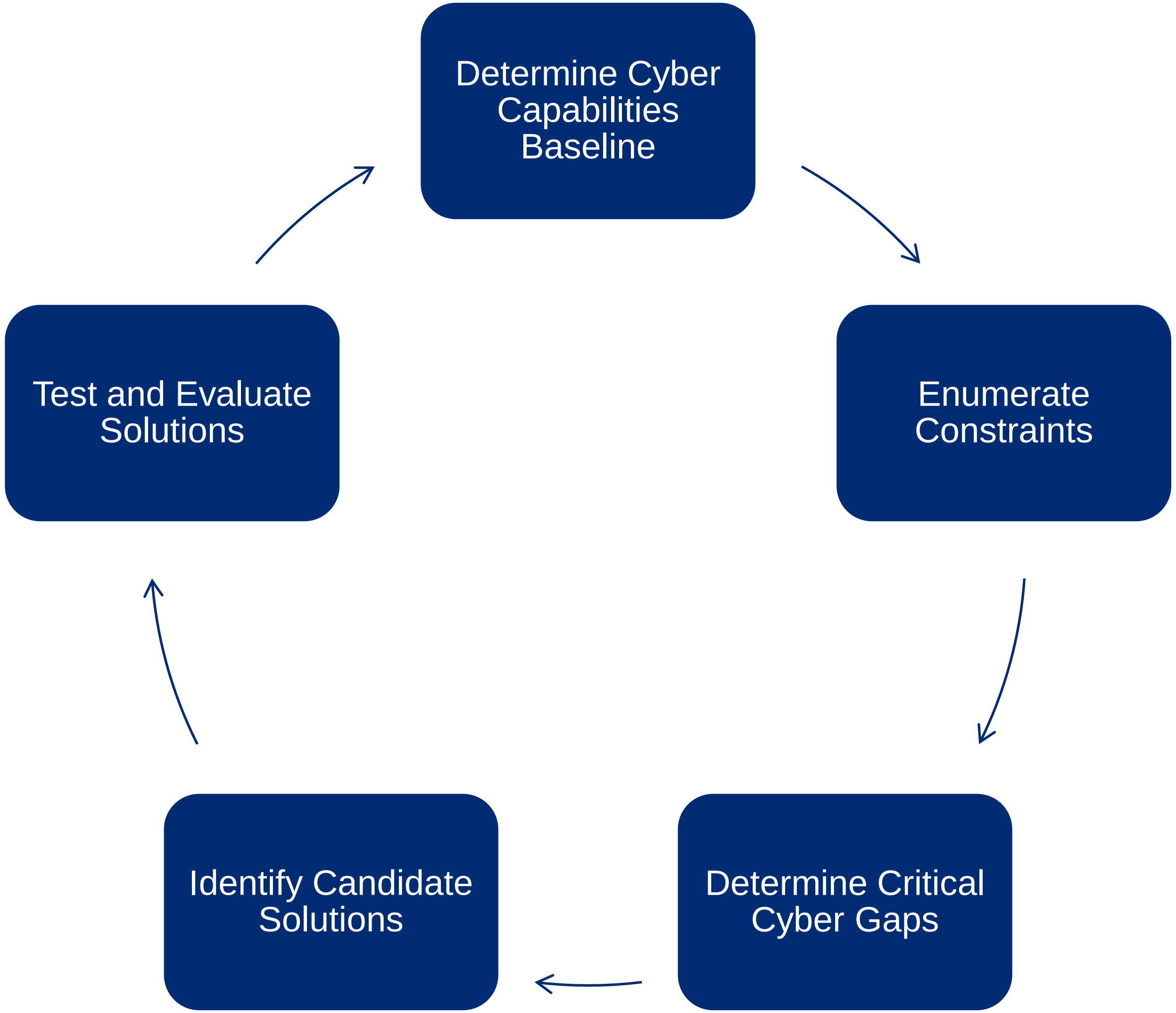
Automated Vulnerability and Risk Analysis

- Goal: Fully automated tool which can use currently available data

- Problem: cyber analysis today is either
  - Manual, non-quantitative, time consuming
  - Data dependent



Cyber Solution Development



Determine Cyber Capabilities Baseline

Enumerate Constraints

Determine Critical Cyber Gaps

Identify Candidate Solutions

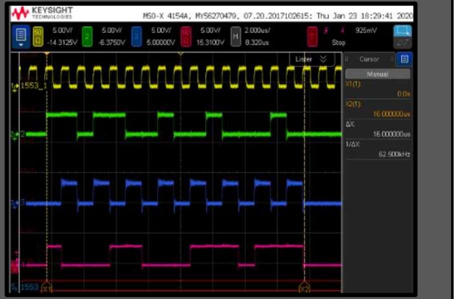
Test and Evaluate Solutions

TETRIS

- Tenacious Experimentation Toward Resilient Integrated Systems

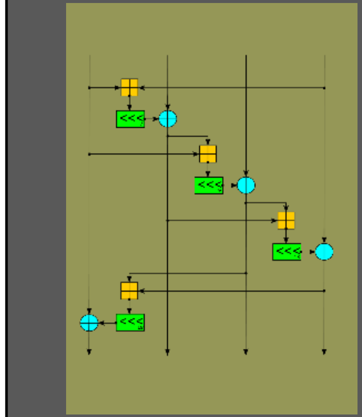
Research & Experimentation

Fully Homomorphic Encryption

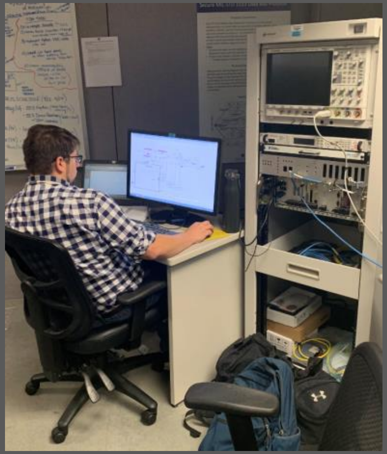


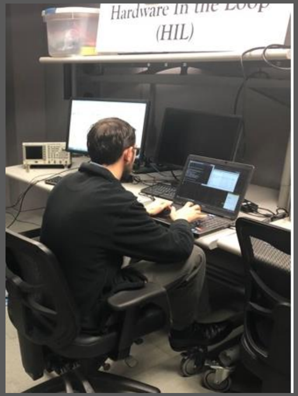
MSO-X 4154A, MY56270479, 07.20.2017102615: Thu Jan 23 18:29:41 2020

X1(1): 0.0s
X2(1): 16.000000us
ΔX: 16.000000us
1/ΔX: 62.500kHz

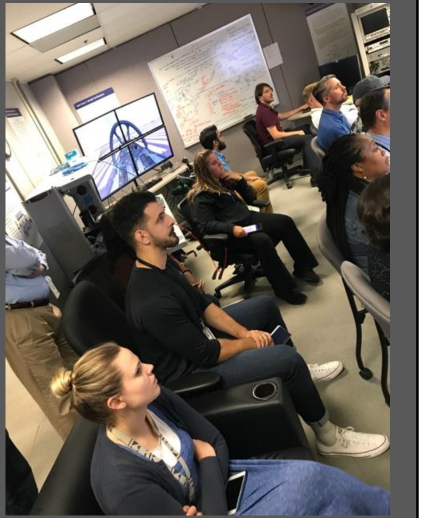


Prototyping



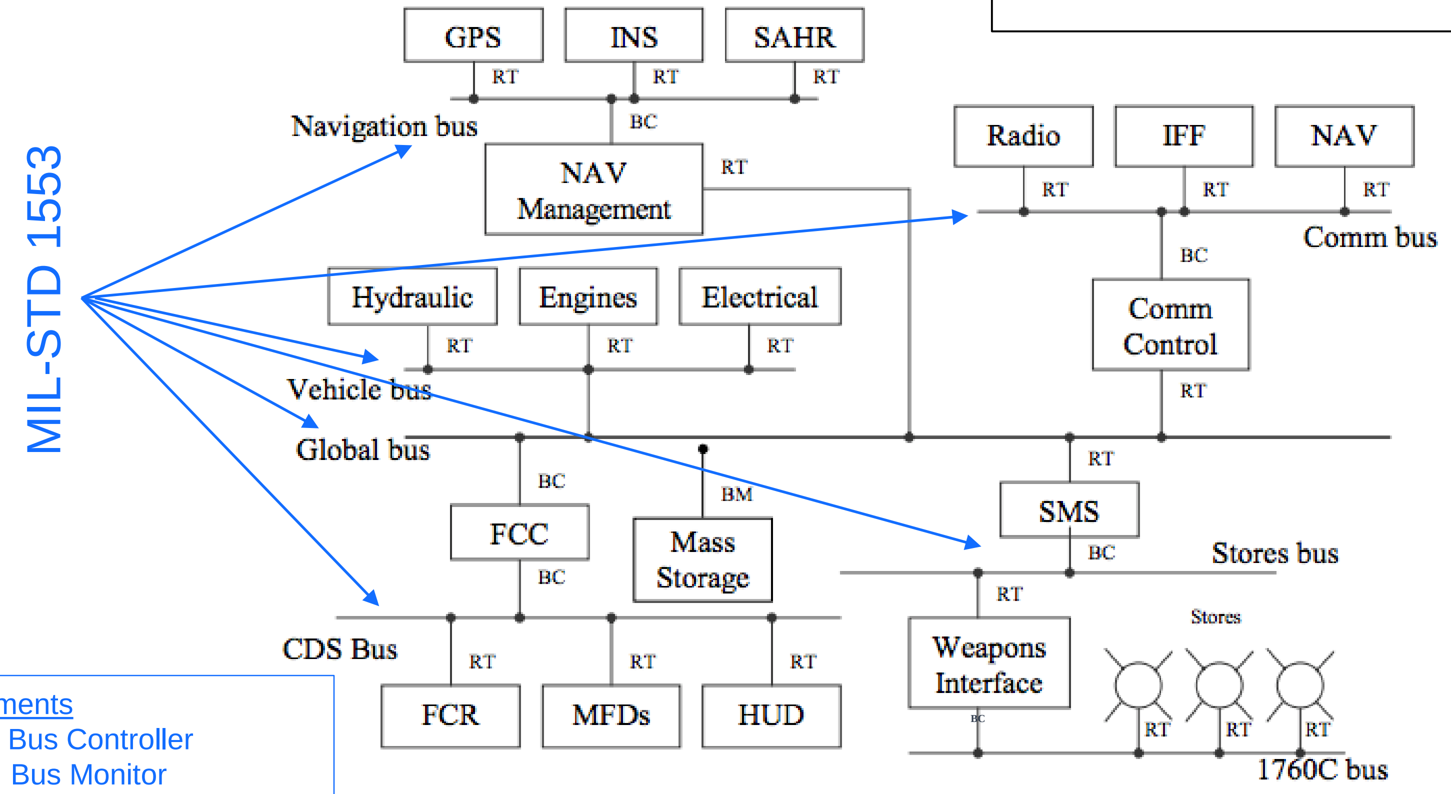


Demonstration



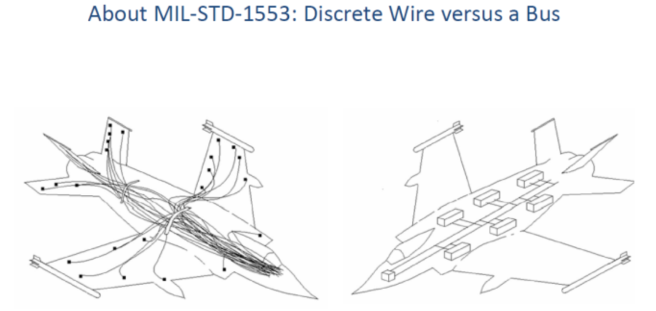
MIL-STD 1553 Typical System

Representative Military Platform Control Busses



Elements
BC: Bus Controller
BM: Bus Monitor
RT: Remote Terminal

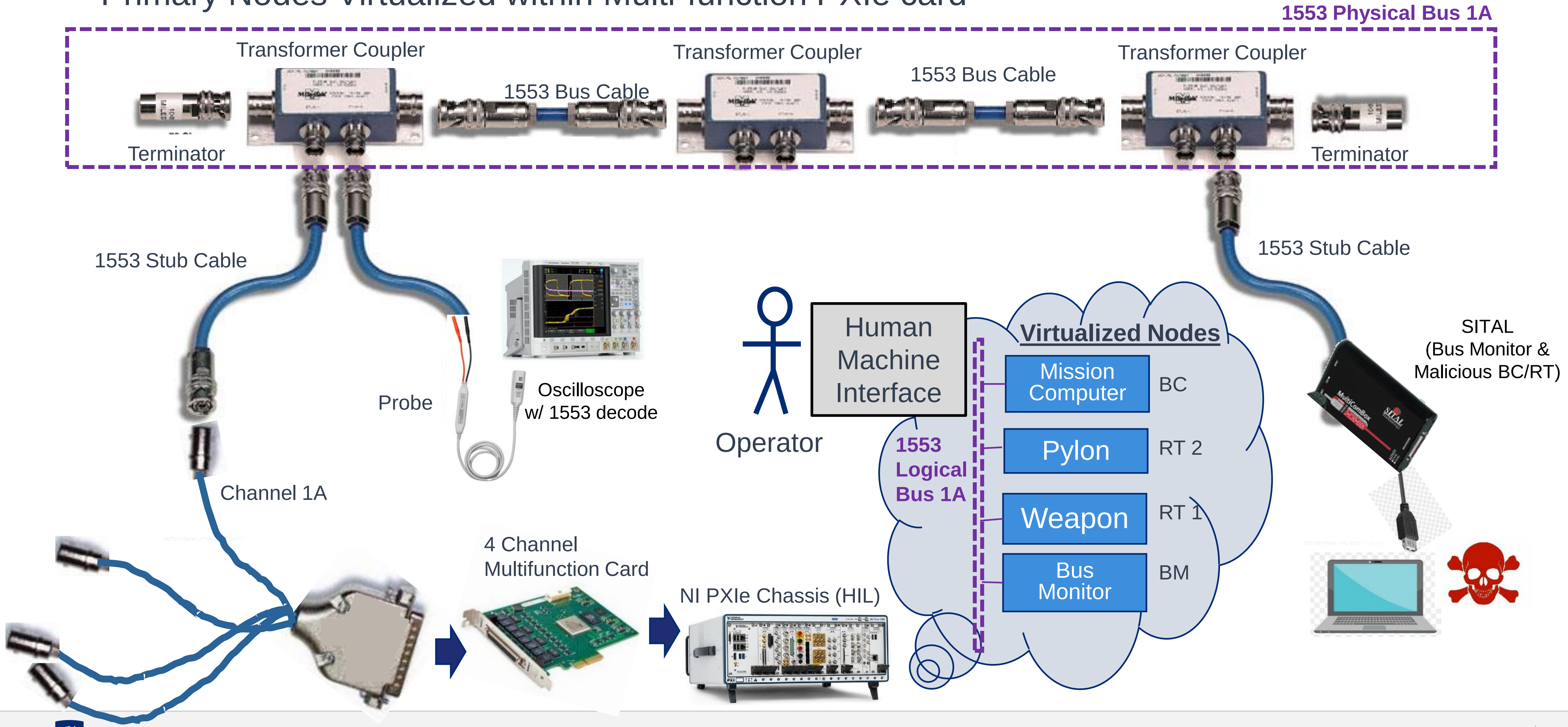
About MIL-STD-1553: Discrete Wire versus a Bus



- 1553 spec: SWaP-driven
- Shared media bus @ 1Mbps
- Response time: 4-12 uS
- Flat bus architecture
  - Up to 32 nodes per bus
  - Up to 32 sub-addresses per node
- Bus Controller manages all comms and timing
- Three fundamental 16-bit message classes:
  - Command Word
  - Data Words
    - 1-32 per message
  - Status Word
- No services explicitly defined above 1553 message layer: all implementations unique

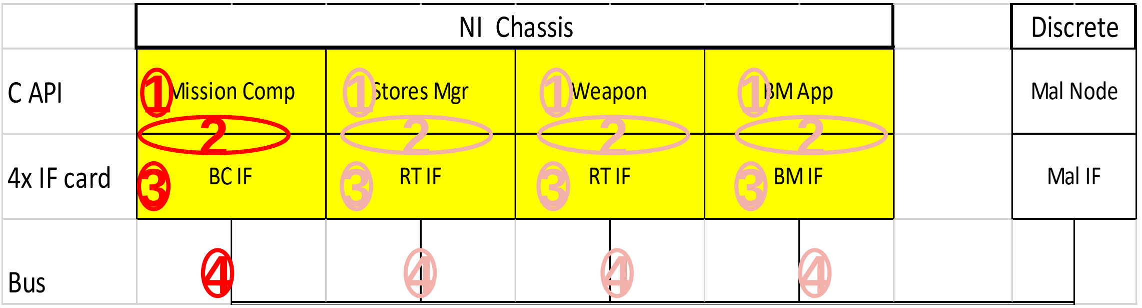
Physical Bench Layout for 1553 IRAD

Primary Nodes Virtualized within Multi-function PXIe card



1553 Systems – Cyber Defense Architectures

- How can we defend?
  - Situational Awareness
  - Authentication Services
  - Cryptographic Protection
- Where can we layer in cyber defense?



Architectural Options

1. Software services at application layer
2. SW shim
3. HW FPGA addition
4. Bump in the wire – external device or "smart coupler"

HW or SW to be replicated at each node

#1 is most simple entry point for proofs-of-concept
#4 is most robust objective solution: application- and interface-transparent

- Initial Mitigation Research
  - Software Crypto – ChaCha proof-of-concept crypto/authentication at application layer
  - Hardware Crypto – One Time Pad using bump in the wire

Summary

- Analyze, asses, mitigate tier IV cyber risk with respect to mission resilience
- Model the adversary and intersection with mission and system
- Improve tools and analytics to quantify mission/cyber concerns
- Address the capability gaps and needs of tactical systems

- Questions?

APL

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY

Zachary Birnbaum, PhD
Chief Scientist – Resilient Military Systems Group, JHUAPL
Zachary.Birnbaum@jhuapl.edu
240-228-6067