Cyber Attack Resilient Cyber Physical Systems

System-Aware Cybersecurity

Barry Horowitz

University of Virginia

Cyber Attack Resilience Presentation Outline

- Underlying Definitions and Concepts
- System-Aware Cybersecurity Resilience Architecture
- Technology Prototypes
  - UAV and Automobile prototype efforts
  - 3D Printing
- Human/Machine Teaming Issues
- Requirements Methodology/Analysis Tools for Resilience Solutions
- Example System Analysis

System Resilience*

- Resilience - the capacity of a system to maintain state awareness (Implies a monitoring process) and to proactively maintain a safe level of operational normalcy in response to anomalies (Implies a process of system reconfiguration, based upon diverse redundancy), including threats of a malicious and unexpected nature.

- The required anticipatory processes for monitoring and reconfiguration is conducted by a subsystem referred to as a **Sentinel**, which should be far more secure than the system being addressed for resiliency

- While the cyber attack detection process is expected to be automated, the level of reconfiguration automation may vary across system functions:
  - Totally Automated (Sentinel determines what to do and informs appropriately trained system operators regarding automated execution)
  - Semi-automated (System operators receive automated recommendation(s) from Sentinel and, accounting for both battle context and a broader set of information available to them, decide on what to do)
  - Manual (Operators, or higher levels in the command hierarchy, determine what to do)

- In addition, resilience includes:
  - Containing the immediate consequences of the detected attack
  - Post-attack forensic support based upon the data collected for addressing anomalies.

*Black Text: Rieger, etal, 2009 IEEE Human System Interactions Conference

*Red Text Related to Cyber Attack Resiliency: B.M Horowitz, UVA

System Engineering

- Integration of:
  - Policies
  - Processes (including accounting for human factors)
  - Technology
  - Data collections and analysis
- To create and continuously improve a satisfying system, based upon designs that have been subjected to significant analysis:
  - Mathematical
  - Historical data analysis
  - Logical and complete arguments
  - Simulation
  - Prototype trials
  - Operational Test and Evaluation

System Engineering and Resiliency

- Reconciling defense and resiliency
- Does my system prevent anomalous events or respond when they occur? Answers depend upon:
  - Consequences and likelihood of the anomalous event
  - Comparison of the effectiveness and costs of solutions, and considerations of policy, process, technology and data that accompany solutions

Traditional Cyber Attack Defense Solutions

- Information security is the process of securing information data from unauthorized access, use, modification, segmentation of distribution, or disclosure.
  - Encryption
  - Authentication
  - Authorization
  - Network

Traditional Resilient Systems

- Nuclear Weapon C2 System
  - Dual phenomenology for detecting a Soviet nuclear attack on US
  - Large multiple of diverse radio communication channels with different bandwidths, to counter nuclear weapon collateral effects, and EW or EMP attacks
  - False alarm attack warning event resulting in bombers being launched for potential nuclear response

- Air Traffic Control System
  - Primary/secondary radar systems
  - DC-10 Incident and prediction of anomalies
  - Airborne Collision Avoidance subsystem – deciding on how much is enough

Important Lessons Learned

- Solutions can vary from very low cost procedural solutions to very expensive system designs that offer resilience
- Solutions can address issues at the overall mission level (difficult to conduct a complete analysis and to manage the $) or at a specific acquisition subsystem level (analysis and $ are more manageable), but better solutions may be discovered when considering the System-of-Systems.
- For responding to rare events, need special training and exercising for operators.
- Need accepted methodologies and probably a specialty group for deciding on:
  - The most concerning anomalies
  - Resilience needs and budget for new systems
  - Adding resilience to legacy systems

SENTINEL-BASED ARCHITECTURE FOR CYBER ATTACK RESILIENCE OF PHYSICAL SYSTEMS

Important Factors Regarding Securing Physical Systems

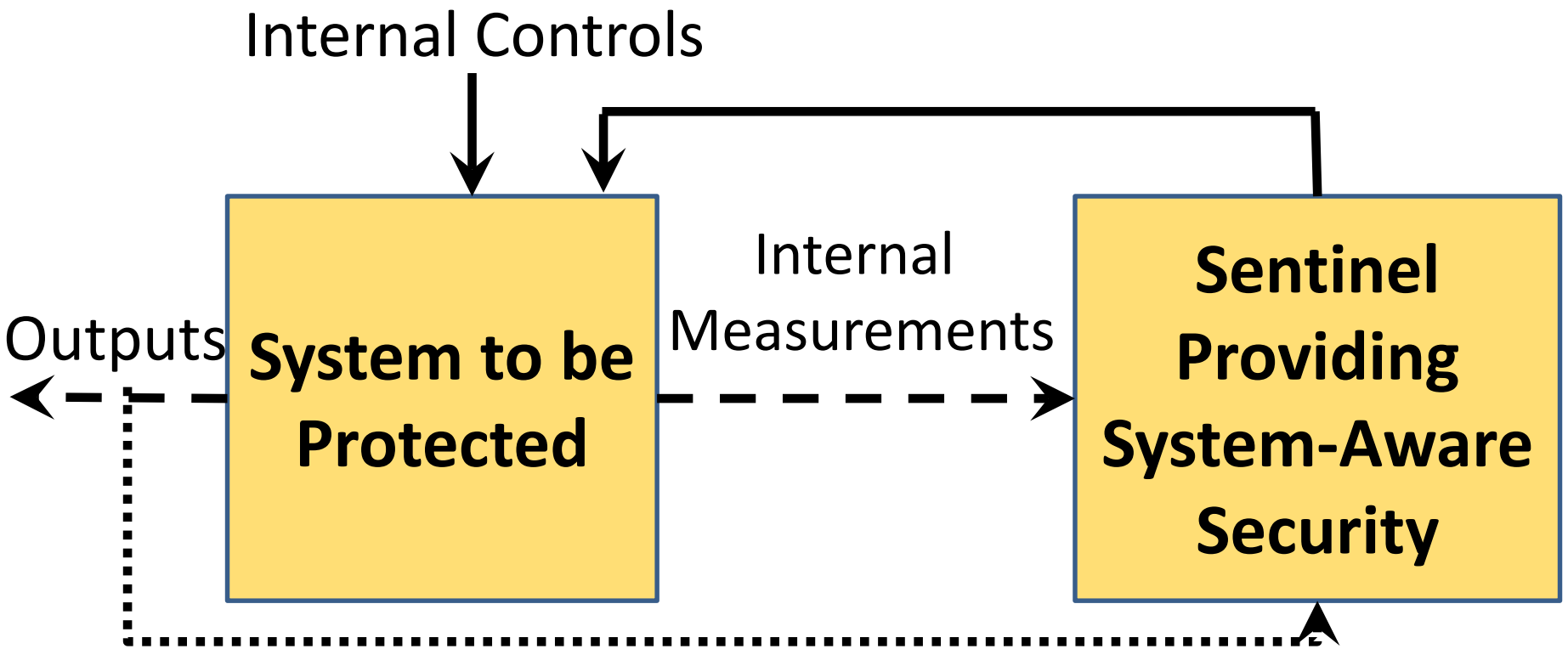
- Attack possibilities for critical physical systems are more contained than for information systems
  - More limited access to physical controls
  - Fewer system functions
  - Less distributed
  - Bounded by laws of physics
  - Less SW
  - Less physical states than SW states
- But
  - Successful attacks can do physical harm
  - Reconfiguration requires operational procedures for rapid response
  - Solutions requires confident operators who are trained to react to unprecedented cyber attack events
  - We have little experience regarding physical system attacks, although demos are coming out of the woodwork
- And

  Design of solutions requires knowledge of electro-mechanical systems and cybersecurity – significant Workforce and Education issues

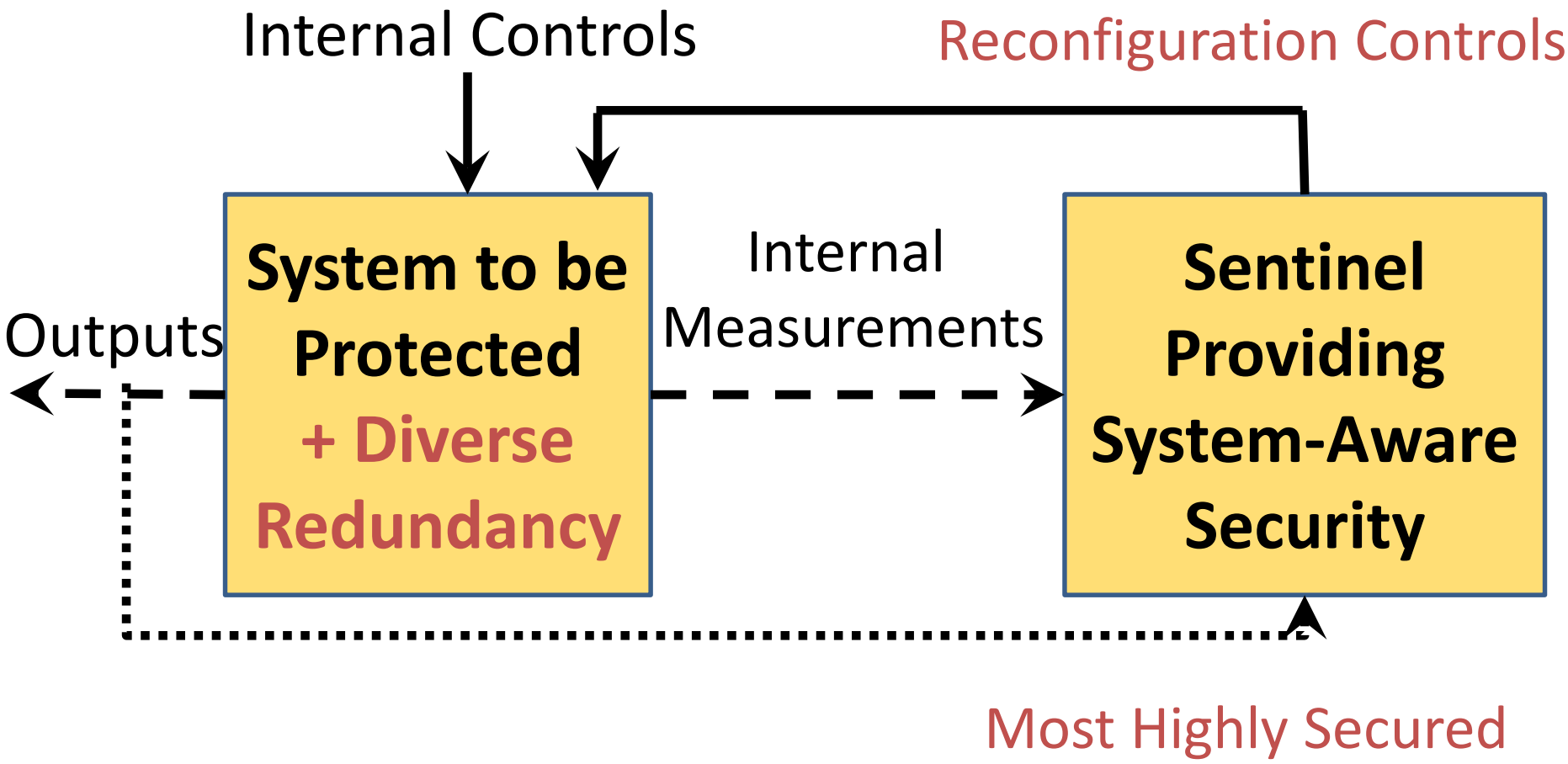
Broad Objective

Reversing cyber security asymmetry from favoring our adversaries (small investment in straight forward cyber exploits upsetting major system capabilities), to favoring the US (small investments for protecting the most critical system functions using System Aware cyber security solutions that require very complex and high cost exploits to defeat)

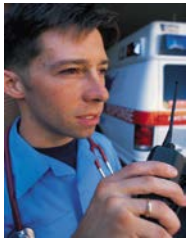
High Level Architectural Overview



High Level Architectural Overview



High Level Architectural Overview



Internal Controls

Reconfiguration Controls

System to be Protected

+ Diverse Redundancy

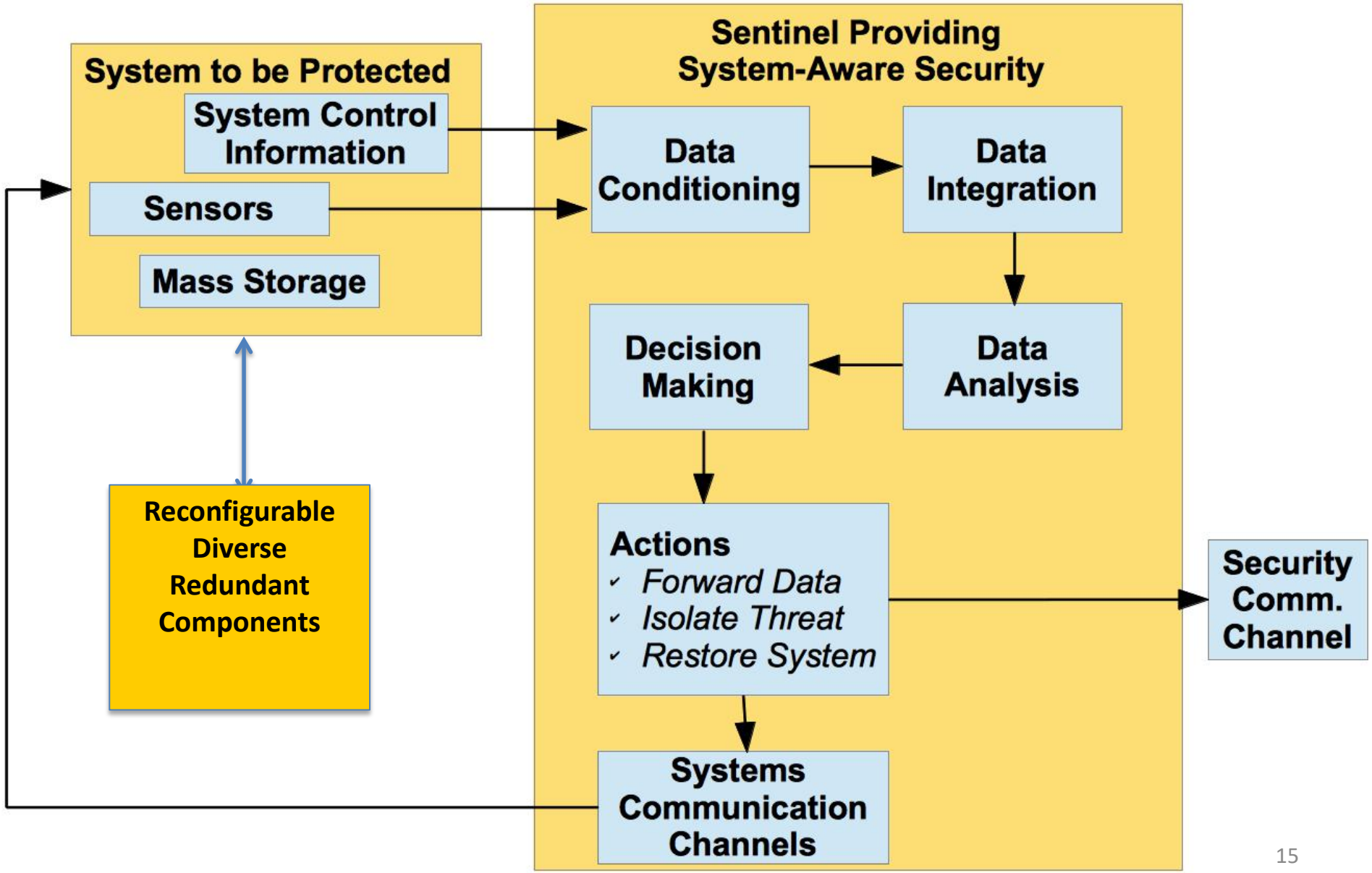
Internal Measurements

Outputs

Sentinel Providing System-Aware Security

Most Highly Secured

Sentinel Data Flow



System Aware Cyber Security Design Patterns

- Design Patterns combine design techniques from 3 communities
  - Cyber Security
  - Fault-Tolerant Systems
  - Automatic Control Systems (for physical systems)

A Set of Techniques Utilized in System Aware Cyber Security

Cyber Security

* Data Provenance
* Moving Target

  (Virtual Control for Hopping)
* Forensics

Fault-Tolerance

* Diverse Redundancy

  (DoS, Automated Restoral)
* Redundant Component Voting

  (Data Integrity, Restoral)

Automatic Control

* Physical Control for Configuration Hopping

  (Moving Target, Restoral)
* State Estimation Techniques

  (Data Integrity)
* System Identification

  (Data Integrity, Restoral)

A Set of Techniques Utilized in System-Aware Security

Cyber Security

* Data Provenance
* Moving Target

  (Virtual Control for Hopping)
* Forensics

Fault-Tolerance

* Diverse Redundancy

  (DoS, Automated Restoral)
* Redundant Component Voting

  (Data Integrity, Restoral)

Automatic Control

* Physical Control for Configuration Hopping

  (Moving Target, Restoral)
* State Estimation Techniques

  (Data Integrity)
* System Identification

  (Data Integrity, Restoral)

This combination of solutions requires adversaries to:

- Understand the details of how the targeted systems actually work

A Set of Techniques Utilized in System-Aware Security

Cyber Security	Fault-Tolerance	Automatic Control
* Data Provenance	* Diverse Redundancy (DoS, Automated Restoral)	* Physical Control for Configuration Hopping (Moving Target, Restoral)
* Moving Target (Virtual Control for Hopping)	* Redundant Component Voting (Data Integrity, Restoral)	* State Estimation Techniques (Data Integrity)
* Forensics		* System Identification (Data Integrity, Restoral)

This combination of solutions requires adversaries to:

- Understand the details of how the targeted systems actually work
- Develop synchronized, distributed exploits consistent with how the attacked system actually works

A Set of Techniques Utilized in System-Aware Security

Cyber Security	Fault-Tolerance	Automatic Control
* Data Provenance	* Diverse Redundancy (DoS, Automated Restoral)	* Physical Control for Configuration Hopping (Moving Target, Restoral)
* Moving Target (Virtual Control for Hopping)	* Redundant Component Voting (Data Integrity, Restoral)	* State Estimation Techniques (Data Integrity)
* Forensics		* System Identification (Data Integrity, Restoral)

This combination of solutions requires adversaries to:

- Understand the details of how the targeted systems actually work
- Develop synchronized, distributed exploits consistent with how the attacked system actually works
- Corrupt multiple supply chains

Examples of Design Patterns That Have Been Prototyped

- **Diverse Redundancy** for post-attack restoration
- **Diverse Redundancy + Verifiable Voting** for trans-attack attack deflection
- **Physical and Virtual Configuration Hopping** for moving target defense
- **Data Consistency Checking** for data integrity and operator display protection
- **Parameter Assurance** for parameter controlled SW functions
- **Application-Layer Introspection** for matching machine work loads to observed system behavior
- **Real-time Resilience Testing** for increased operator confidence

Illustrative Examples of Illogical Control

- Navigation waypoint changed, but no corresponding communication received by UAV
- Automobile sensor shows distance between cars reducing, but collision avoidance control system speeds up the following car
- Selected material to create part of a 3D printed object does not match what the executing design calls for
- Mode of Fire Control System changed, but no touch screen input from operator
- Operator display system shows little activity, but related CPU and memory utilization is high

Parameters in Systems

- Parameters control how systems function – for instance:
  - Detection Thresholds
    - For example, target detection for active sensors (Radar), Passive sensors (SIGINT), impacting missed detection/false alarm performance
  - Modes of operation for “Smart Systems” that modify performance on a situational basis
    - CFAR (Constant False Alarm Rate) in sensor systems
  - Flight control boundary values
    - For example, bounds on accelerations, velocity, altitude
  - Navigation Waypoints
  - Tracking algorithm parameters determine sensitivity and latencies for position/velocity estimates relative to timing of accelerations
  - Communication system mode parameters, impacting QOS

Parameters in Systems

- Parameters control how systems function – for instance:
  - Detection Thresholds
    - For example, target detection for active sensors (Radar), Passive sensors (SIGINT), impacting missed detection/false alarm performance
  - Modes of operation for "Smart Systems" that modify performance on a situational basis
    - CFAR (Constant False Alarm Rate) in sensor systems
  - Flight control boundary values
    - For example, bounds on accelerations, velocity, altitude
  - Navigation Waypoints
  - Tracking algorithm parameters determine sensitivity and latencies for position/velocity estimates relative to timing of accelerations
  - Communication system mode parameters, impacting QOS

    Parameter tables provide an organized means for changing operating modes in smart, situational aware system designs and a high leverage opportunity for exploits

Rapid Prototype Example Implementations

- UAV (Air Force)
- Weapon systems (Army)
- Police Cars (Virginia State Police)
- 3d Printer
- Ship Plant Control System (Northrop)
- Power Plant (GE)
- Image Exploitation System (Leidos)

3D Printer Example

- https://youtu.be/l2nHraDKYD4

Video for Automobile Cyber Attack

HUMANS

Role of the Human

- Automation is rule based; Human-role is knowledge-based for addressing cases where rules have not yet been developed
- Will humans know what to do when informed that a cyber attack has been detected?
- How does the human utilize pre-mission information that is not being utilized by the Sentinel?
- Will the person be ready to respond?
  - Know what is happening
  - Decide what to do
  - Rapidly do it
- How do we prepare humans and certify their abilities to carry out their roles?
- These questions are not only pertinent to cyber attack responses, but also to address unanticipated shortfalls in AI designs related to cyber physical systems

Creech AFB Project Results - Feedback from 8 Pilots (2014 UVA, MITRE Project)

- 432 WG pilots and WOC leadership are not aware of any other initiative that is addressing this issue from the operational perspective
- Unless there is intelligence or Sentinel cueing, cyber attack responses at the tactical level (pilot level) would be executed under the assumption that there is some unknown anomaly (maintenance issue).
- Identified cyber attacks would likely result in immediate Return to Base unless Sentinel-like technology provides assurance that critical systems are protected
- Timing of appropriate response is important – react quickly if needed vs. being more considerate about decision
- If a Sentinel reports a cyber event and helps correct it, how does one know that the attack will not be followed by yet another attack that could take over the aircraft or fire weapons
- Would like ability to immediately access a cyber person…wouldn't know who to call…expertise not at the unit
- Many "Can Not Replicate" cases have occurred- Were they cyber attacks?

Remote Control Vehicle Experiment (2017 UVA, AFIT Project) (1 of 2)

- AF Lt Col C. Gay's PhD Dissertation addresses operator HMT roles/performance in providing cyber resilience
- Scenario of delivering important materials to a remotely located war fighting group
  - High priority mission
  - Training mission
- Disruptive cyber attacks with Sentinel correct detections, some false detections, and some missed detections
- Measure performance based on a pre-experiment determined ranked set of possible operator decisions and delay times in responding

Remote Control Vehicle Experiment (2017 UVA, AFIT Project) (2 of 2)

- Built upon prior research related to the general suspicion level of a person and their HMT level of performance
- These cyber attack experiments evaluated 32 AF Officers engaging in 8 operational scenarios
- Experiments involved remotely managed vehicles operating on the grounds of WPAFB being disrupted by various cyber attacks
- Major Findings:
  - More suspicious operators required longer times to decide on resilience responses, but solutions were no better and delays made attack consequences worse
  - The delays were more pronounced for the higher consequence scenarios
  - Need to develop training programs that prepared operators for addressing the breadth of cyber attack situations that can occur as well as address cyber attack scenarios/response possibilities as part of pre-mission planning efforts
- UVA/AFIT are currently completing a follow-on experimental effort to explore the possibilities for better preparing operators to respond to detected cyber attack

RISK-BASED METHODOLOGY AND SUPPORTING ANALYSIS TOOLS FOR PRIORITIZING POTENTIAL RESILIENCE SOLUTIONS

Fundamental Assumptions (1)

- Although cybersecurity solutions are distinctly categorized into 2 classes (defense, resilience), system security solution requirements should be holistically determined, considering these 2 classes of solutions as complementary to each other

- The requirements process should be accomplished through the integration of:
  - Experience-based analysis - referred to as an “Experience-based Step” in the overall process
  - SE Model-based analysis - referred to as a “Model-based” step

- The integrated process for establishing requirements should include inputs from multiple communities:
  - Operations
  - Mission Planning
  - Logistics (Deployment and Rapid Response Readiness)
  - System Engineering/ Resilient Systems
  - Cybersec/ Both Defense and Red team oriented
  - Threat Analysts
  - OT&E

- Model-based analysis methods should include employment of :
  - System description tools(e.g. SysMl)
  - Attack related tools(e.g., SecurITree)
  - Existing data bases regarding cyber attacks (e.g., CAPEC, CVE,CWE, ATT&CK)
  - Analytical techniques that support cybersecurity-related design and development decisions (e.g., use of static analysis tools) based upon the integration of risk-related information and other factors influencing the overall design of the system under development
  - Rapid prototyping tools to enable evaluation of the operational and technical implications of potential resilience solutions

Fundamental Assumptions (2)

- Establishment of cybersecurity design requirements through a process that integrates experience-based and model-based methods can be accomplished within the time window allocated to a system's overall design requirements process

- The cybersecurity design requirements process can be started early in the development process and in a sequential manner gain greater specificity together with other parts of the system's design
  - Start with high level risk-related experience-based steps (accounting for both consequences and likelihood) at the system function level
  - Based upon more specificity in system design, transition the cybersecurity design process to include model-based steps including rapid prototyping-based requirements derivations for resiliency

- When the system design becomes ready for implementation decisions, system planners and program managers can be provided with computer-aided support for utilizing both experience-based and model-based results to finalize their decisions regarding cybersecurity solutions

Blue Team, Red Team, and SE Team Contributions to Risk Analysis

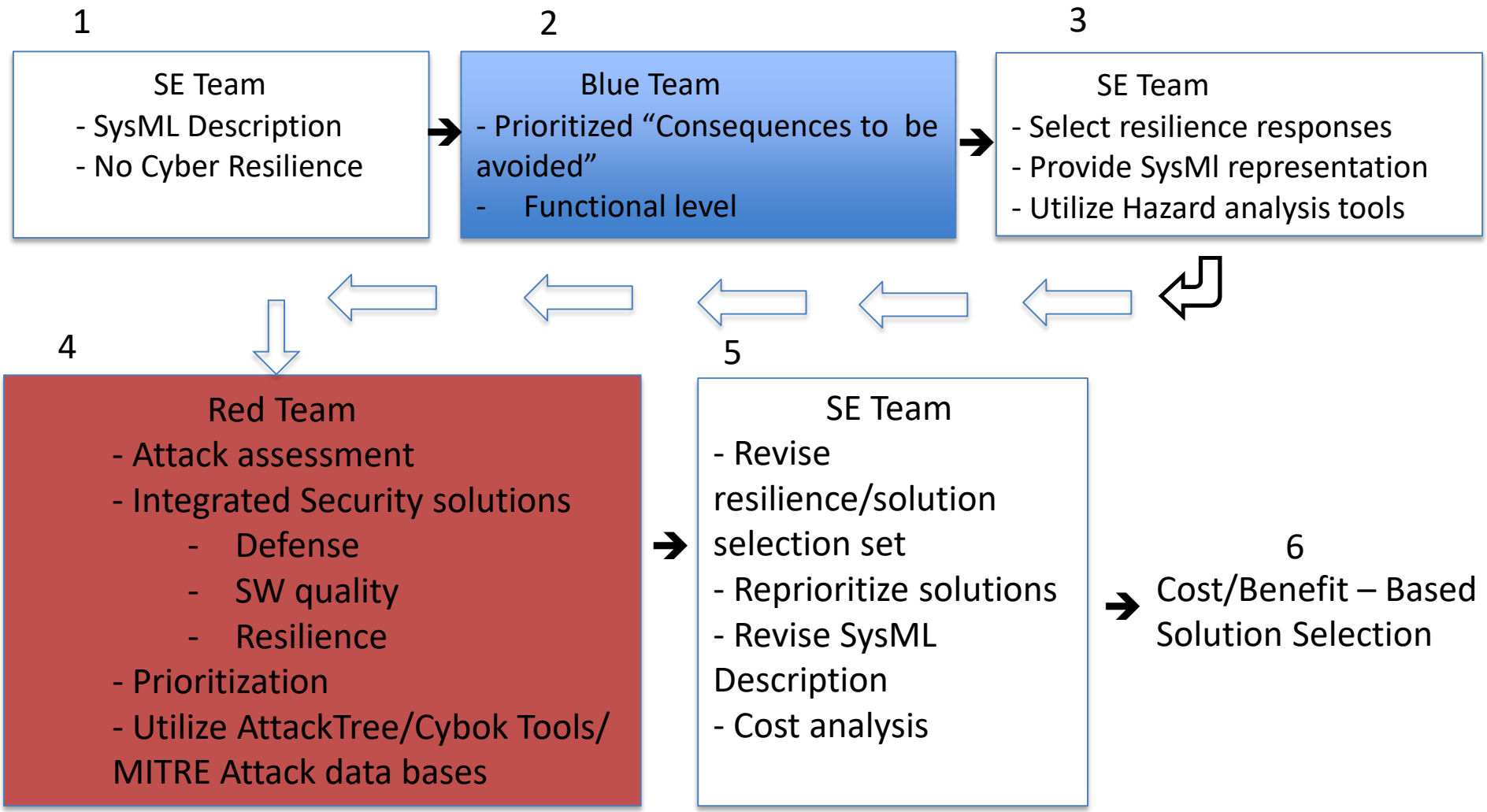
- Risk= Consequence X Likelihood

- **Blue Team** is responsible for, and most knowledgeable about, the consequence portion of risk – Provide a prioritized set of consequences to be avoided, assuming that system design/implementation and life cycle costs, complexity, implementation time, etc. were equal (Blue Team does not derive possible attacks that would achieve the consequences).

- **Red Team** is responsible for, and most knowledgeable about, the likelihood portion of risk – Provide a prioritized set of attacks based upon their view of the attacks' feasibility, consequences, complexity, cost, implementation time, etc.

- **SE Team** organizes and supports an integrated process for selection of a satisfying combination of defense/resilience system security solutions that is based upon prioritizing risk (i.e., the combinations of consequences and likelihoods) subject to constraints on budget, complexity, implementation time, etc.

6 Part Iterative Process



Examples of Potential Consequences

- Possible military impacts for cyber attacks against a cyber physical system
  - Deployment
    - Apparent failure of deployment tests
    - Successful tests, but improper deployment
  - Communications
    - Denial of communications (overt or covert)
    - Message delay
    - Message modification
  - Operator situation awareness
    - Loss of information presentation
    - Corruption of presented information
    - Delays in presentation of information
  - System control
    - Manipulate or delay doctrinal messages
    - Modify operators' selections among alternative system modes of operation
    - Deny, manipulate or delay fire control messages, test-related messages, control confirmation messages
  - Data extraction

Red Team Table

ID	Intended Effect	Attack Profile	Attack Method	Attack Architecture	Cost (time, test, difficulty, monetary)	Mitigation Potential

- Intended effect
  - What consequences are the attackers seeking? E.g. gain control of weapons, deny use of weapons
- Attack Profile
  - Potential way to achieve the intended effect e.g. code injection, delay data transfer, data element change.
- Attack Method
  - Supply Chain, Insider, Network, Reuse of existing attack
- Attack Architecture/ATT&CK

  Does this attack consist of a sequence of attacks to achieve an outcome, if so what are they?
- Cost
  - The cost in terms of time, testing needed for the attack, the difficulty of the attack, and any monetary costs
- Mitigation Potential
  - How easy would it be for the defenders to make this attack too difficult, impossible, etc.?

Potential Attack Scoring Methods

- Cost Likert Scale
  1. Attack is not difficult to implement, nor does it require much overhead
  2. Attack is not difficult to implement, but requires some testing or time before implementation
  3. Attack is moderately difficult and/or requires testing/time before implementation
  4. Attack is very difficult to implement and requires significant overhead
- Mitigation Likert Scale
  1. Securing against this attack would require significant prevention or resiliency measures to be implemented in the system
  2. Some defense or resiliency measures would make this attack significantly more difficult to implement
  3. Simple defense or resiliency measures would eliminate this attack as a viable option
- Use selected MITRE ATT&CK model matrix elements to address attack architecture
  1. Persistence
  2. Defense Evasion
  3. Exfiltration
  4. Command and Control

Silverfish Use Case

Defense Against Ground-based Attack Within a 100 Acre Area

System of Systems Functionally-Based USE CASE Description

Command Center

- Mission planning
- C2
- Doctrine Control

Surveillance Systems

- IR
- Obstacle-based acoustic/seismic
- UAV-Based

Silverfish Weapon

- Weapon System Obstacles/Munitions
- Deployment Support Subsystem

Communications Systems

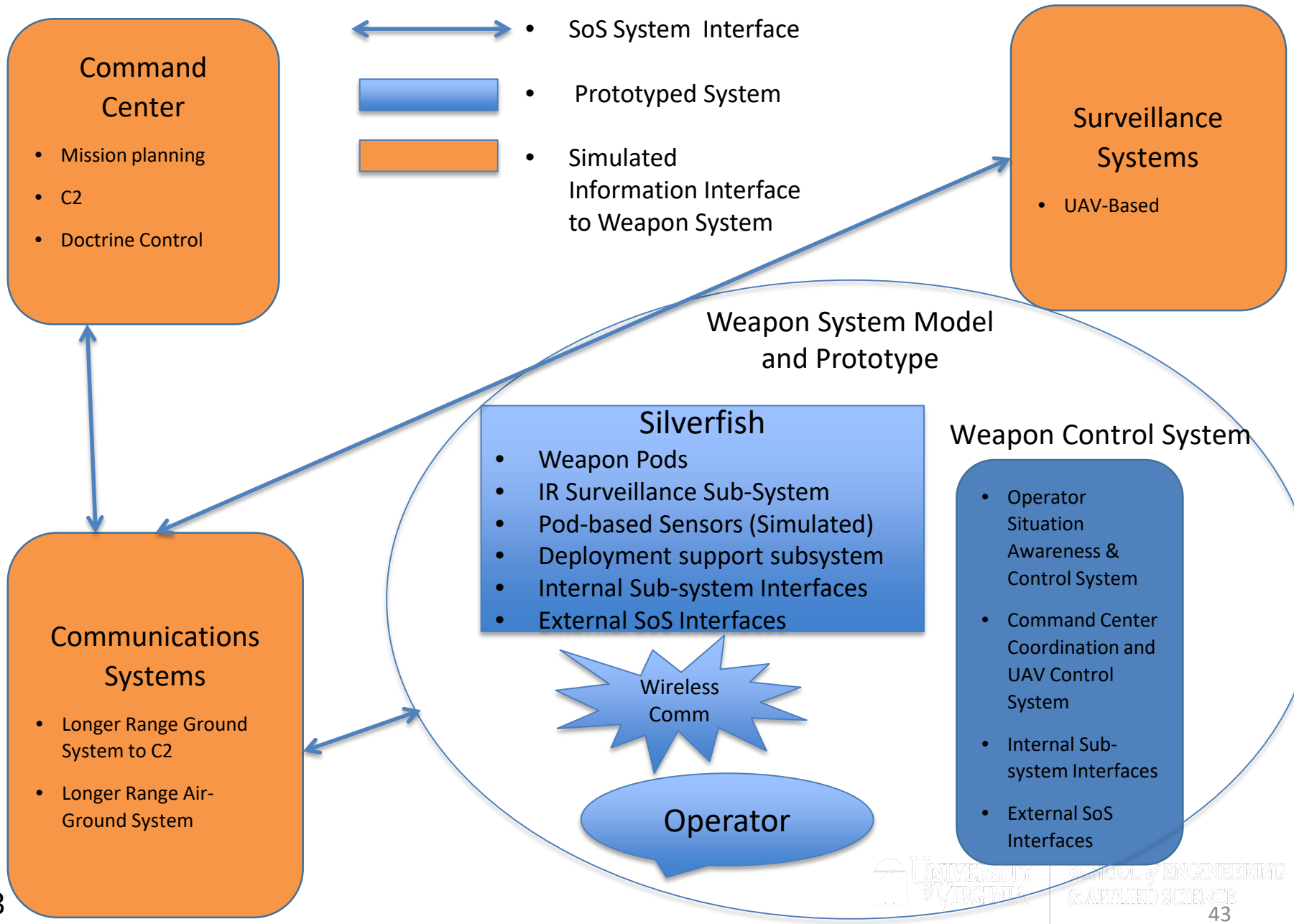
- Weapon Wireless Network
- Longer Range Ground Comm System for C2-Weapon Operator Comm
- Air-Ground System for UAV-Operator Comm

Silverfish Weapon Control System

- Operator Situation Awareness
- Weapon Control System
- Warnings to Adversaries
- Command Center Coordination and UAV Control System

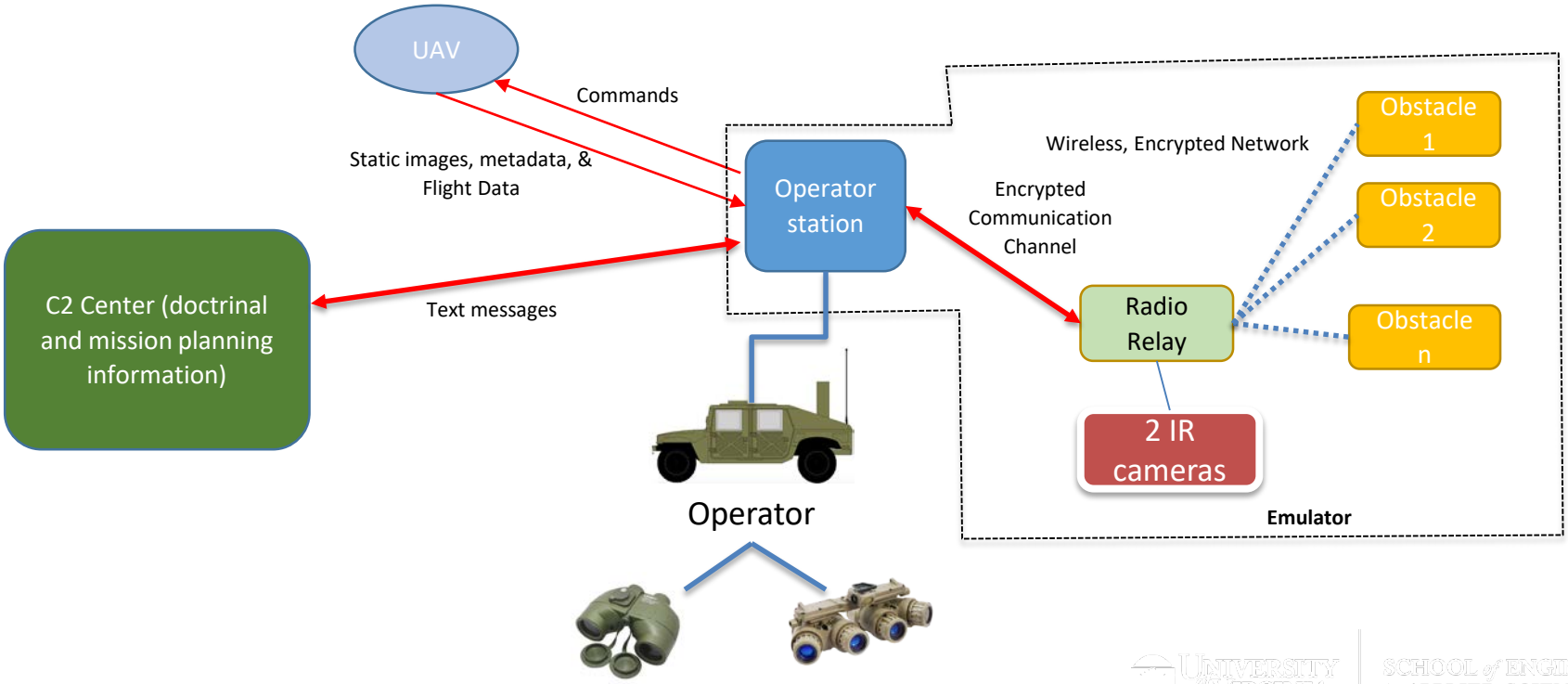
42

Rapid Prototype USE CASE Description for Operational Evaluations



43

System Description (pre-resilience design)



44

Obstacle Description

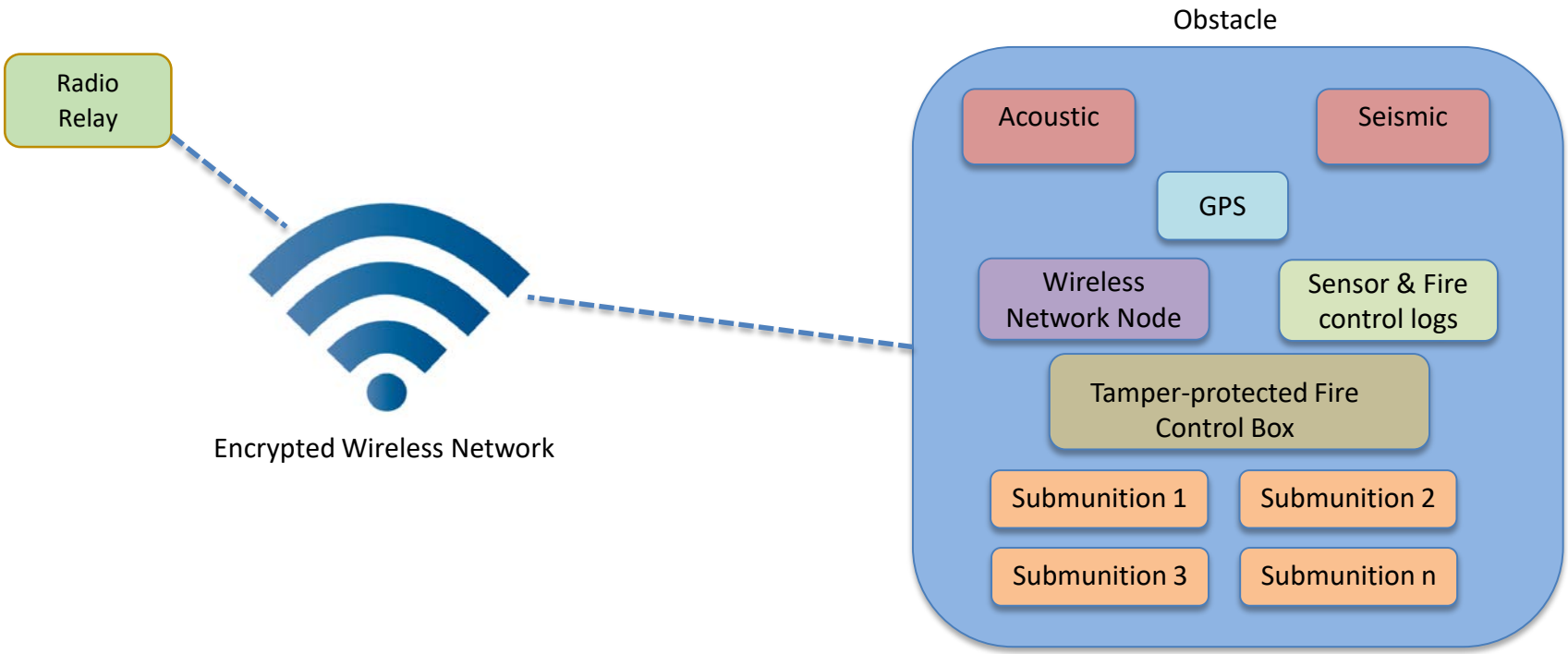


Table of Blue War Room Output

ID	Attack Outcome	Attack Target(s)	Attack Method	STPA Type	Likert Priority
1.1	Inappropriate firings via manipulating operator commands	Operator control display, radio comm links	External, supply chain, insider	1, 2, 3	1
1.2	Delays in fire time (sufficient delay to cross field)	Obstacles, control station, radio comm links	External, supply chain, insider	2, 3	1
1.3	Delays in deployment	Obstacles, deployment support equipment	Supply chain, insider	2, 3	1
1.4	Deactivation of a set of obstacles	Obstacles	External, insider	1, 3	1
2.1	Delays in situational awareness	Operator display, sensors	External, insider, supply chain	1, 2, 3	2
2.2	Prevent or corrupt transmission of situational awareness data	Radio comm links, operator display, sensors	External, insider, supply chain	1, 2, 3	2
2.3	Gain information to help adversary navigate through field	Obstacle, operator control station	External, insider	2, 3	2
3.1	Reduced operational lifespan	Obstacle	External, supply chain, insider	1, 2, 3,	3
3.2	Prevent transmission/execution of non-firing commands	Operator display, obstacles	External, insider, supply chain	1, 2	3
4.1	Delays in sending/receiving C2 information	Operator display, radio comm links	External, supply chain	1, 2, 3	4
4.1	Delays in un-deployment	Obstacles	External, insider, supply chain	1, 2, 3	4

Key for the table

STPA hazard types (System Theoretic Process Analysis)

1. Providing a control action causes a hazard
2. Not providing a control action causes a hazard
3. Incorrect timing or improper order of control actions causes a hazard
4. A control action is applied too long or stopped too soon

Likert Priority Scale

1. Unacceptable and highest priority to provide resiliency
2. Avoid as long as resiliency solution does not over-complicate operation
3. Would like to avoid, but solution needs to be incremental
4. Lowest priority, low-cost, simplistic solutions should be considered
5. Not of interest at the present time, recorded for future use

Silverfish Design Options for Cyber Attack Resilience

Resilience Design Options

- Design 1 – Control Resilience
  - Resiliency measures focused on ensuring continued ability to properly control weapons
- Design 2- Network Resilience
  - Focuses on maintaining situation awareness and control-related communication integrity between different nodes
- Design 3 – Situational Awareness Resilience
  - Focuses on maintaining the integrity of situational awareness data

Resilience Design 1 – Control Resilience (1 of 2)

- Military Functions of interest
  - Fire control
  - Weapon mode control
- Potential Attack Effects
  - Overt Denial of Operation
    - » Operator's screen goes blank
  - Covert Denial of Operation
    - » Button pressed by operator, different or no action performed , confirmation of received message presented to the operator
    - » Delay in control message being sent from operator's control station
- Detection Methods (Data Consistency and Introspection)
  - Sentinel monitors keyboard inputs and operator control computer outputs to detect situations of inputs coming in but not going out, commands out not matching operator input, commands out time delay too long

Resilience Design 1 – Control Resilience (2 of 2)

- Resilience Solution (Diverse Redundancy, Operator Confidence Test)
  - Alert operator, semi-automatically switch to diverse computer, run real-time test on new system to ensure it is working, operator confirms through observation of situational awareness data
- Additional HW/SW required for resilience
  - Secondary, diverse control system computer
  - HW: 1 Sentinel connected to operator's control station and with wireless communication to the network for test observations
  - SW: Monitoring and detection SW, testing SW, presentation-related SW to support Operator/Sentinel interactions
- Operator's roles
  - Decide to act on detection information and on the prompt to switch computers
  - Confirm tests based upon situational awareness information

Resilience Design 2 – Network Resilience (1 of 2)

- Military Functions of interest
  - Communication for weapon control & situational awareness
- Attack Effects
  - Overt Denial of Operation
    - » Network goes down (no messages sent/received)
  - Covert Denial of Operation
    - » Messages sent to incorrect recipient or messages do not reach recipient
- Detection Methods (Data Consistency, Introspection)
  - Sentinels monitor the interface between the network and its users (operator station, obstacles, sensors) for:
    - Message header content, send/receive times, metadata regarding message flow
    - Data quantity and rate (e.g. number of packets sent by operator or sensors versus packets received)

Resilience Design 2 – Network Resilience (2 of 2)

- Resilience Solution(Diverse Redundancy, Operator Confidence Test)
  - Alert operator, semi-automatically switch to diverse network, run real-time test on new network to ensure it is working
- Additional HW/SW required for resilience
  - Secondary, diverse network
  - 3 sentinels – operator-side, obstacle/sensor-side, central sentinel for coordination of operator/obstacle Sentinels
    - Monitoring interface input/output data for consistency and detection algorithms
    - Presentation layer for sentinel data
  - Post-switch testing SW
- Operator's roles
  - Decide to act on prompt to switch networks
  - Confirm tests based upon situational awareness information

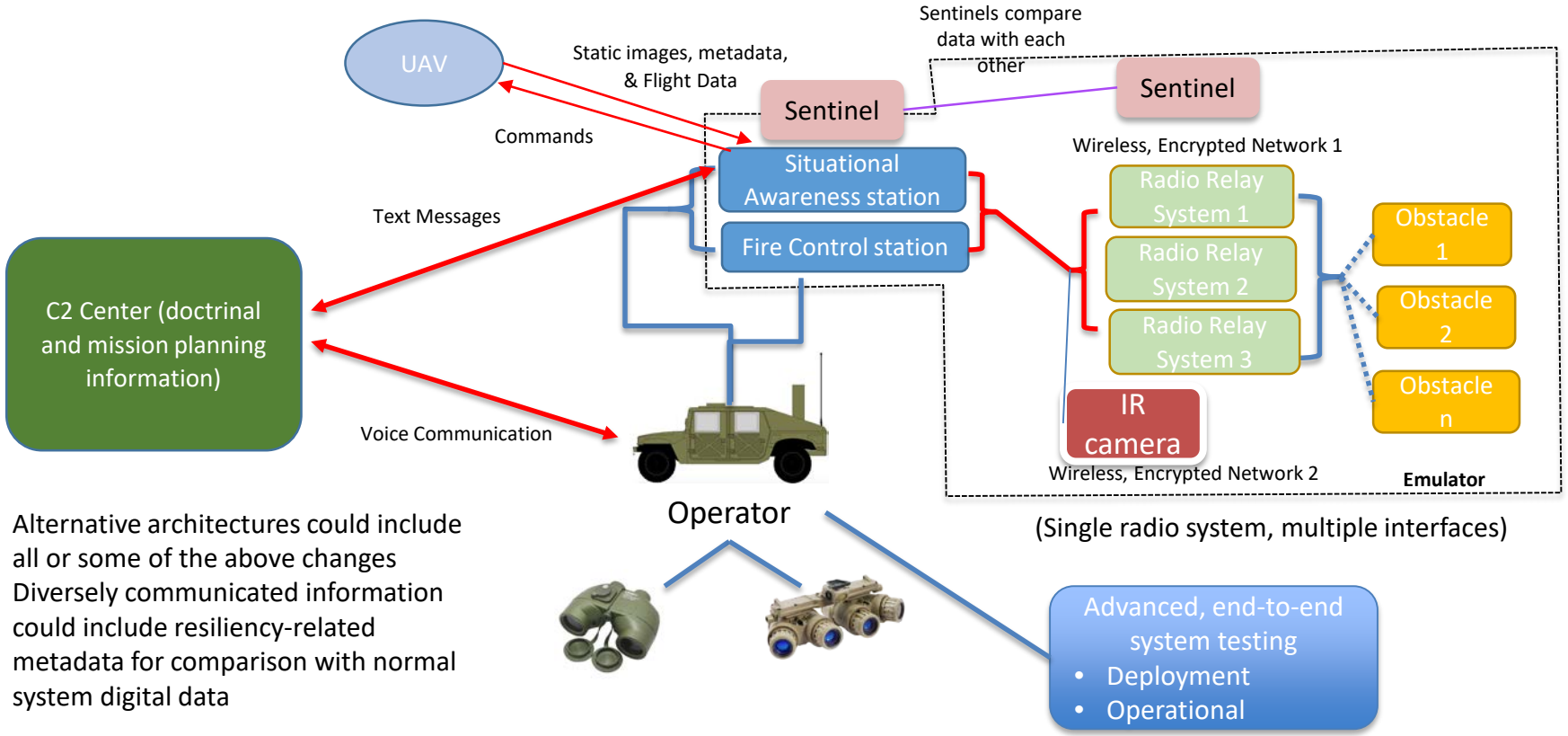
Resilience Design 3 – Situational Awareness Resilience (1 of 2)

- Military Functions of interest
  - Presentation of accurate situational awareness data
- Attack Effects
  - Overt Denial of Operation
    - » Situational awareness display goes down
  - Covert Denial of Operation
    - » Data changed on situational awareness display
    - » Disparity between sensor data (includes not receiving data from one/more sensors)
- Detection Methods (Data Consistency, Introspection, Voting with Diverse Redundant Sensors)
  - Sentinel monitors
    - Situational awareness display for disparities between data packets received versus information presented
    - Data packet consistency across sensors

Resilience Design 3 – Situational Awareness Resilience (2 of 2)

- Resilience Solution (Diverse Redundancy including Manual Mode, Operator Confidence Test)
  - Alert operator, semi-automatically switch to separate computer, run real-time test on new system to ensure it is working
  - Sensors- Alert operator of disparity, use voting to kick out bad sensor, fall back to remaining sensors, prompt or suggest falling back to manual mode
- Additional HW/SW required for resilience
  - Secondary, diverse situational awareness computer
  - 3 sentinels – operator-side, obstacle/sensor-side, central sentinel
    - Monitoring software for consistency
    - Presentation layer for sentinel data
  - Post-switch test SW
- Operator's roles
  - Decide to act on prompt to switch computers
  - Possibly switch to pre-determined manual situational awareness methods, including re-locating vehicle to enhance visibility

Alternative System Sub-Architectures for Achieving Cyber Attack Resiliency



- Alternative architectures could include all or some of the above changes
- Diversely communicated information could include resiliency-related metadata for comparison with normal system digital data

SE Methodology Use Case (Step 4 of 6)- Red Team Response

1. Supported use of suitable encryption as suggested by the Blue Team and assumed by the SE team
2. Suggested that the weapon control system HW/SW be separated from the situation awareness related functions, including separate operator displays
3. Based on the limited weapon control sub-system functionality, recommended use of the following SW development practices for the control functions:
   - Full suite of software quality tools (static and dynamic test tools),
   - Extensive end to end testing
   - High end SW designers/developers
   - Correspondingly, assuming adoption of the proposed SW development practices, suggested lowest priority for diverse redundancy solution
4. Suggested voice-only military communications system to the Command and Control system to avoid potential attacks through the C2 system
5. Considered the communication sub-system as highest priority for resilience, using diverse redundancy to address attacks resulting in Denial of Service and Message Delays
6. Suggested that the resiliency design for situation awareness be the second highest priority for resilience, including diverse redundant IR sensors
7. Suggested considering attack detection capability for weapon control system
8. Suggested considering adding operator authentication solution if there were potential scenarios for interactions across separately defended areas

SE Methodology Use Case (Step 4 of 6 continued)- Tool-Based Inputs

- Using the SysMl models as input, CYBOK produced an attack surface that highlighted attacks on the Communications network
  - Specifically it found potential attacks on the communication network from CAPEC, CWE, and CVE
  - E.g., CAPEC 615 Evil Twin (Man-in-the-Middle) Wi-Fi Attack**,** CWE-287: Improper Authentication, and many CVEs for violations on Wi-Fi in specific products

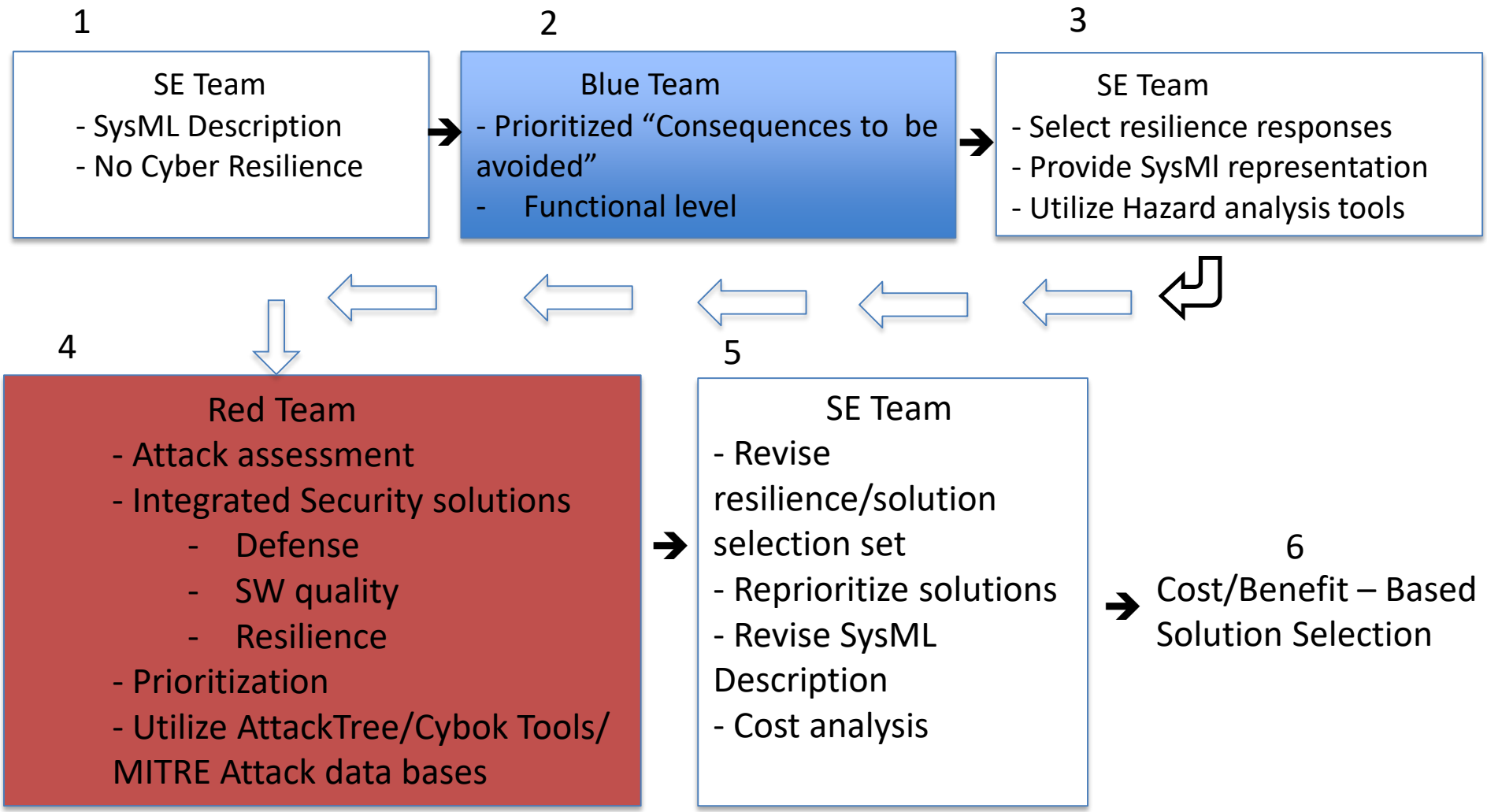
- Confirmed Red Team assessment regarding resilience priority for the communication system indicating that attackers can disrupt the mission in several ways:
  - Change the data in real-time if no encryption is used (supporting use of encryption)
  - Denial of Service
  - Possibly move laterally to violate the behavior of other coupled systems

SE Methodology Use Case (Step 5 of 6)- SE Team Integration of Results

- SE team produces SysMl representation of the various cybersecurity design options derived through the risk-based methodology

- SE team initiates a cost analysis related to each of the cybersecurity solution options (not part of this research effort)

6 Part Iterative Process



POTENTIAL OPERATIONAL TEST AND EVALUATION COMMUNITY ROLES

Managing Reusable Design Patterns and Corresponding Reusable T&E Patterns (1 of 2)

- The acquisition and lifecycle support communities will be addressing cyber resiliency for multiple systems concurrently
- Especially in the early stages of addressing cyber resiliency, valuable efficiencies and knowledge transfers could be achieved through a centralized process addressing reuse
- The OT&E community can potentially serve in this role, given that their workforce will be engaged in critical system evaluations and test

Managing Reusable Design Patterns and Corresponding Reusable T&E Patterns (2 of 2)

- The DoD can establish a format for documenting reusable design patterns (as is done in the open source community) and for operational procedures/training
- The OT&E community can be the responsible agent for creating the collection of design patterns
- The acquisition and lifecycle support communities can provide needed inputs to the OT&E collection of designs and experiences that had important influence on designs
- This information can be utilized by the OT&E community to establish a format for documenting reusable T&E patterns for use in helping SPO's plan for their T&E test requirements, and for reuse of data collection and analysis tools

Implications To OT&E Community

- Need to build up expert workforce regarding cybersecurity and resilience
- Need to participate in program resilience planning activities during early stages of development
  - Risk-based prioritization in selecting resilience requirements
  - Development of operational procedures/training
  - Planning and supporting OT&E

GETTING STARTED

Getting Started

Recognizing the opportunity and the lack of maturity regarding development of cyber resilience solutions:

- Need to start the process through early adopter system developments
- Early adopter system solutions should be selected for both their early value and their simplicity, so as to support the required design, test and evaluation learning curves
- A “small team” oriented management process needs to be established to provide:
  - rapid responses and flexibility while learning
  - information distribution regarding outcomes

UVA Publications (1 of 3)

Journal Articles

1. I. Kim, C. Gay, B.M. Horowitz, P. Bobko, J, Elshaw, Operator suspicion and human-machine team performance under mission scenarios of unmanned ground vehicle operation, IEEE Access, To appear December 2019
2. B. Carter, S. Adams, G, Bakirtzis, T. Sherburne, P. Beling, B. Horowitz, C. Fleming, A preliminary design phase security methodology for cyber-physical systems, Systems 2019, 7(2), 21, April 2019
3. Y. Y. Haimes, B. M. Horowitz, Z. Guo, E. Andrijcic, and J. Bogdanor, Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems, Systems Engineering, 18(3), 284-299, 2015
4. R. A. Jones, B. Luckett, P. Beling, B. M. Horowitz, Architectural Scoring Framework for the Creation and Evaluation of System-Aware Cyber Security Solutions, Journal of Environmental Systems and Decisions 33, no. 3 (2013): 341-361
5. B. M. Horowtiz and K. M. Pierce, The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems, Systems Engineering, vol 16, Issue 4 (2013): 401-412
6. R. A. Jones and B. M. Horowitz, A system-aware cyber security architecture, Systems Engineering, Volume 15, No. 2 (2012), 224-240.
7. J. L. Bayuk and B. M. Horowitz, An architectural systems engineering methodology for addressing cyber security, Systems Engineering 14 (2011), 294-304

UVA Publications (2 of 3)

Conference Proceeding Articles

1. G. Bakirtzis, B. Simon, C. Fleming, and C. Elks. Looking for a Black Cat in a Dark Room: Security Visualization for Cyber-Physical System Design and Analysis, IEEE Symposium on Visualization for Cyber Security (VizSec), Berlin, Germany, (2018)
2. S. Adams, B. Carter, C. Fleming, P.A. Beling. Selecting System Specific Cyber-Security Attack Patterns using Topic Modeling, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18), New York, NY, (2018)
3. B. T. Carter, G. Bakirtzis, C. R. Elks, C. H. Fleming, A systems approach for eliciting mission-centric security requirements. 2018 Annual IEEE International Systems Conference (SysCon), Vancouver, Canada (2018). Best Student Paper Finalist
4. G. Bakirtzis, B. T. Carter, C. R. Elks, C. H. Fleming, A model-based approach to security analysis for cyber-physical systems. 2018 Annual IEEE International Systems Conference (SysCon), Vancouver, Canada (2018)
5. C. Gay, B. Horowitz, P. Bobko, J. Elshaw, I. Kim, Operator Suspicion and Decision Responses to Cyber-Attacks on Unmanned Ground Vehicle Systems, HFES 2017 International Annual Meeting, Austin, TX (2017)
6. G. L. Babineau, R. A. Jones, and B. M. Horowitz, A system-aware cyber security method for shipboard control systems with a method described to evaluate cyber security solutions, 2012 IEEE International Conference on Technologies for Homeland Security (HST), 2012
7. R.A. Jones, T.V. Nguyen, and B.M. Horowitz, System-Aware security for nuclear power systems, 2011 IEEE International Conference on Technologies for Homeland Security (HST), 2011, pp. 224-229

UVA Publications (3 of 3)

Magazine Articles

B.M. Horowitz, AFCEA SIGNAL – Cybersecurity for Unmanned Aerial Vehicle Missions, April 2016 (pp40-43)

B.M. Horowitz, D. Scott Lucero – INCOSE INSIGHT, System-Aware Cybersecurity: A Systems Engineering Approach for Enhancing Cybersecurity, July 2016