System-Aware Cybersecurity Technology, Human Factors, Model-based Analysis and Education Needs

Sponsor: DASD(SE)

By
Barry M. Horowitz

9th Annual SERC Sponsor Research Review
November 8, 2017
FHI 360 CONFERENCE CENTER
1825 Connecticut Avenue NW, 8th Floor
Washington, DC 20009

www.sercuarc.org

Resilience in Highly Automated (Autonomous) Physical Systems

SYSTEMS ENGINEERING RESEARCH CENTER

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), including cyber attack threats of a malicious and unexpected nature.
- In addition, resilience includes post-attack forensic support based upon the data collected for addressing anomalies.

Black Text: C.G. Rieger, Idaho National Labs

Red Text: B.M. Horowitz, UVA

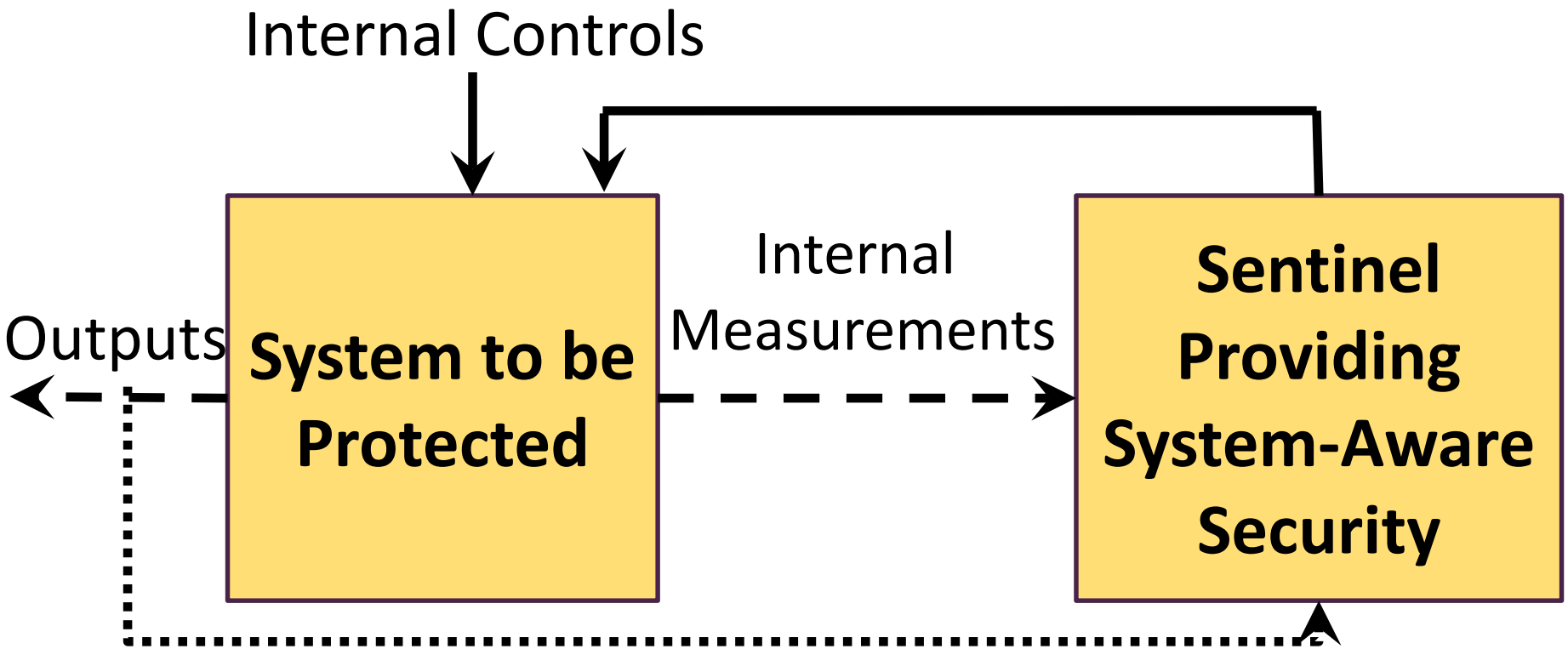
TECHNOLOGY

SYSTEMS ENGINEERING RESEARCH CENTER

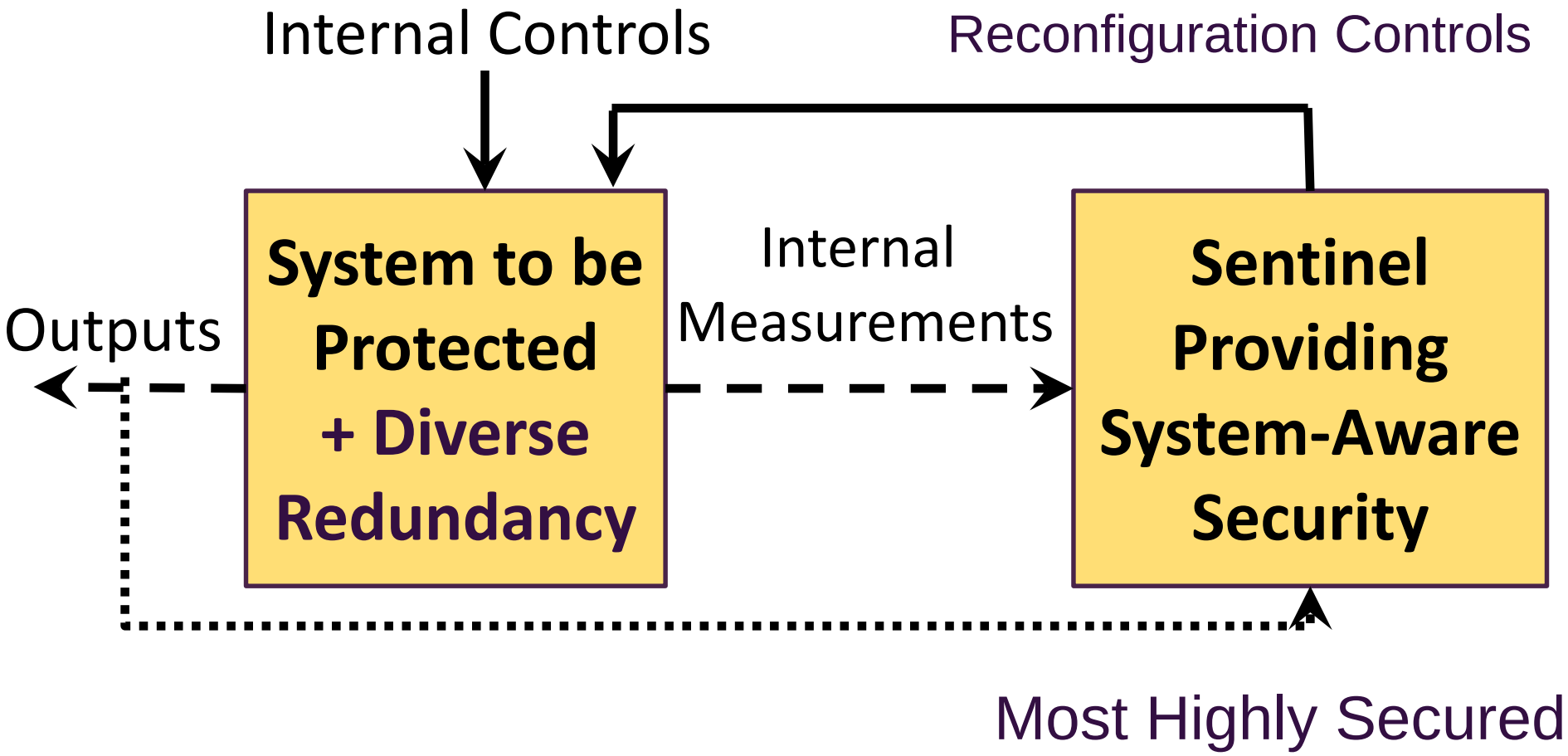
System-Aware Cybersecurity

- Adds layer of security to protect physical system control functions through resilience mechanisms
- Monitor for illogical system behavior and, upon detection, reconfigures for continuous operation
- Builds on cybersecurity, fault tolerant and automatic control technologies
- Monitoring/reconfiguring accomplished through a highly secured Sentinel(s), employing many more security features to protect the Sentinel(s) than the system being protected can practically employ
- Addresses not only network-based and perimeter attacks, but also insider and supply chain attacks
- Employs reusable monitoring and system reconfiguration design patterns to enable more economical solution development
- **Selection of solutions to actually employ based upon model-based analysis including, for example, system modeling tools (SysML), and cyber attack tree tools (SecurITree).**

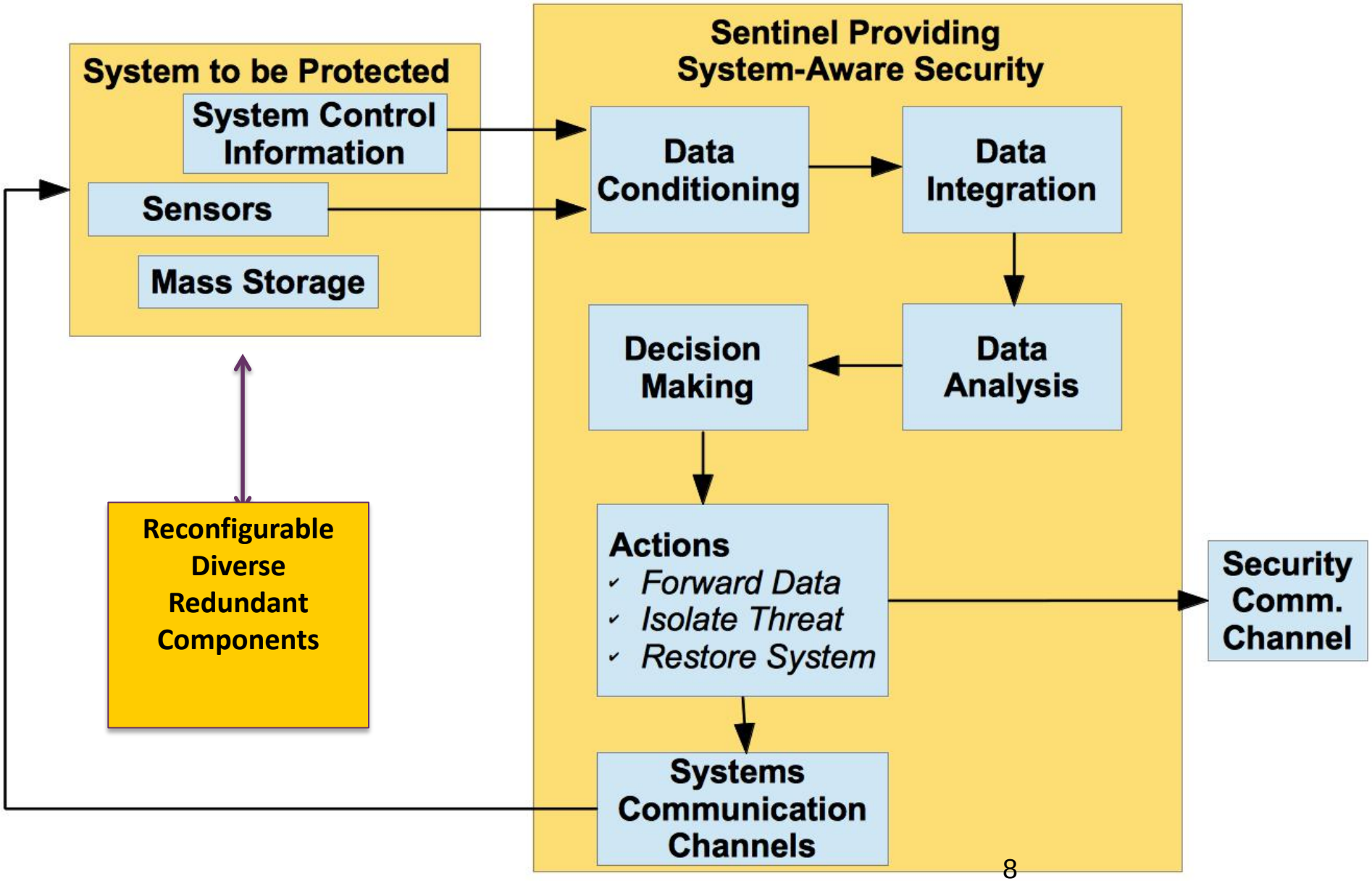
High Level Architectural Overview



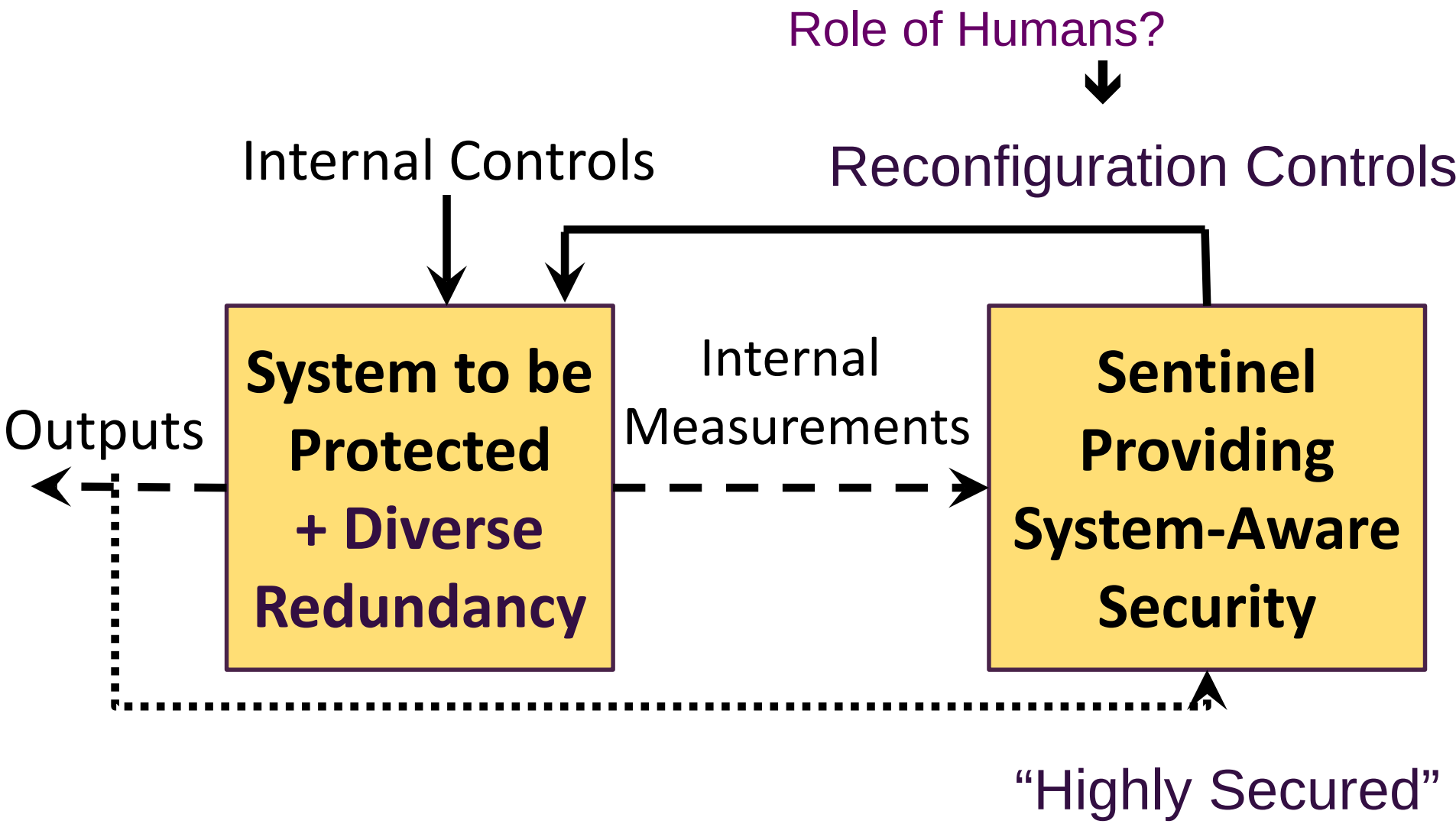
High Level Architectural Overview



Sentinel Data Flow



High Level Architectural Overview



Critical Factors in 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 require confident operators who are trained to react to unprecedented cyber attack events**
  - We have no experience or expectations 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

UVA led Prototyping Based Research Efforts

- Prototypes include developing potential attacks and corresponding resilience-based Sentinel solutions
- Prototype-based explorations include:
  - UAV's (OSD/USAF)
  - Automobiles (Virginia State Police Cars)
  - 3D Printers (NIST)
  - Ship Physical Plant Control System (Northrop)
  - 2 Weapon Systems (Armament R&D Engineering Center at Picatinny Arsenal)

Examples of Illogical System 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
- Through exploitation of on-ship commercial message switches, inconsistent data to and control inputs from operators
- Mode of Fire Control System changed, but no touch screen input from operator

SYSTEMS ENGINEERING RESEARCH CENTER

UAV Prototype

- Live flight tests in December 2014
- Multiple attacks/detections/responses
  - —Waypoint changes
  - —Camera pointing control
  - —GPS navigation errors
  - —Changes to meta data that supports ground-based video interpretation
- Secure Sentinel
  - —Triple diverse redundancy – Computer HW/Operating Systems/ Monitoring SW for monitoring
  - —Configuration hopping
  - —Monitoring both the airborne and ground-based subsystems for continuity
- Accomplished within power, cooling and physical footprint of an Outlaw UAV carrying video cameras and small phased array radar (currently implemented within a 3”cube) 13

Sample of Prototyped Reusable Design Patterns

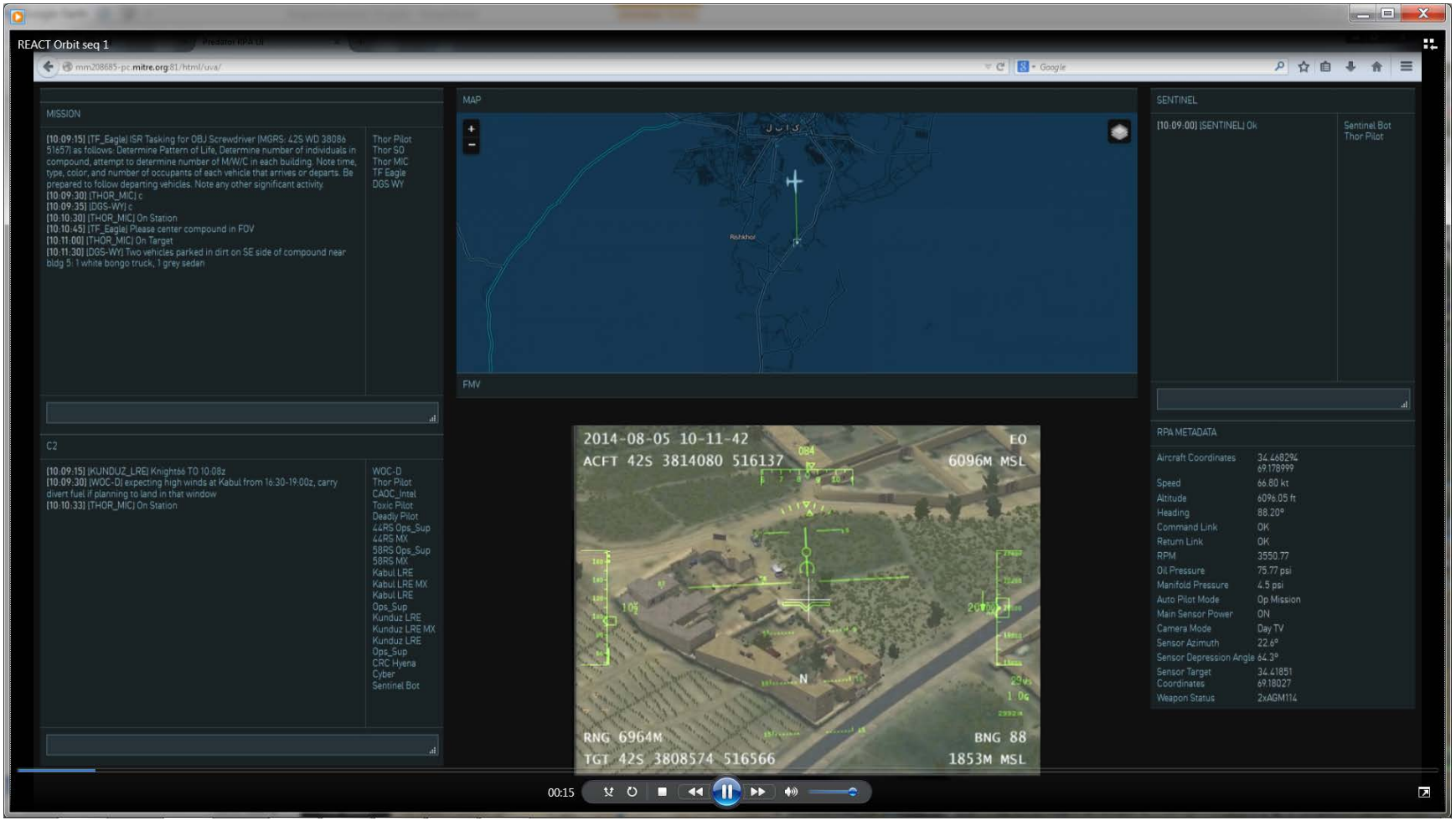
- **Diverse Redundancy** for post-attack restoration
- **Diverse Redundancy + Verifiable Voting** for trans-attack attack deflection
- **Physical Configuration Hopping** for moving target defense
- **Virtual Configuration Hopping** for moving target defense
- **Data Consistency Checking** for data integrity and operator display protection
- **Parameter Assurance** for parameter controlled SW functions
- **Doctrinal Assurance Checking** for critical decisions

HUMAN FACTORS

Post-UAV Flight Test Consideration of Human Factors

- How will the military services feel about totally automated resilience-based system reconfigurations?
- Joint UVA/MITRE simulation-based experiments at Creech AFB.
- Simulated Environment:
  - UAV surveillance of an area that included an unmanned military storage facility
  - Ground-vehicle based physical attack to deplete stored materials, coupled with a cyber attack to disrupt UAV-based detection of the attack

Creech AFB Desk Top Simulation Online User Interfaces/Video Capture



MITRE Corporation REACT Simulation Vehicle

Creech AFB Results - Feedback from 8 Pilots

- The involved pilots and the interviewed 432nd Wing leaders were not aware of any other initiative that was addressing UAV-related cyber attack responses 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 wrong assumption that there was some unknown, maintenance-related physical anomaly
- Operator involvement is required in order to gain a situation-specific related context for resilience-related decision-making
- Identified cyber attacks would likely result in immediate Return To Base responses unless Sentinel-like technology could provide assurances that critical systems are protected
- If a Sentinel reports a cyber event and helps to 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
- Timing of the needed response is important – react quickly if needed, vs being more considerate about a decision
- Would like ability to immediately access a cyber person…wouldn't know who to call…expertise not at the unit
- What about other UAV's in the hanger?

How to Define, Quantify, & Improve Human-Machine Team (HMT) Resilience-related Performance?

- Initiated research activity, with Air Force Institute of Technology (AFIT) as a partner, that:
  - Addressed the handling of situation awareness discrepancies between Human and Sentinel (including Sentinel missed detections & false alarms)
  - Aimed at supporting development of operator selection and training processes that account for the impact of human traits (suspicion levels, risk-taking orientation, improvising orientation) on HMT performance

Accounting for Human Traits in Operator Selection and Training:

Does Suspicion Matter?

Suspicion

- Prior AF research activity to characterize a person's level of suspicion on a Likert Scale (1-7)
  - —Concern related to uncertainty
  - —Concern related to potential for malicious intent
  - —Cognitive activity level
- Question 1: How does suspicion effect human-machine team (HMT) performance?
- Question 2: How do potential consequences effect the relationship between suspicion and HMT performance?
- Do we prefer more or less suspicious operators?
- Do we prefer autonomous Sentinels or human-in-the –loop or conditionally-based integration of the human?

Emulation-based Experiments at WPAFB

- Remote controlled truck experiments
- Experiments involving 32 airmen, measuring
  - Perceived uncertainty, malicious intent, and suspicion
  - Perceived task workload and seriousness of attack consequences
  - System decision support performance including human decision-making time
- 256 individual experiments - 8 experiments for each airman, including scenarios ranging from US-based training mission to Middle East-based conflict situation, including cases of cyber attacks and no attack, Sentinel missed detections and false alarms

SYSTEMS ENGINEERING RESEARCH CENTER

Findings Related to Roles and Selection of Operators

- Based upon use of a project-based, operation-specific, expert judgment scoring system, HMT performance was worse for more suspicious operators
- Sentinel alerts served as a catalyst for wider spread information searches by the operator, whose results led to increases in operator suspicion and increased response times.
- For certain attacks response time can be critical; for others less so. Sentinel forecasting related to acceptable response times has not been considered in our research activity to-date.
- Increases in the perceived potential consequences of attacks increased suspicion levels, which reduced performance and in turn, increased response times

SYSTEMS ENGINEERING RESEARCH CENTER

How to Define, Quantify, & Improve Human-Machine Team (HMT) Resilience-related Performance?

- Need follow-on research that extends the UVA research activity that has:
  - Addressed the handling of situation awareness discrepancies between Human and Sentinel (including Sentinel missed detections & false alarms)
  - Addressed development of operator selection and training processes that account for the impact of human traits (suspicion levels, risk-taking orientation, improvising orientation) on HMT performance
- Need new research initiatives that support:
  - Real-time interactive HMT design development
  - Development of adaptive HMT designs that address Human and Sentinel learning patterns
- Important to recognize that the human roles in addressing non-cyber attack related out-of-norm situations in autonomous physical systems are very closely related to the cyber attack research topics

MODEL-BASED ANALYSIS

Choosing Solutions for Improving Cybersecurity

- Recognize defense (attack prevention) and resilience (sufficiently timed technical or operational system reconfiguration responses to detected successful attacks, so as to minimize consequences) as complementary solutions regarding disruption of important physical system functions
  - Defense – Selected when the important disruptions that are prevented can occur through attacks that exploit specific SW & admin process vulnerabilities (requires knowledge of the SW and admin system designs and implementations)
  - Resilience – Selected based upon attack consequences and cost/complexities of reconfiguration (requires knowledge of the function-related system technical architecture and corresponding operational procedures)

- For a given system function:
  - Favor defense for cases where attack surfaces are sufficiently bounded, potential new attacks are related (derivatives of historical attacks), and solutions are considered to be cost effective
  - Favor resilience when attack surface is considered as too broad to defend and system reconfiguration is considered to be cost and operationally effective

Model-based Research Regarding Solution Selections

- UVA-led research team including Army, SEI, VCU as actively engaged partners
- Mission-based (System-of-Systems)
- UVA led decision-support tool process including:
  - War Room, providing operational judgments regarding consequences of attacks
  - Threat methodology development, including historical attack considerations and other factors
  - Potential combined defense/resilience solutions
  - System Description model(SysML-based)/ Attack Tree model (SecurITree) addressing attack consequences with and without resilience solutions
  - Development of algorithms that could supported prioritization of solutions
  - Army selected hypothetical weapon system use case to support research
- Solution selection will require multi-discipline Industry and government teams with expertise in military ops, cybersec, electro-mechanical systems, and model-based engineering

SUPPORTING EDUCATION NEEDS

Education Related to Resilient System Design

- There is a significant shortage of people with the required broad set of skills and the integrated view required to achieve and properly prioritize resiliency solutions
- Given shortage of sufficiently skilled people, creating education programs by using internal in-house government and industry people will face obstacles relative to use of those people on projects
- UVA and GaTech have conducted a DoD-sponsored study of academic programs and industry/academia – based laboratory designs that, if used as building blocks for development of new academia-developed educational programs, can serve as a basis for addressing the skill shortages of the needed work forces.
- In addition, at DIA's request, UVA has recently developed, and is delivering,, a professional education program focused on cyber attack resiliency for cyber physical systems – Exposes students to the operational, technology and tool-based analysis capabilities that are critical to developing effective resiliency solutions, including hands-on laboratory activities

SYSTEMS ENGINEERING RESEARCH CENTER

Gaining Academia's Interest

- Critical factors in accelerating academia's interest in becoming a strong force in addressing this need are;

1)DoD/Industry demand for academic institutions to provide resilience-focused programs for multiple student categories, and

2) Academia's readiness to create cross-department programs that bring together knowledge about cybersecurity, electro-mechanical system design, and resilience-related technologies, and

3) Industry/government willingness to share sensitive data regarding system designs with academia

Conclusions

- There is a need and opportunity for resilience-based solutions related to cyber attacks on physical systems
- The need exists to address not only technology, but also human factors, model-based analysis and educational programs as critical path items to moving resilience solutions forward
- Need to take a broad view regarding the importance of all of these requirements and develop paths for addressing them