A Few Words First

Courtesy – Please mute your phone (*6 toggle).

Upcoming Meetings:

- **Jan 20-23, INCOSE International Workshop, Jacksonville, FL.**
- **Jan 21, FREE SEP Certification Exam at IW18 – sign up on registration page**
- **Feb 14, MBSE Implementation Across Diverse Domains**
  Dr. Ron Carson, Seattle Pacific University, Adjunct Professor
- **Mar 14: Systems Engineering Transformation**
  Troy Peterson, System Strategy, VP; Director INCOSE's Transformation Initiative

CSEP Courses by *Certification Training International:*
Course details | Course brochure
Upcoming Course Schedule (close by, but many more locations and dates):
2018 Feb 26-Mar 02 | Las Vegas, NV
2018 Apr 02-Apr 06 | Denver, CO
2018 May 21-May 25 | Austin, TX
2018 Oct 15-Oct 19 | Albuquerque, NM
Chapter SEP mentors: Ann Hodges alhodge@sandia.gov, Heidi Hahn hahn@lanl.gov

First slide, not recorded but retained in pdf presentation.

And Now - Introductions

Enchantment Chapter Monthly Meeting

10 January 2018 – 4:45-6:00 pm:

Cybersecurity for Highly Automated Physical Systems
"System Aware Cybersecurity"

Dr. Barry Horowitz, University of Virginia, bh8e@eservices.virginia.edu

Abstract: As exemplified in the 2010 Stuxnet attack, it is well recognized that cyber attackers can embed infections in electronic equipment that result in disruptions to the operation of mission critical cyber-physical systems. To combat this threat, a new set of resilience-based cybersecurity solutions is proposed to enhance the security of systems by complementing existing defense-oriented security solutions. These resilience solutions are intended to sustain the operation of critical system functions that have been successfully attacked. Cybersecurity solutions of this type must take into account the specifics of how the system being protected operates, leading to identifying the potential solutions as System Aware Cybersecurity. Based upon a series of results derived from research efforts initiated in 2010, this presentation discusses the opportunity to develop a generally applicable *Smart Sentinel* platform to facilitate the integration of reusable resilience design patterns that protect critical system functions from high risk cyber attacks. Based upon experience and specific results gained from a series of prototype-based operationally oriented technology experiments, the presentation will highlight the critical path importance of coupling research addressing human factors and system-level, model-based solution evaluation tools, to technology-focused research activities.

Download slides today-only from GlobalMeetSeven file library or anytime from the Library at www.incose.org/enchantment

NOTE: This meeting will be recorded

Today's Presentation

Things to Think About

How can this be applied in your work environment?

What did you hear that will influence your thinking?

What is your take away from this presentation?

Speaker Bio

Dr. Horowitz joined the University of Virginia's faculty as a Professor in the Systems and Information Engineering Department in September 2001, after an industrial career involving the application of systems engineering to many large and complex systems. He served in the role of Department Chair from 2009 -2017.

Since 2010 he has been leading research efforts on a systems engineering approach for addressing cyber security through resiliency solutions. From 1969 through 1996 he was employed in a variety of positions at the MITRE Corporation, including serving as President and CEO.

In 2014, Horowitz was appointed by the Governor of Virginia to serve for a 2-year period as a Commissioner for Cybersecurity, leading an economic development working group within the Commonwealth to create new initiatives that couple cyber security and physical systems.

In 1996 Dr Horowitz was elected into the National Academy of Engineering. Early in his career he led an FAA sponsored prototyping-based research effort at MITRE that resulted in the initial flight tests for what eventually became the internationally adopted airborne collision avoidance system, TCAS. For his efforts during Desert Storm, resulting in a systems integration solution for detecting and destroying Scud missile carriers, he received the Air Force's highest award for a civilian.

Dr. Horowitz has served as a member of the Naval Studies Board (NSB), of the National Academy of Science, as a member of General Electric's Academic Software Advisory Panel and is a member of the Cyber Security Advisory Board for the Virginia Joint Commission on Science and Technology (JCOTS). In addition, Dr. Horowitz has served on and led study groups for the NAE, the Defense Science Board and the Army Science Board. Dr. Horowitz received an MSEE and PhD from New York University and a BEE from the City College of New York.

Cybersecurity for Highly Automated Physical Systems

System-Aware Cybersecurity
Barry Horowitz
University of Virginia
January 2018

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 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: Rieger, Gertman, McQuuen, 2009 IEEE Human System Interactions Conference

Red Text: B.M. Horowitz, UVA

System Engineering and Resiliency (1 of 2)

- Systems Engineering
  - Addresses the integration of:
    - Policies
    - Processes (including accounting for human factors)
    - Technology
    - Data collections and analysis
  - So as to create and continuously improve a satisfying system, based upon designs that have been subjected to significant analysis:
    - Mathematical
    - Logical and complete arguments
    - Simulation
    - Prototype trials

System Engineering and Resiliency (2 of 2)

- 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

Some History Related to 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 (dust impacting communications), EW or EMP attacks
  - False alarm attack warning event resulting in bombers being launched for potential nuclear response
  - Bunkers to assure continuity of government and military C2

- Air Traffic Control System
  - Primary/secondary radar systems
  - Parallel runway separation standard for IFR landings
  - 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, operators need special training
- Need accepted analysis methodologies and probably a specialty group for deciding on:
  - The possible anomalies
  - Resilience needs and budget for new systems
  - Adding resilience to legacy systems

Traditional Cybersecurity for Internet-based Information Systems

- Standard cybersecurity approaches are infrastructural in nature: Network protections/System perimeter protections
- Little emphasis on protecting applications within specific information systems
  - Considered as too expensive
  - Too many unique systems and functions to practically deal with
  - Change too fast
  - Too big, distributed and complex
  - Too many suppliers and variable quality
  - Solutions impact user friendliness
  - Costs of financial losses can be absorbed by spreading over large user bases
- As a result, in general, the cybersecurity community does not have experience in securing system application functions, especially physical system control functions
- And system application designers, in general, do not have experience with designing for better cybersecurity, especially physical system designers

Advanced Automation

Rapidly growing initiatives in advanced automation of physical systems (e.g., UAS's, Automated Control of Automobiles, Digital Factories, 3D Printers, Internet of Things)

Business Insider predictions show the overall Defense and Commercial UAV market doubling over the next 10 years, with the commercial UAV market increasing from ~0.5bb in 2014 to over $3bb by 2024

45 million connected cars were produced by 2013, and IDATE predicts this number will increase at a 57% compound annual growth rate to total 420 million by 2018.

Forbes predictions show the 3D Printing market increasing from $1.3BB in 2014 at a compound annual rate of 40 – 50%, to reach over $5bb by 2018.

Siemens in their Pictures of the Future Magazine indicates that on a global basis, advanced automation in manufacturing will have increased by 25% to $200BB in 2015 from $160bb in 2012. In addition, Markets and Markets forecast that smart factories will grow to $67bb in value by 2020, a 6% compounded annual growth rate.

IDATE predicts 80 billion objects will be connected to the Internet by 2020. Many of these objects will be parts of cyber physical systems, ranging from smaller systems (e.g., meters) to larger scale physical systems (e.g., turbines, automobiles).

Logistics, Health Management, Remote Control and Autonomy for Cyber Physical Systems

- Great economic incentive to tie physical systems to the Internet
  - Remote Control and Autonomy: Limited, back-up roles for humans to reduce cost and perhaps achieve other benefits as well
  - Logistics Management – move to multi-factor, use-based maintenance rather than accumulated hours of use only. For example: Temperature, Loads, Continuity of Use
  - Health Management : Dynamically shift machines to maximize profit while addressing a predicted (or actual) failure
- Data collection needs are likely to include measurements embedded in the controllers of cyber physical systems, thereby connecting control to external systems and networks

Opens up new cyber attack possibilities

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 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

SYSTEM AWARE CYBERSECURITY

UVa's "System-Aware Cybersecurity"* for Computer-Controlled Physical Systems

- 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 for implementation based upon model-based analysis including, for example, system modeling tools (SysML), and cyber attack tree tools (SecurITree).

*Sponsored by DoD and the Stevens Institute's Systems Engineering Research Center

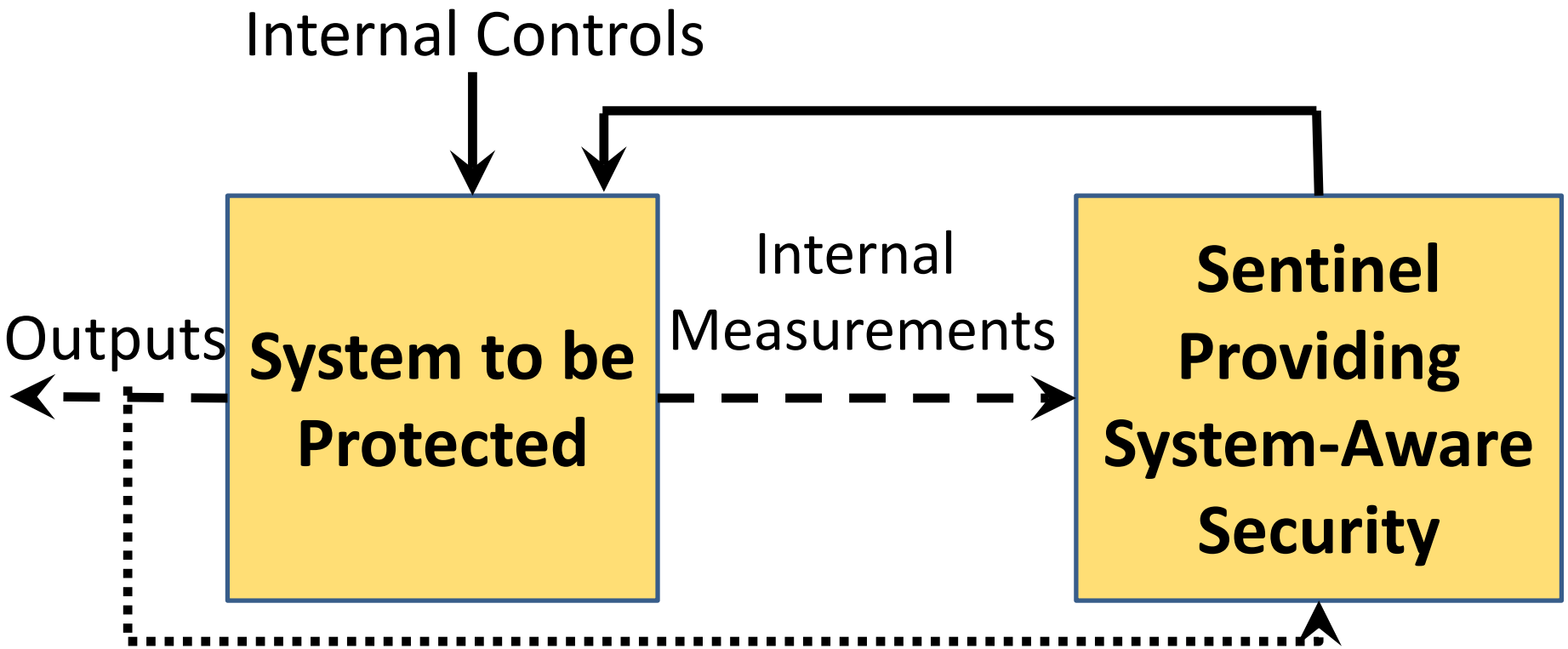
Illustrative Examples of Illogical Control

- Navigation waypoint changed, but no corresponding communication received by UAV
- Automobile sensor shows distance between cars reducing, bur 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

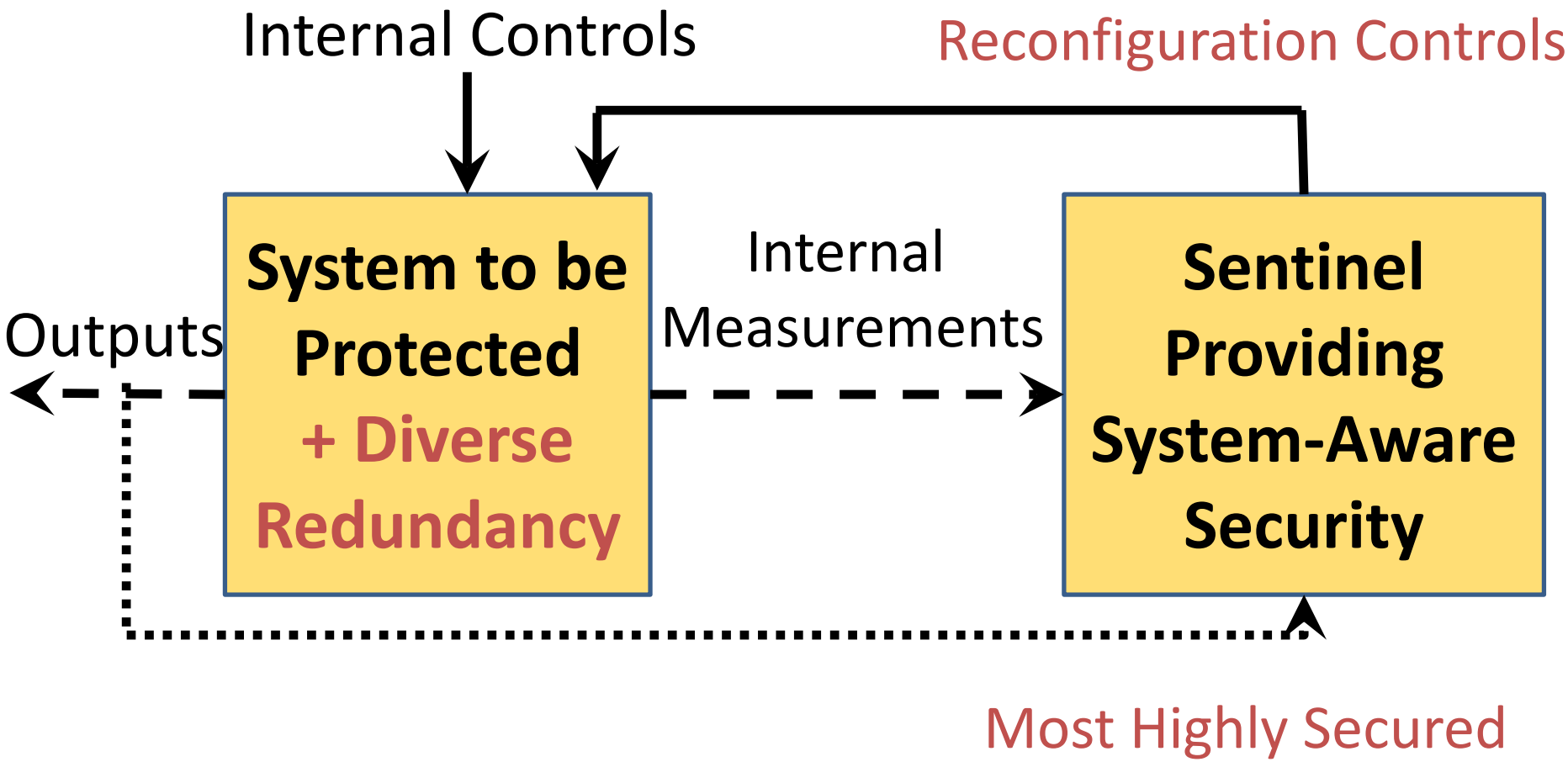
Broad Objective

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

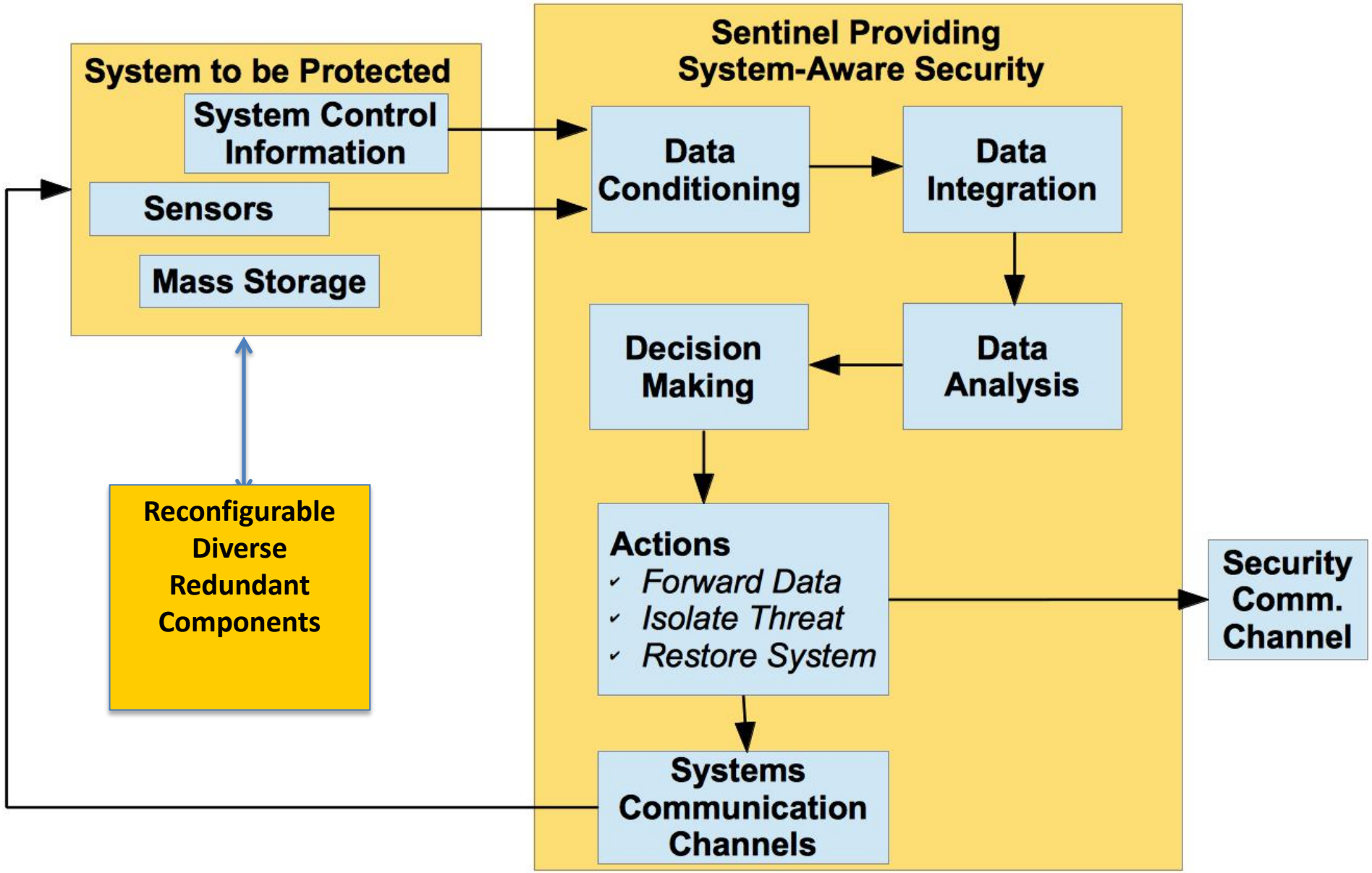
Outputs

Internal Measurements

Sentinel Providing System-Aware Security

Most Highly Secured

Sentinel Data Flow



Operator Inputs

- Pre-Mission Intelligence
- MissIon Specific Factors
- Use of out-of-Sentinel Information

System Disruption Detection → Attack Classification → Disruption Purposes → Operator Presentation

- Parameters
- Displays
- Algorithms
- Data
- Inputs

- Natural HW/SW Failure
- Cyber External
- Cyber Insider
- Cyber Supply Chain

- Disrupt Situation Awareness
- C2 Disruption of Commands
- Mission Planning Disruption
- C2 Delays in Execution

- To Who
- What Info
- What for
- What Method

Sentinel Data Analysis Functions

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)
- The System Aware solution designers need to come from the communities related to system design and system engineering, providing a new orientation to complement the established approaches of the information assurance community

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

* 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
- Develop synchronized, distributed exploits consistent with how the attacked system actually works

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
- Develop synchronized, distributed exploits consistent with how the attacked system actually works
- Corrupt multiple supply chains

Examples of Prototyped 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
- **System Restoration** using diverse redundancy
- **Doctrinal Consistency** for assuring commands are properly coupled to approved operational processes

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

UVA led Prototyping Based Research Efforts

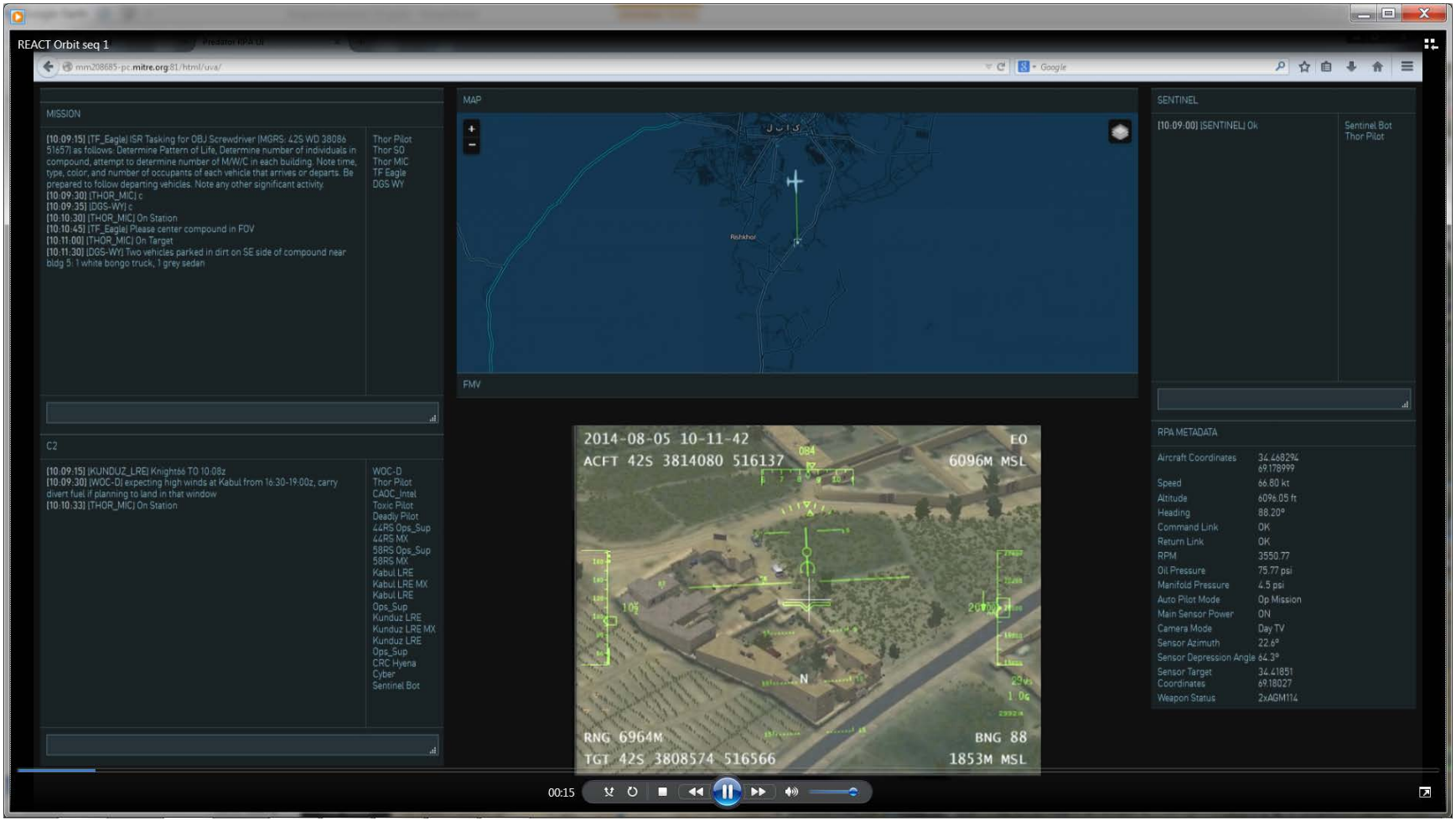
- Prototypes include developing potential attacks and corresponding resilience-based Sentinel solutions
- Prototype-based explorations include:
  - UAV's (OSD/USAF)
  - Automobiles (Virginia State Police Cars)
  - 3D Printers (NIST)
  - Ship Physical Plant Control System (Northrop)
  - 2 Weapon Systems (Armament R&D Engineering Center(ARDEC) at Picatinny Arsenal)
- In FY18 initiated transition effort with Army

HUMAN FACTORS

Initial 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 and Improve Performance of the Human-Machine Team (HMT) for Resilience-Management?

- 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:

Operator Suspicion and Detection/Response to Cyber-Attacks

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)

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 Wright Patterson AFB

- 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

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

How to Define, Quantify and Improve Performance of the HMT for Resilience-Management?

- 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 Cyber Security

- Recognize defense (attack prevention) and resilience (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 operational consequences of attacks 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 Decision Support 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 including expertise in military operations, cybersec, electro-mechanical system design, and model-based systems engineering

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, and model-based analysis as critical path items to moving resilience solutions forward
- Need to take a broad view regarding the importance of each of these requirements and develop paths for addressing them

Today's Presentation

Things to Think About

How can this be applied in your work environment?

What did you hear that will influence your thinking?

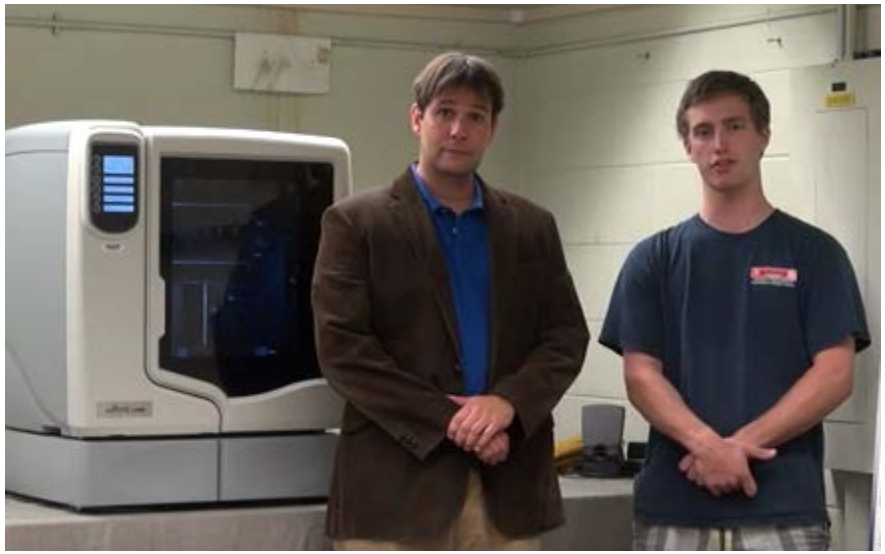
What is your take away from this presentation?

Guest Speakers: Gavin Garner and Bryan Kessel

File6.5

Cyber Security in Additive Manufacturing

Picatinny Arsenal Demo 2015 by University of Virginia Personnel



This is a demonstration of a cyber security hack on a 3D printing machine – and the protection against the hack offered by Sentinel, an independent agent that monitors cyber-physical system behavior.

Video**:** https://www.youtube.com/watch?v=l2nHraDKYD4&feature=youtu.be

Please

The link for the online survey for this meeting is

www.surveymonkey.com/r/2018_01_MeetingEval

www.surveymonkey.com/r/2018_01_MeetingEval

Look in GlobalMeet chat box for cut & paste link.

Slide presentation can be downloaded now/anytime from:

The library page at: www.incose.org/enchantment.

Recording will be there in the library tomorrow.