SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

WELCOME

"How Do We Prepare the People Who Will Need to Manage the Real-time Responses to Cyber Attacks on Physical Systems?"

Dr. Barry Horowitz and Dr. Inki Kim, University of Virginia

August 2, 2017 | 1:00 pm ET

- ❑ Today's session will be recorded.
- ❑ An archive of today's talk will be available at: www.sercuarc.org/serc-talks/
- ❑ Use the Q&A box to queue questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.
- ❑ If you are connected via the dial-in information only, please email questions or comments to Ms. Mimi Marcus at mmarcus@stevens.edu.
- ❑ Any issues? Use the chat feature for any technical difficulties or other comments, or email Ms. Mimi Marcus at mmarcus@stevens.edu.

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, ASD(R&E), nor the SERC.

This material has been approved for public release and unlimited distribution.

Human Factors Related to Cybersecurity for Computer- Controlled Physical Systems

System-Aware Cybersecurity

Barry Horowitz, Inki Kim

University of Virginia

August 2017

Resilience- based Cybersecurity

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: C.G. Rieger, Idaho National Labs

Red Text: B.M. Horowitz, UVA

SYSTEMS ENGINEERING RESEARCH CENTER

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, employing many more security features to protect the Sentinel than the system being protected can practically employ
- Addresses not only network-based attacks, but also insider and supply chain attacks
- Employs reusable monitoring and system reconfiguration design patterns to enable more economical solution development

SYSTEMS ENGINEERING RESEARCH CENTER

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

SYSTEMS ENGINEERING RESEARCH CENTER

Illustrative Examples of Illogical System Control, Based upon Research Prototyping Projects

- 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

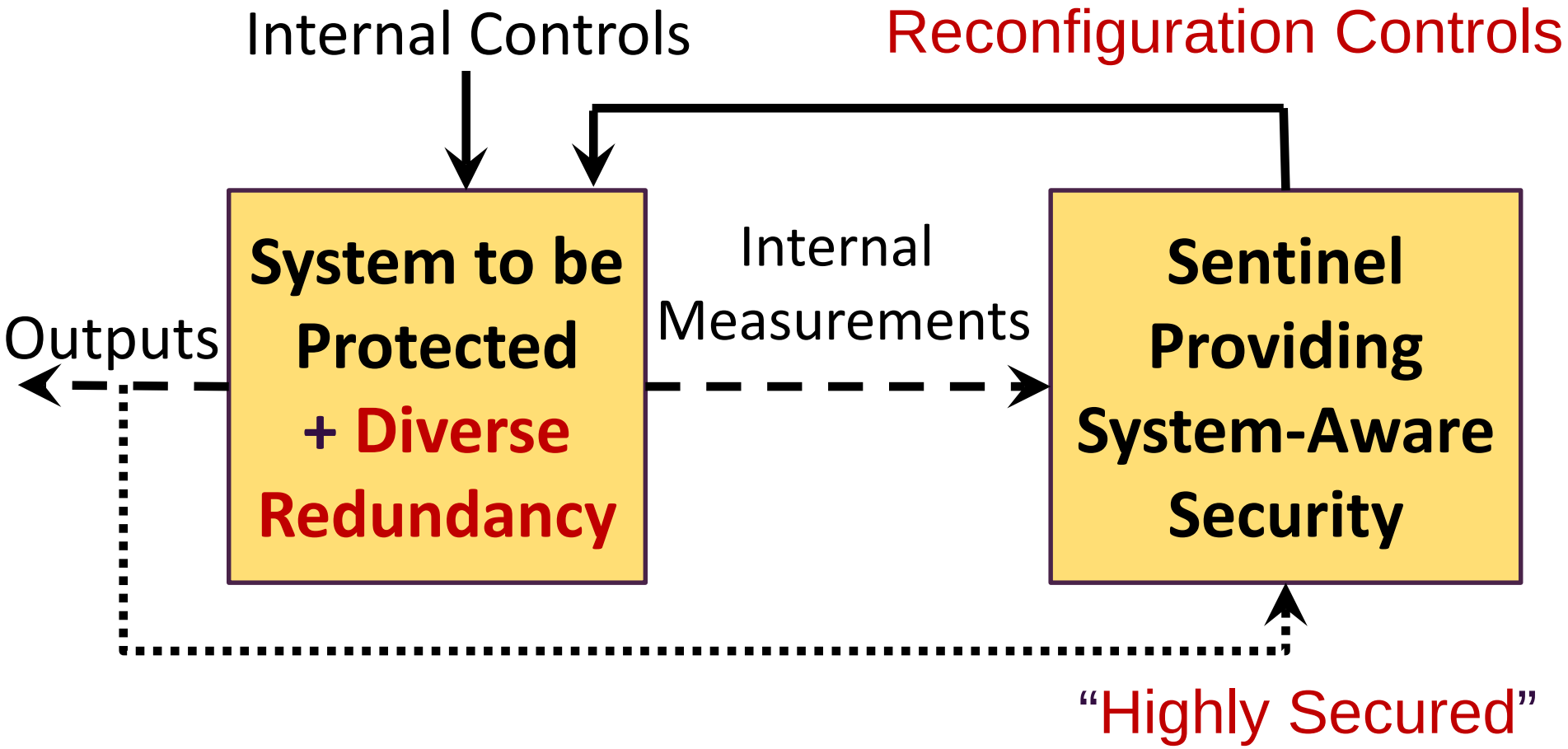
UAV Prototype

- Live flight tests in December 2014
- Multiple attacks/detections/responses
  - Waypoint changes
  - Camera pointing control
  - GPS navigation errors
  - Meta data to support 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)

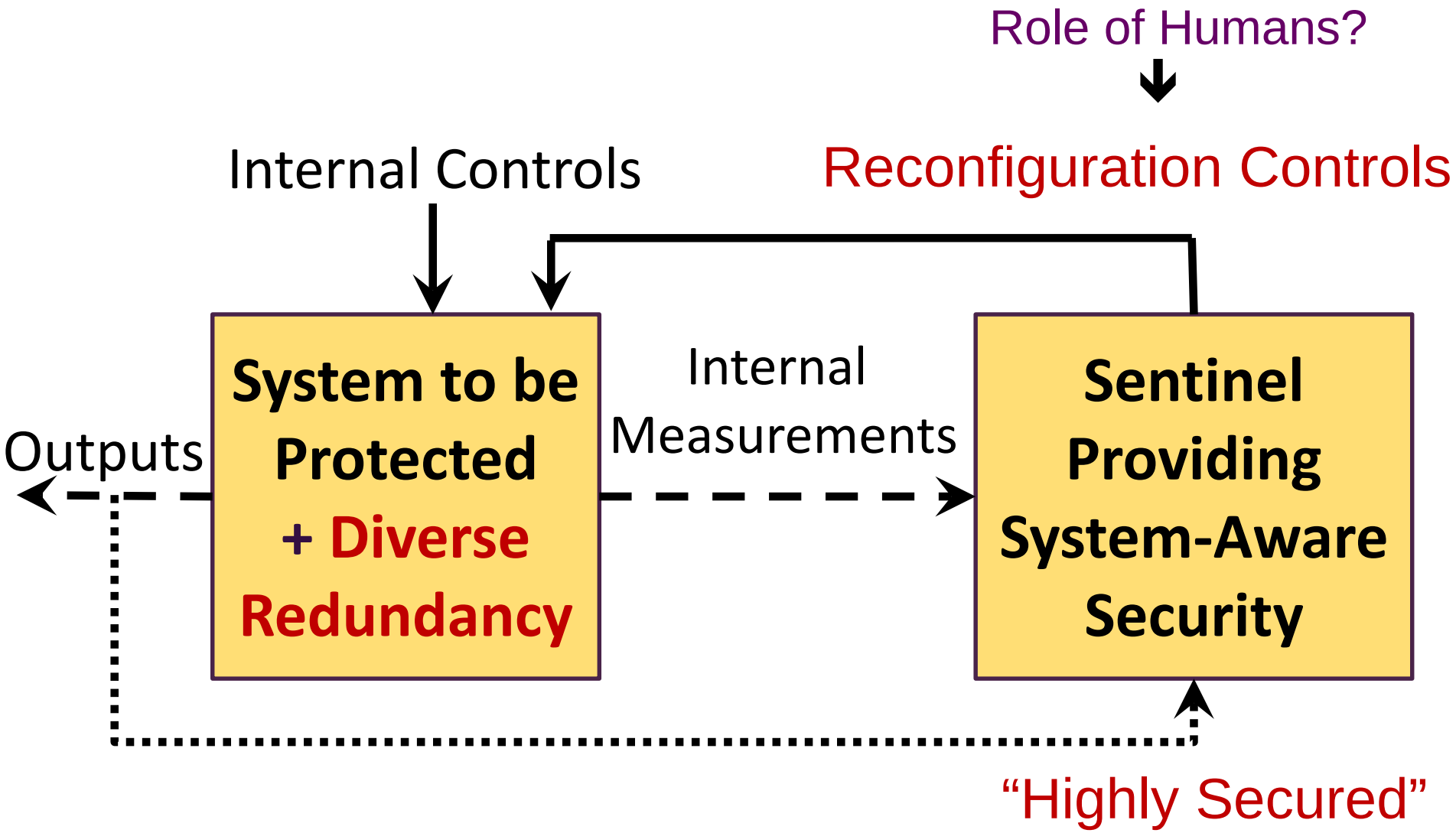
Sample of Prototyped Reusable Design Patterns

- **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

High Level Architectural Overview



High Level Architectural Overview

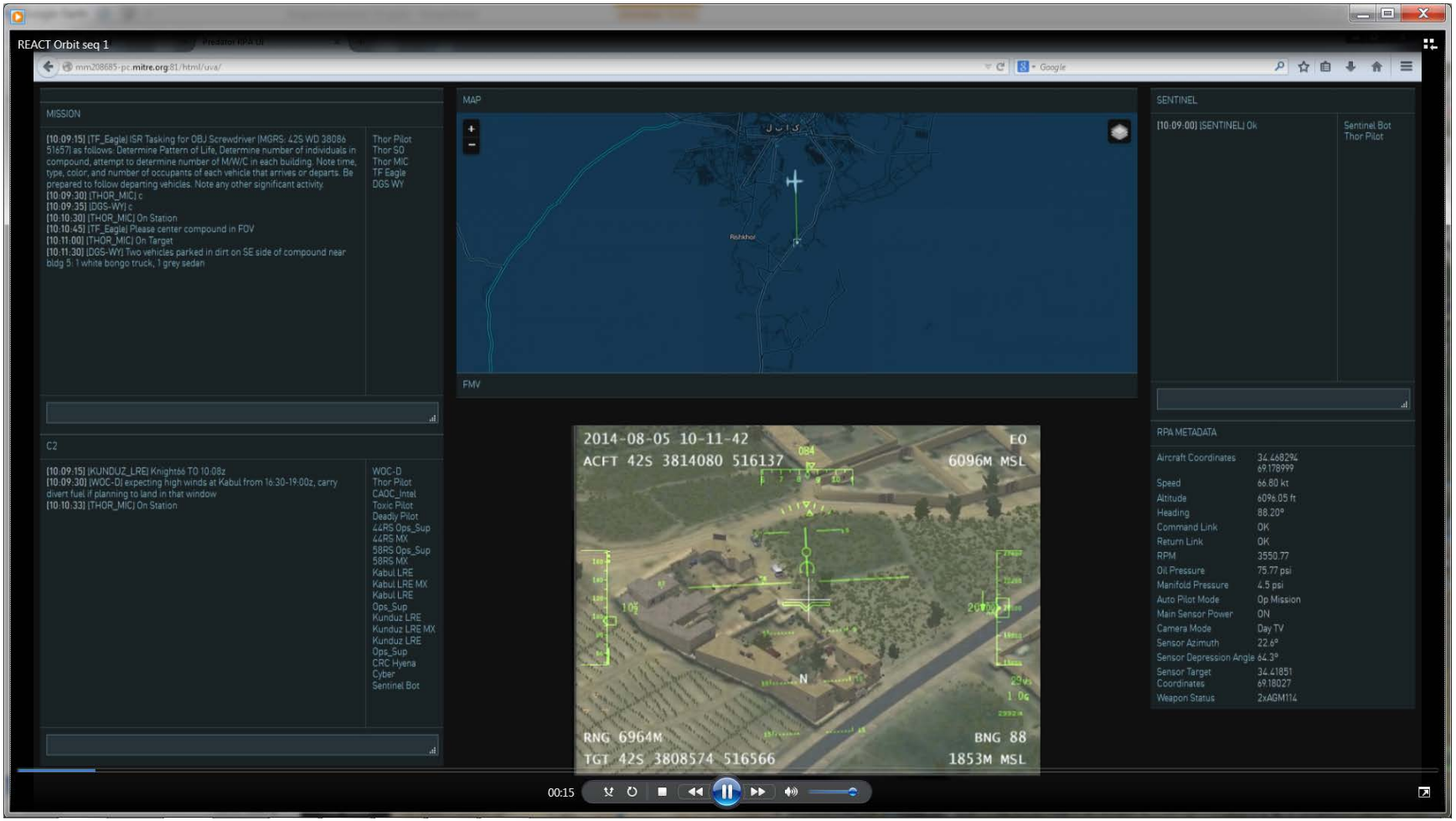


HUMAN FACTORS

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

SYSTEMS ENGINEERING RESEARCH CENTER

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?

SYSTEMS ENGINEERING RESEARCH CENTER

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

- Need research that:
  - Addresses the handling of situation awareness discrepancies between Human and Sentinel (including Sentinel missed detections & false alarms)
  - Supports 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
  - Supports development of adaptive HMT designs that address Human and Sentinel learning patterns
  - Supports real-time interactive HMT design development

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

- Need research that:
  - Addresses the handling of situation awareness discrepancies between Human and Sentinel (including Sentinel missed detections & false alarms)
  - Supports 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
  - Supports development of adaptive HMT designs that address Human and Sentinel learning patterns
  - Supports real-time interactive HMT design development

Accounting for Human Traits in Operator Selection and Training:

Operator Suspicion and Detection/Response to Cyber-Attacks

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?

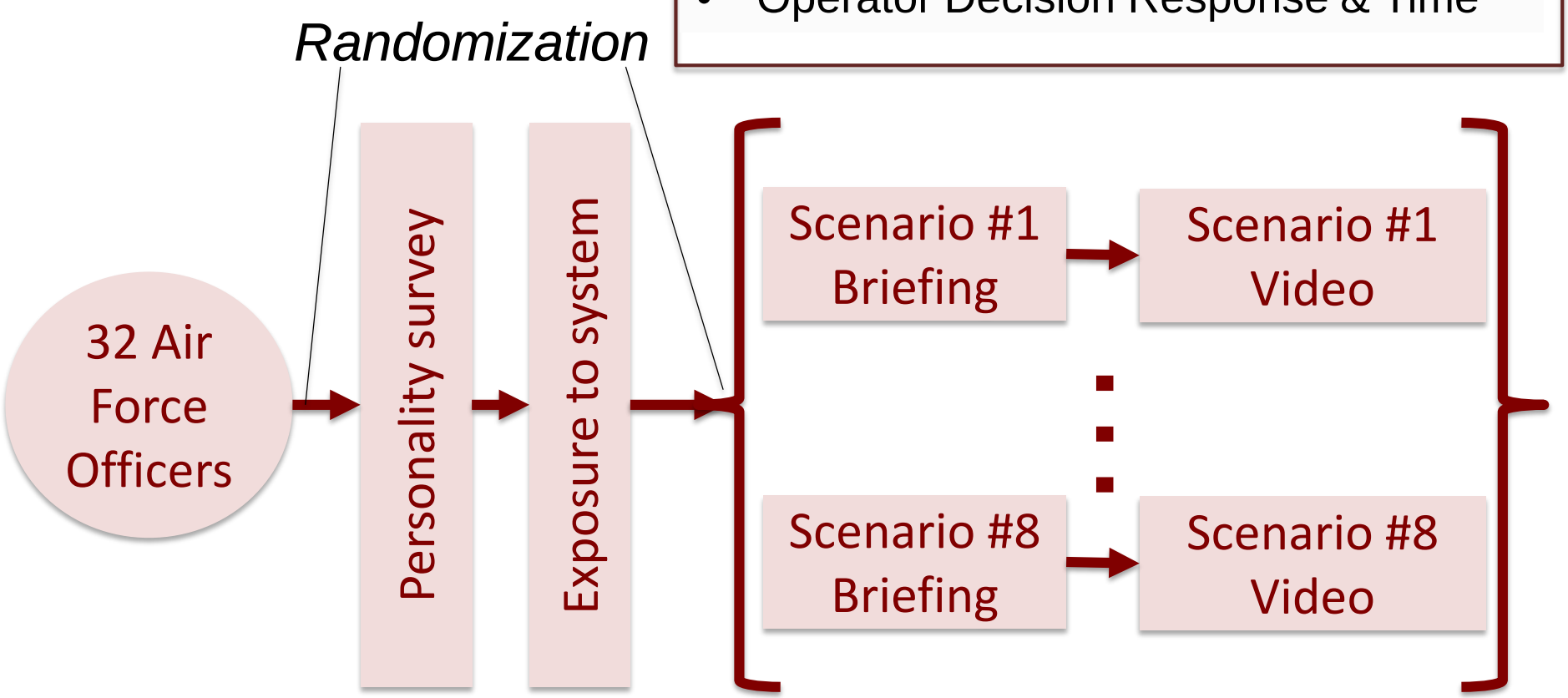
Emulation-based Experiments at Wright Patterson AFB

- 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

Overview of Experimental Design

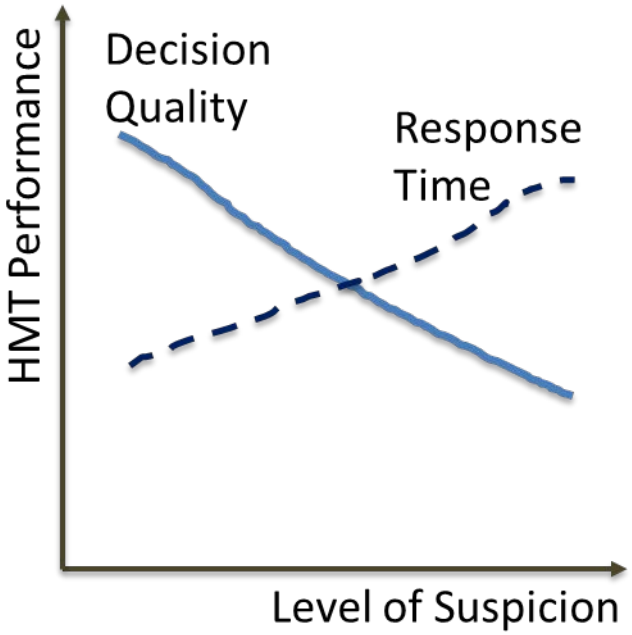
Dependent Variables (DV)

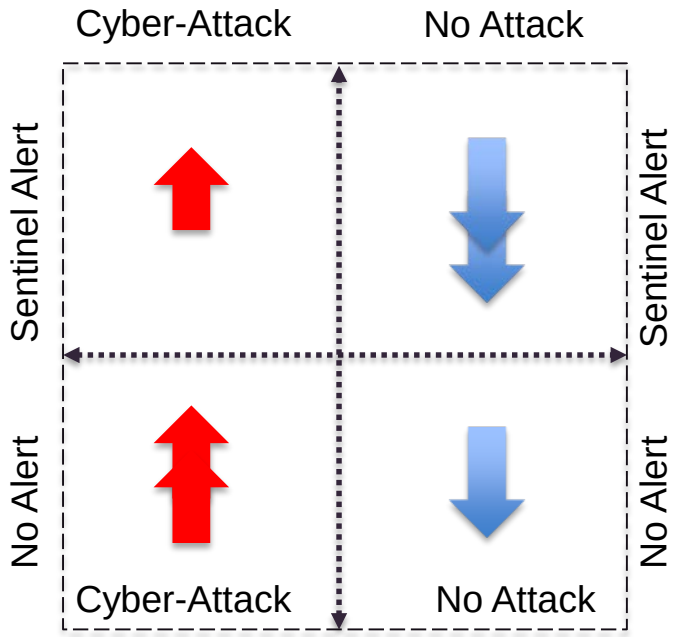
- Mental Workload (NASA-TLX)
- Suspicion Index (13-item survey)
- Operator Decision Response & Time



Findings Related to Roles of Operators

- HMT performance was worse for more suspicious operators, and increases in the perceived consequences of attacks increased suspicion levels
- Sentinel alerts served as a catalyst for wider spread information searches by the operator, whose results led to increases in operator suspicion





Follow-up Research Activities

- Although the level of suspicion is subject to individual differences, an appropriate design of sentinel can significantly influence it:

  → **Eye tracking analysis** at the level of interface elements, combined with suspicion study, is promising to reveal the incremental effects of sentinel design components

- Empirical experiments of abnormal, rare events (i.e. cyber attacks) may create an operator's mental model that deviates from that of reality, in terms of expected "norms" that may have been constructed through experimental runs:

  → **Decision model** that is built to consider task-specific expectations and suspicion can help accurately project an operator's decision and responses into those in reality

SYSTEMS ENGINEERING RESEARCH CENTER

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

Questions?

SERC 2017 Annual Events

REGISTER NOW

For more information or any questions regarding this event, please contact:
Ms. Monica Brito or Ms. Megan Clifford

SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

UPCOMING TOPICS:

Cybersecurity Series

What are the Top Ten Software Security Flaws?

Dr. Gary McGraw, Vice President Security Technology, Synopsys

October 4, 2017 | 1:00 pm ET

TBD

Dr. William Scherlis, Institute for Software Research, Carnegie Mellon University

November 29, 2017 | 1:00 pm ET

Thank you for joining us!

Please check back on the SERC website for today's recording and future SERC Talks information!