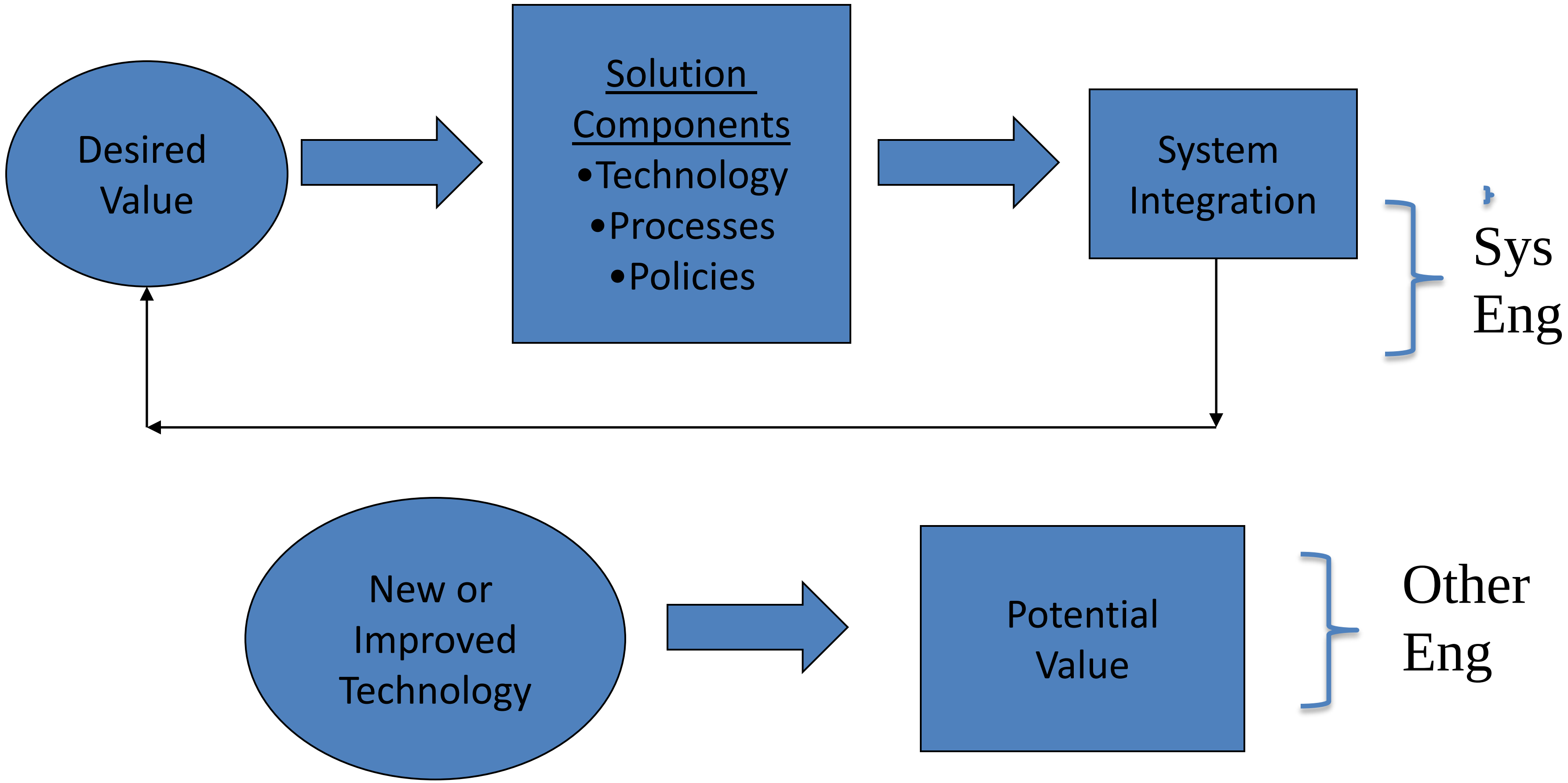
Transitioning System Engineering Research Efforts into Practice

Barry Horowitz

October 2015

Systems Engineering vs Other Engineering Research



Examples of What's Different About SE Research

- Need to address policy/process issues as an early transition activity
- Integrative in nature, so transition requires "platform" partners, as well as policy/process partners
- The specifics of integration may vary from application to application (not a commodity), so no directly repeatable cost or benefit
- The trade-off space varies from application to application
- Issues of scalability: Can have a broad range of what constitutes required scale
- Unlike a new technology component, can't easily compare the new technology to existing components that it would replace or supplement

So How to Transition a SE Innovation

- Integrated early demonstrations of value that address important needs more effectively than current technology research approaches and create integrated learning environment
  - Realistic scenarios integrated with existing systems
  - Operational partners
  - Policy partners
  - Comparison with other possible system approaches
- Need for a cost benefit analysis that recognizes a range of applications (low scale to high scale)
- Need to address evolutionary aspects of the innovation
- Need to make the uncertainties visible and provide a path for addressing uncertainties while making progress

Example: System Aware Cybersecurity

New SE Direction(1): Not Only the Network and Perimeter

- Too Many Penetrations
- Insider Attacks
- Supply Chain Attacks
- Need to Include:
  - Weapon Systems
  - C2 Systems
  - Sensor Systems
  - Logistics Systems
  - Computer Controlled Physical Plant Systems (Engines, Electrical Power, Rudder Control, etc.)
  - Etc.

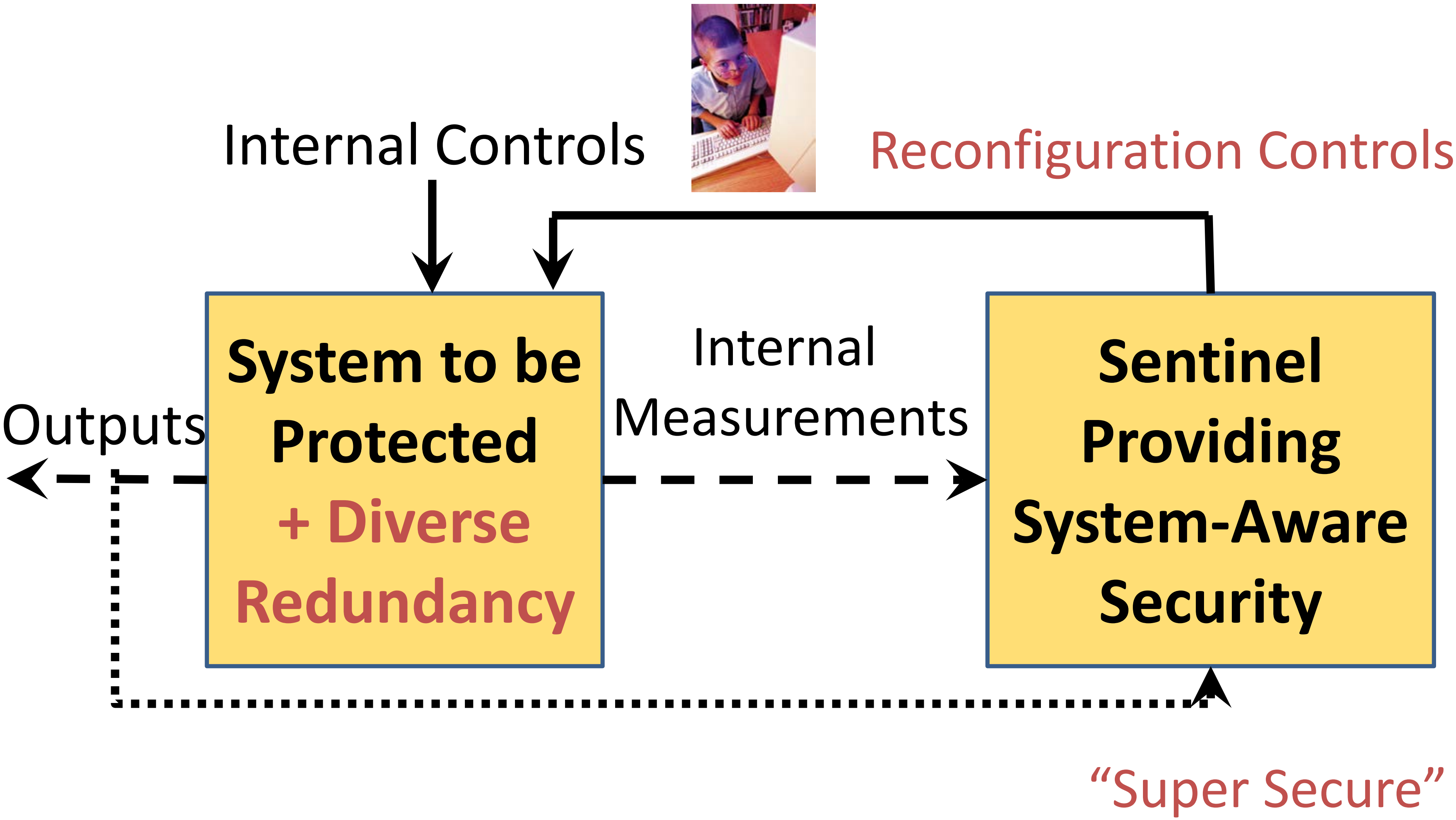
New SE Direction(2): Mission-Based Security Strategy

- Need to make solution designs and decisions on a mission execution basis, rather than limited to a widget or single subsystem basis
  - Attack occurs at Subsystem 1, symptoms appear at Subsystem 2
    - Meta data example
    - Attack initiation example
  - Detecting an attack through system consistency checks
    - Waypoint change example
    - Multiple and diverse sensors

New SE Direction(3): Security Through Monitoring System Functions, Emphasizing Physical Systems

- DoD-funded System Aware Cybersecurity effort
  - December 2014 flight evaluation of protection for an autonomous surveillance system onboard a UAV
  - Defended on-aircraft attacks to prevent specific surveillance operations:
    - Waypoint change
    - Camera Pointing Control
    - GPS information for navigation or camera pointing
    - Image meta data changes

High Level Architectural Overview



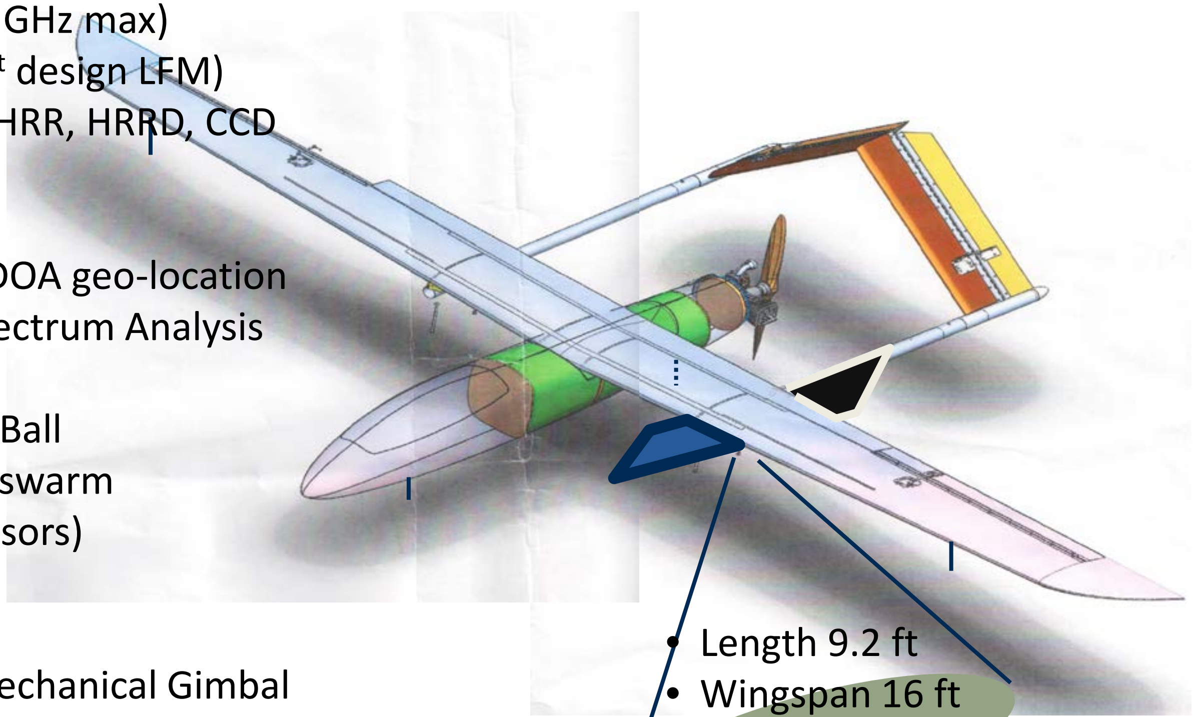
SECURITY FOR AUTONOMOUS SURVEILLANCE SYSTEM ON BOARD A UAV (TECHNOLOGY)

GAUSS– GTRI AIRBORNE UNMANNED SENSOR SYSTEM

FOUR SENSOR OBJECTIVE BASELINE

- Multi-Channel Radar (8 channels)
  - ESA Antenna: 8 phase centers, each 4 x 4 elements
  - X-band, 600 MHz BW (design; 1 GHz max)
  - Arbitrary Waveform Capable (1st design LFM)
  - Acquisition Modes: DMTI, SAR, HRR, HRRD, CCD
- Multi-Channel SIGINT
  - Near 1 and 2 GHz Bands
  - Two orthogonal dipole pairs: TDOA geo-location
  - Ambient Complex-Baseband Spectrum Analysis
  - Signal Copy Selected Sub-Bands
- Gimbaled, Stabilized EO/IR Camera Ball
- High Precision GPS & INS (eventual swarm capable inter-UAV coherent RF sensors)

Modified Griffon Aerospace Outlaw (MQ-170) – Extended Range (ER) Unmanned Aircraft System (UAS)



- Length 9.2 ft
- Wingspan 16 ft
- GTOW ~180 lbs
- Payload ~35-40 lbs
- Ceiling 14 kft
- Cruise speed 70 knts
- Endurance 9 hrs

CAPABILITIES

- Electronic Scanning; No Antenna Mechanical Gimbal
- Multi-TB On-Board Data Recording
- Reconfigurable for Other Sensors: LIDAR, HSI, Chem-Bio
- Multi-Platform Distributed Sensor Experiments (eg, MIMO)
- Autonomous & Collaborative Multi-Platform Control
- Space for Future GPU/FPGA On-Board Processing

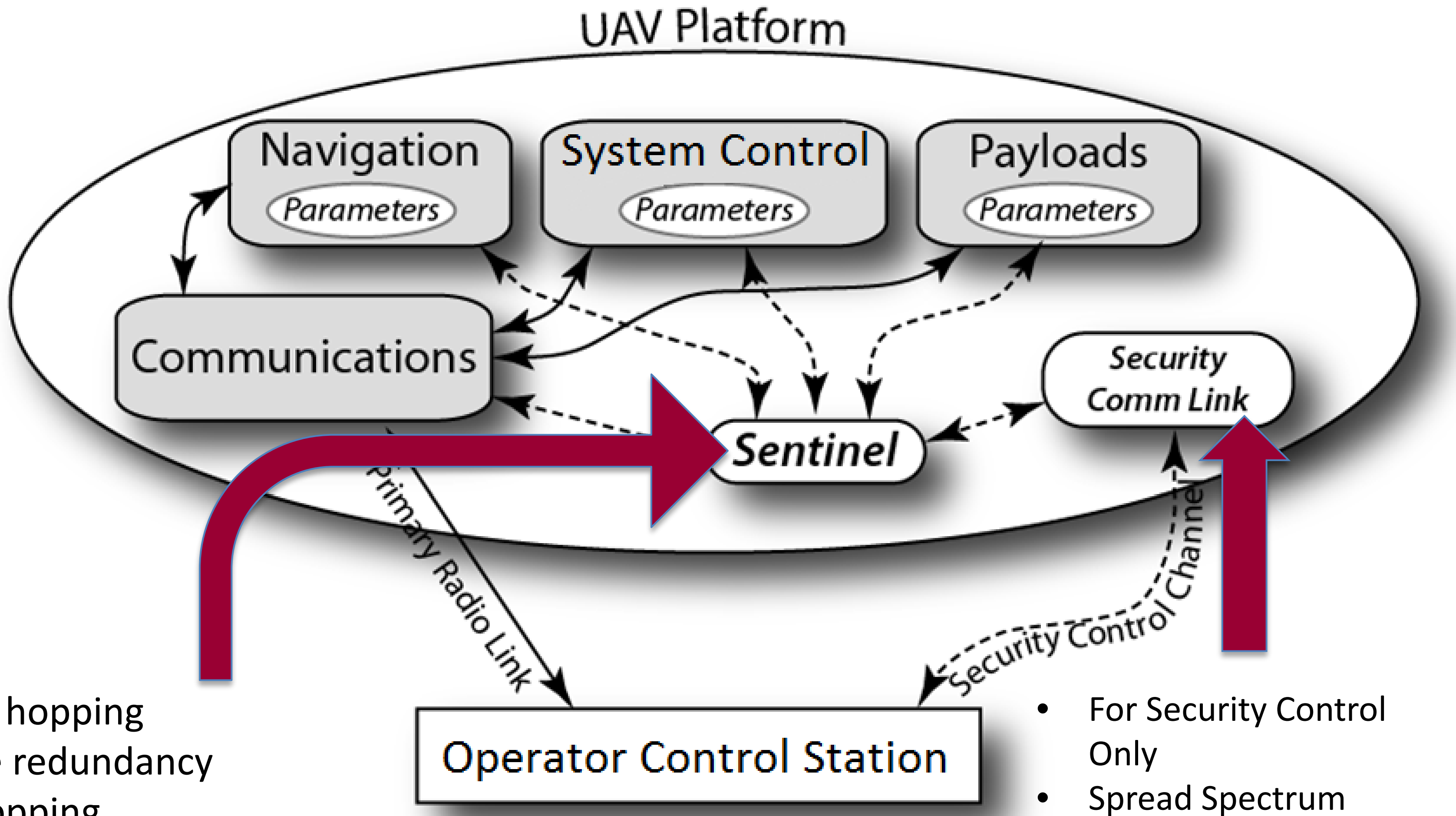
Current Project Exploits and Solutions

- Exploits
  - Waypoint Manipulation from ground or onboard the aircraft
  - Meta Data manipulation on imagery
  - GPS embedded data manipulation
  - Pointing control of surveillance camera
- Solutions
  - Airborne and ground-based detection of attacker waypoint changes, classifying the nature of the attack, and restoration
  - Airborne detection of meta data manipulation
  - Airborne detection of embedded GPS attack
  - Airborne detection of attacker control of camera pointing and correction

System Characteristics for Monitoring Supports Feasibility of Highly Secure Sentinel Implementations

- Experience To-Date Shows:
  - Very small monitoring apps (< 500 SLOC)
  - No requirement for high performance or tight synchronization
  - No complex intertwining of applications
  - Manageable number of hardware components
  - Diverse low cost hardware is available, supporting diverse OS's, diverse programming languages, diverse communications protocols, etc.

Example Implementation



Config. hopping
Diverse redundancy
Port Hopping
Dedicated voting processing
SW power utilization fingerprint
SW CPU and memory usage fingerprint

- For Security Control Only
- Spread Spectrum Waveform
- Low Data Rate

Formed a Company to Productize the Technology Component of UVa Research

- Center for Innovative Technology Grant to plan for a new company to transition Sentinel technology and tools into practice
- UVA initiative included:
  - Partial company ownership by the University
  - Protection of IP through patents
  - Licensing IP to new company
- Transfer of UVA research staff from UVA to the new company

Gain Horizontal Experience with Multiple Prototypes/Different Partners

- DoD
  - UAV/Surveillance system, including in-flight evaluation
  - Currently employed AF/Army AIMES video exploitation system
  - Radar system (In early design phase)
  - Initiating Army tank project related to advanced fire control system
  - Laboratory-based multi-sensor collection system for mission security research

- NIST (Best practices) - 3d Printers

- Automobile cybersecurity
  - Security for Perrone Robotics DARPA Urban Challenge autonomous vehicle
  - Virginia State Police project

Automobile Video

Voluntary Technology Partners

- Air Force/SiCore – Small business security technology company focused on FPGA security
- NIST SW Testing Tools Technology Group
- MITRE
- Aerospace Corp
- APL
- Kaprica Security
- Digital Bond

RISK BASED METHODOLOGY FOR SELECTING FUNCTIONS TO MONITOR (POLICY)

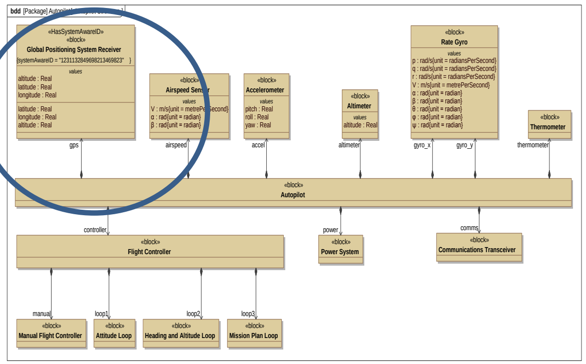
Architecture Selection Teams

- Blue Team 1 – Identifies and prioritizes critical system functions
- Red Team – Identifies most desirable/lowest cost attacks (cost measured in complexity, risk of discovery, dollars required, etc.)
- Blue Team 2 – Identifies the set of security design patterns that address results of Blue/Red team prioritization analyses
- Green Team – Conducts cost/asymmetry analyses and selects desired solution that fits budget constraints

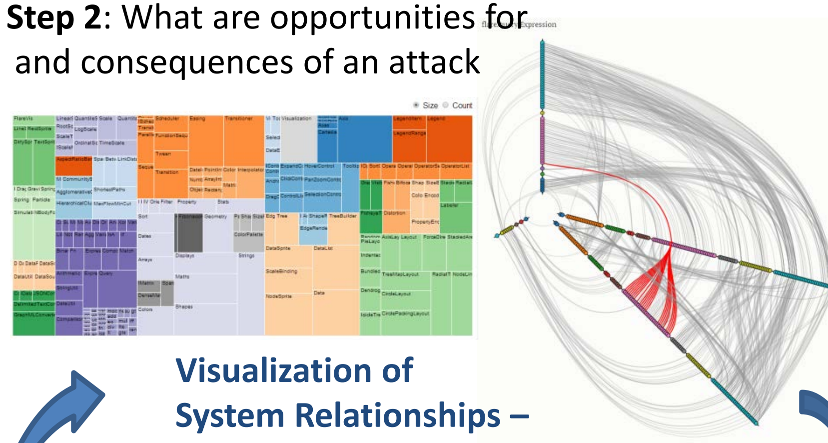
System Aware Cyber Security Framework: V2.0

Step 1: Identify Critical Assets

SysML models of UAV
(**High fidelity Model Semantics**)



Step 2: What are opportunities for and consequences of an attack

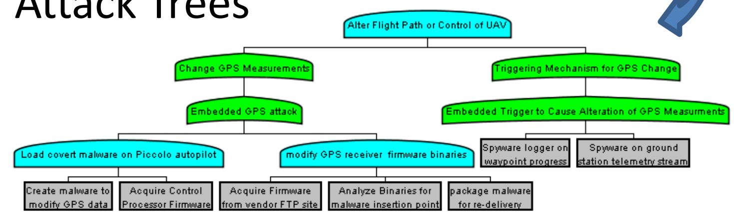


Visualization of System Relationships – Better Coverage of Attack Surfaces

Explicit information exchange- Information from SysML models helps create Attack Trees closer to reality

Step 3: What is exploitable and by whom

Attack Trees



Resources for Attack

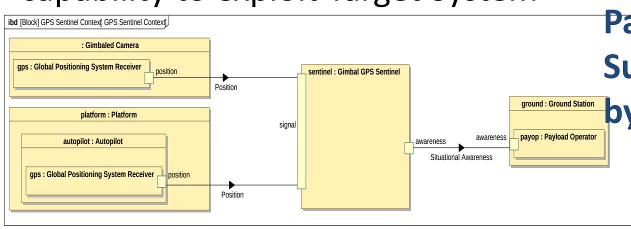
Attack Descriptions

Agent Profiles

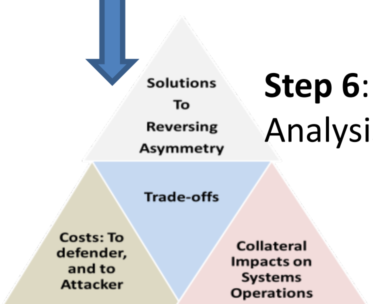
Output:

- Ease of Attack
- Capabilistic Propensity
- Relative Risk

Step 4 and 5: Select/Evaluate Best Design Patterns to effect Adversary's capability to exploit Target System



Evaluation of Design Patterns Now Supported by Functional Models



Step 6: Cost Benefit Analysis

Decision making now aided with Easy to use Data Analysis/Visualization Tools

Partners for Policy-related Research

- APL
- Leidos
- Spectrum
- Army CRADA being developed

OPERATIONAL AND HUMAN FACTORS (PROCESS)

Operational Considerations (Process)

- Human Factors and Training Requirements
  - Zero day attack that happens once in your career
- Simulation experiments with UAV operators at Creech AF base resulting in important new system insights
- UAV operator attributes for confident response
  - Live experiments at Wright Patterson in February

Operational Procedures and Human Factors Partners

- MITRE on Creech AFB experiment, including on-site UAV operations people
- AFIT/AFRL on operator training, including providing test environment

Observations

- Due to lower costs for technology components and standards that simplify integration, we can use operational prototyping to evaluate new concepts (e.g., autonomous cars)
- Operational prototyping allows for Technology, Policy and Process to be concurrently addressed and learned about
  - More degrees of innovation freedom
  - More rapid time-lines compared to a sequential transition strategy
- While more degrees of freedom for innovation, also are more issues to be concurrently addressed and evaluated
- Voluntary partners who can support either technology, process or policy find opportunity in engaging in a university-based systems focused project