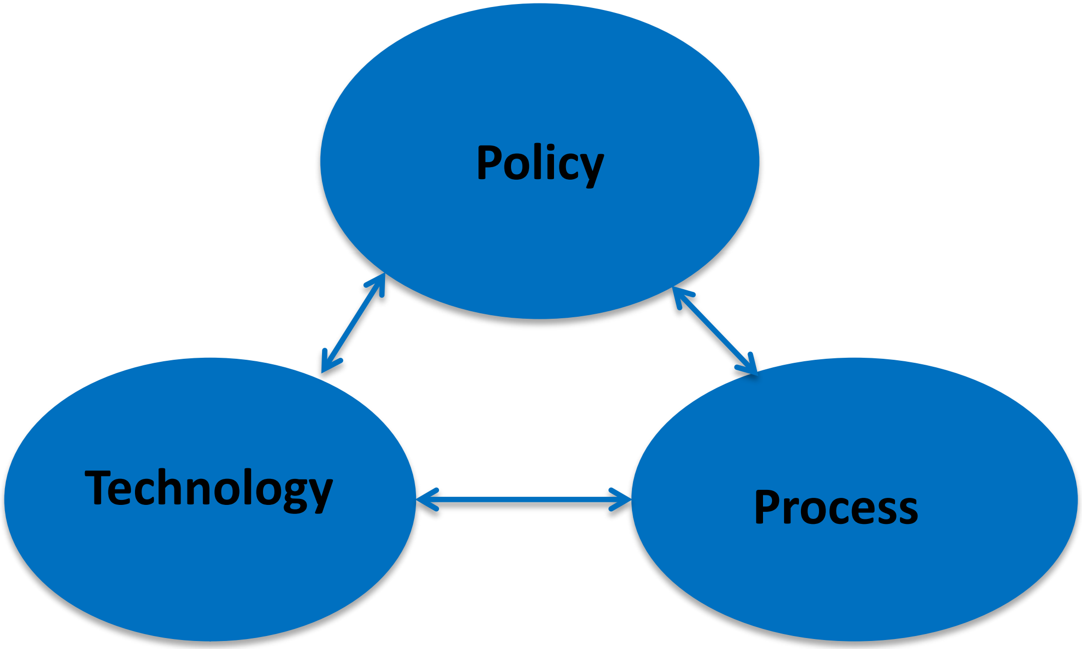
Systemic Security

Presented By
Rick A. Jones
University of Virginia

5th Annual SERC Sponsor Research Review
February 25, 2014
Georgetown University
Hotel and Conference Center
Washington, DC

www.sercuarc.org

System Engineering for a New System



- Integrate Policy, Technology and Process (including human factors) to satisfy
- Objectives of diverse system stakeholders
- Subject to constraints (e.g., Cost, Schedule)

Cyber Security of Combat Systems

- Cyber security community has not addressed the cyber security of missions as opposed to the systems that together carry out a mission
- Cyber security community has focused on network and perimeter security, and has not addressed the protection of mission functions which reside within combat systems:
  - —Weapon Systems
  - —Sensor Systems
  - —C2 Systems

SERC Cyber Program

- Addresses Policy, Process and Technology
  - Policy: Solution selection methodology that focuses on the cyber security of the combined set of systems that conduct a mission
  - Technology: Development of a technology architecture and specific solutions that protect critical functions within individual combat systems
  - Process: Human in the loop, simulation-based exploration and evaluation of candidate operational procedures for response to attack detections(be they false alarms or true detections)
- Integrating these diverse efforts through use of a UAV-based surveillance mission as the test case for prototypes in each area
- Working with SERC and the DOD SERC sponsor, we are gaining tangible outside support ($, simulation vehicle, UAV, hardware and software) to the SERC program from stakeholders interested in transitions of developed technology and system concepts

Policy: Decision Process and Support Tools for Selection of the Integrated Set of Solutions for Securing Military Missions

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)

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)

Focus on Defense Against Exploits that Impact System Performance (e.g., Data Corruption, Functional Degradation, System Latencies)

Selection Methodology

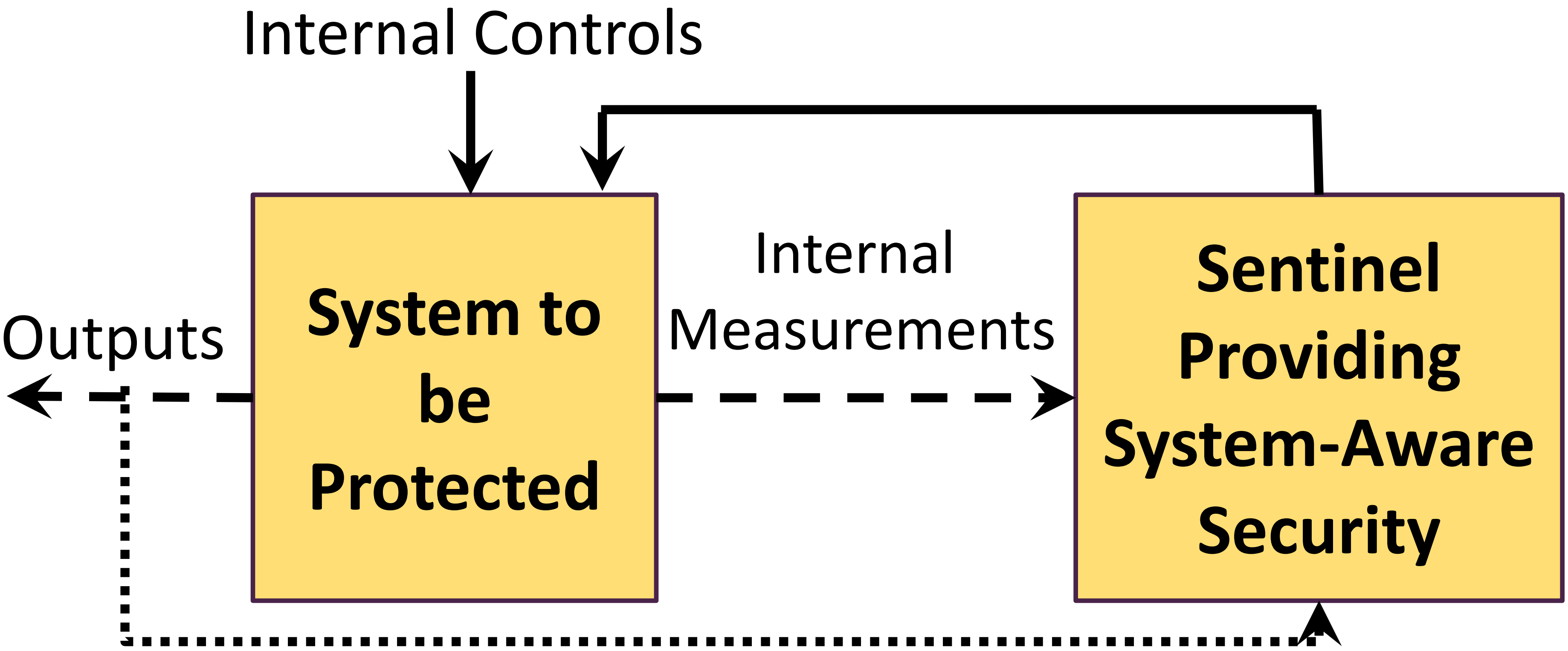
- Blue/Red/Green team analysis for individual combat systems to identify:
  - Most Critical Individual System Functions (Blue)
  - Identification of specific asymmetric attacks on these functions (Red)
  - Identification of technical solutions to counter asymmetric attacks
  - Assessment of costs and security benefits to select the most desirable integrated solution sets
- At the mission level, using individual system level inputs, the service Cyber Commands could integrate the individual system analyses on a mission security basis
- Utilize analytical tools to support decision-making

Status

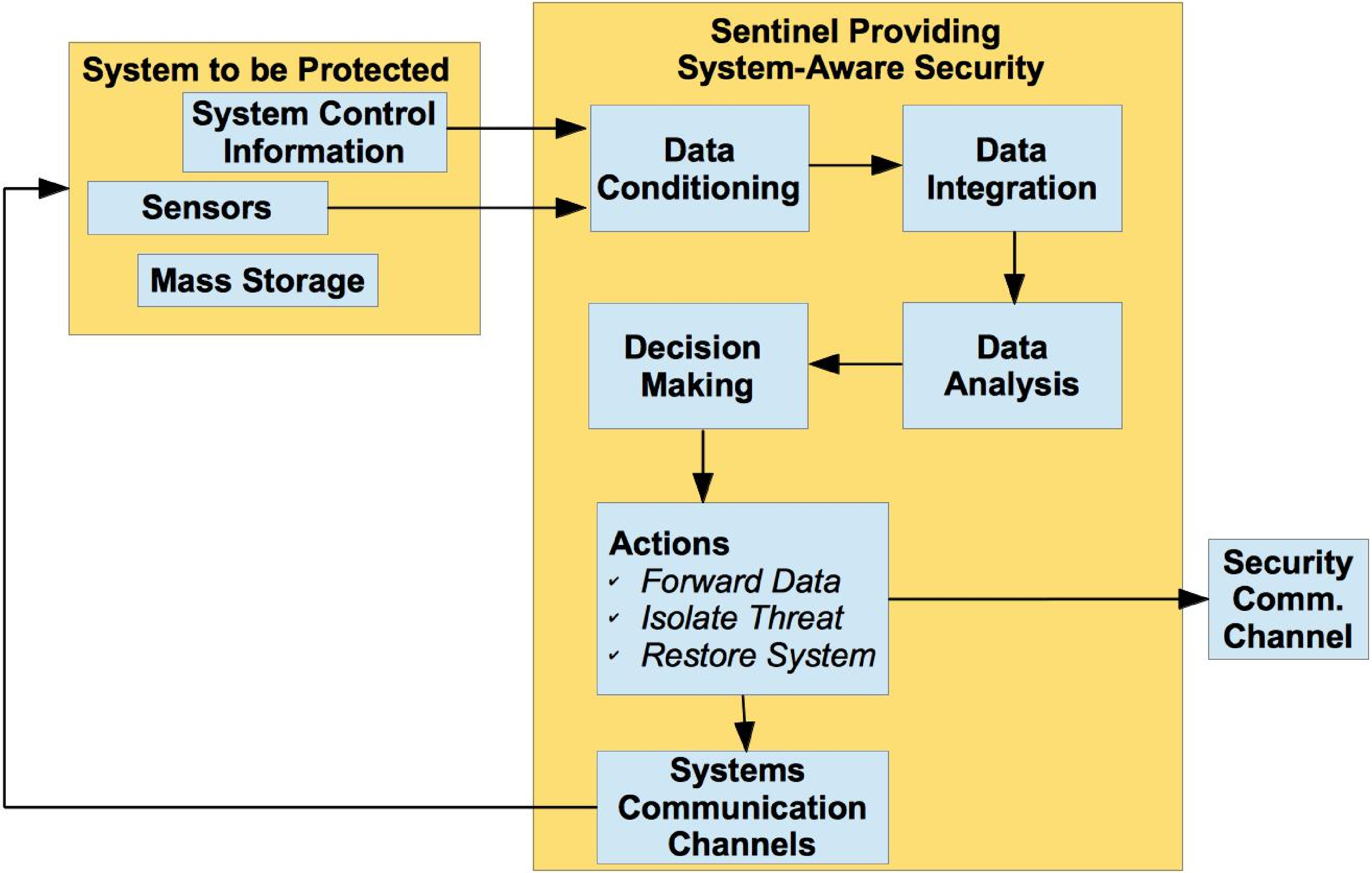
- Refining decision-support techniques and tools based on our internal project first use of the methodology and prototype tools
- Preparing for an October Workshop with interested military planners
  - Recently had discussions with Navy 10th Fleet
  - With Mitre support, preparing for discussions with AF Cyber Command
  - Considering invitation to a representative(s) of the National Defense University

Technology: System Aware Cyber Security

High Level Architectural Overview



Sentinel Data Flow



Super Secure Sentinel

- Architecture is based upon development of Sentinels that can be more trusted than the systems that they monitor

- Characteristics of monitoring applications support potential for Super Secure Sentinel implementations

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.

Technology Prototype: Autonomous Surveillance System On Board a UAV

GAUSS– GTRI AIRBORNE UNMANNED SENSOR SYSTEM

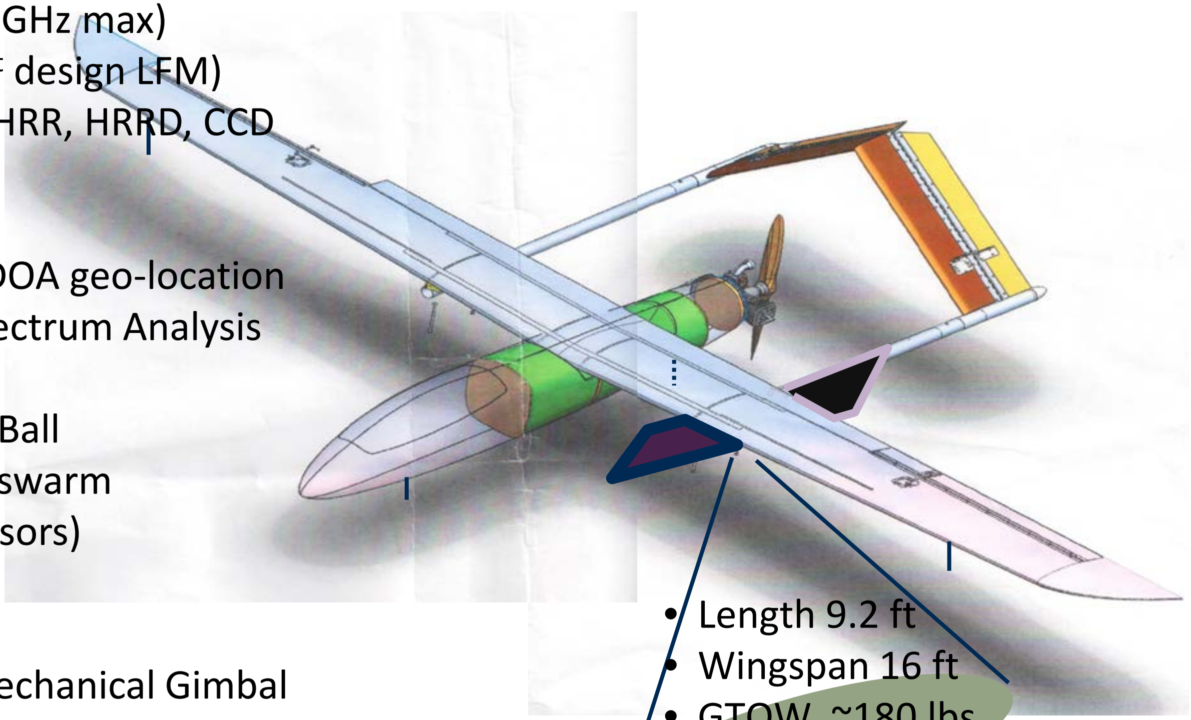
FOUR SENSOR OBJECTIVE BASELINE

- 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)

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

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

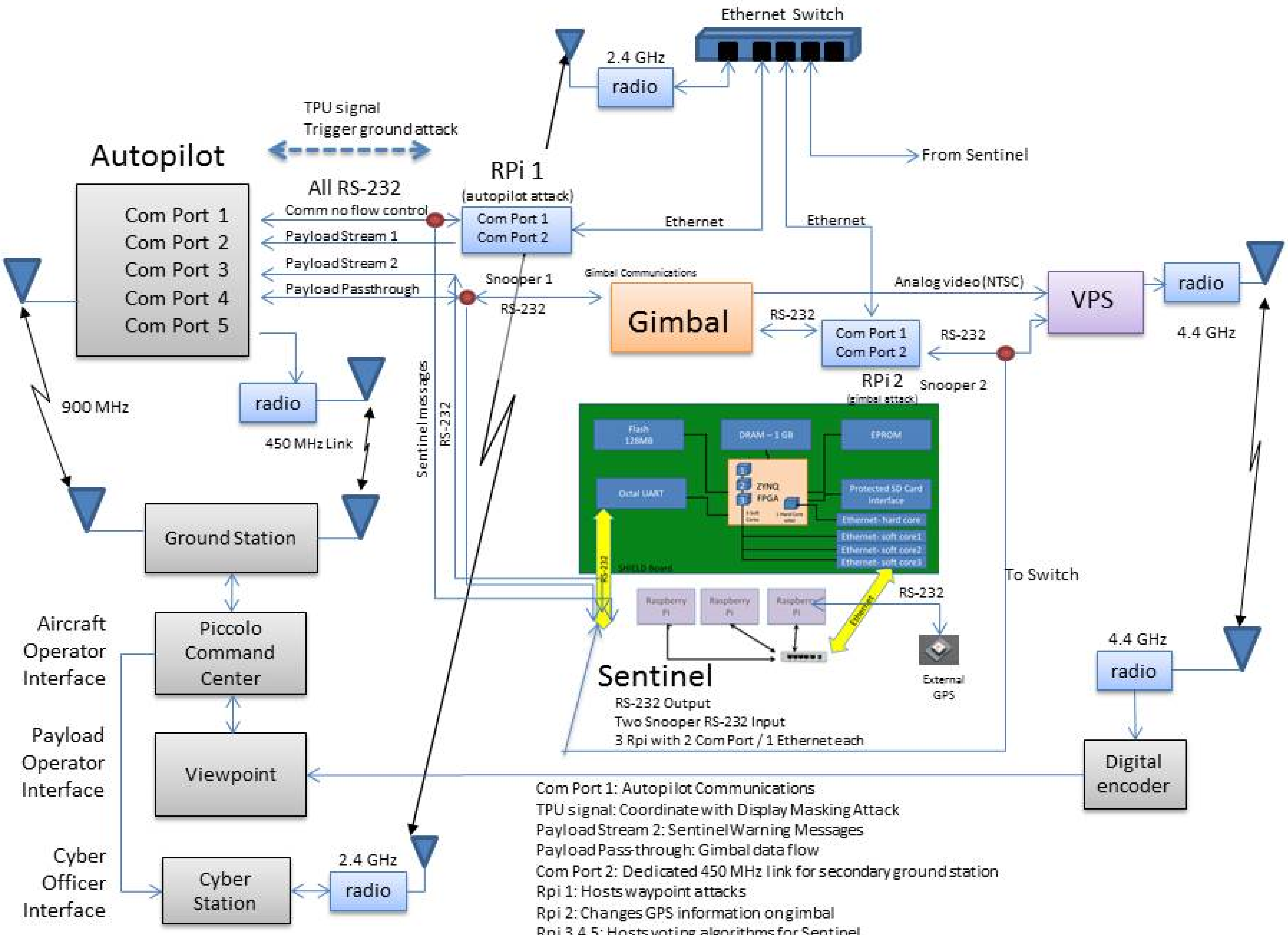


- Length 9.2 ft
- Wingspan 16 ft
- GTOW ~180 lbs
- Payload ~35-40 lbs
- Ceiling 14 kft
- Cruise speed 70 knts
- Endurance 9 hrs

15

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



RS-232 Output
Two Snooper RS-232 Input
3 Rpi with 2 Com Port / 1 Ethernet each

Com Port 1: Autopilot Communications
TPU signal: Coordinate with Display Masking Attack
Payload Stream 2: Sentinel Warning Messages
Payload Pass-through: Gimbal data flow
Com Port 2: Dedicated 450 MHz link for secondary ground station
Rpi 1: Hosts waypoint attacks
Rpi 2: Changes GPS information on gimbal
Rpi 3,4,5: Hosts voting algorithms for Sentinel
● Passive Snooper

CML
NetFPGA7
XILINX
KINTEX-7
XC7K325T
PIC
BTN1
BTN2
BTN3
BTN4
BTN5 RESET
Prog Done
XILINX PWR CABLE
USB PROG
J3
J10
J11
J16
GND
VCC3V3
VCCIVO
MGTAVTT_1V2
MGTAVCC_1V0
#1

Technology Status

- Developed a number of design patterns for cyber security solutions to protect system functions
- Implementing a live prototype with live flight evaluations scheduled for the end of this coming summer with GTRI (aircraft integration and flight testing) and SiCore (secure electronics board design and implementation, funded by AF) support
- Starting an new effort to develop a Sentinel on a private cloud to monitor imagery exploitation system in use by the AF and Army (with Leidos support)

Process: Team –Based Response to Detected Cyber Attacks

Operational Concept Development for Response to Cyber Attacks on Combat Systems

- Based on current AF UAV Surveillance operational procedures

- Add a Cyber Officer to a team of:
  - Pilot
  - Surveillance Officer
  - Intel Officer
  - Mission Commander

- Human in the loop, simulation-based exploration and evaluation of candidate operational procedures for response to detected attacks
  - Team Structure
  - Information needs and situation presentation mechanisms
  - Repeatability of responses
  - Robustness across different attacks
  - Influence of “context factors” on responses
  - Responses to false alarms

- Mitre team at Creech AFB is supporting this effort, including providing simulation vehicle to support the evaluation

Status of Process Effort

- Determined what the needed simulation capabilities are and Mitre will lead the development work
- By end of the summer we expect to have conducted some human-in-the-loop experiments and will start discussions with AF at Creech AFB (led by Mitre) to hopefully start experiments with AF operational people

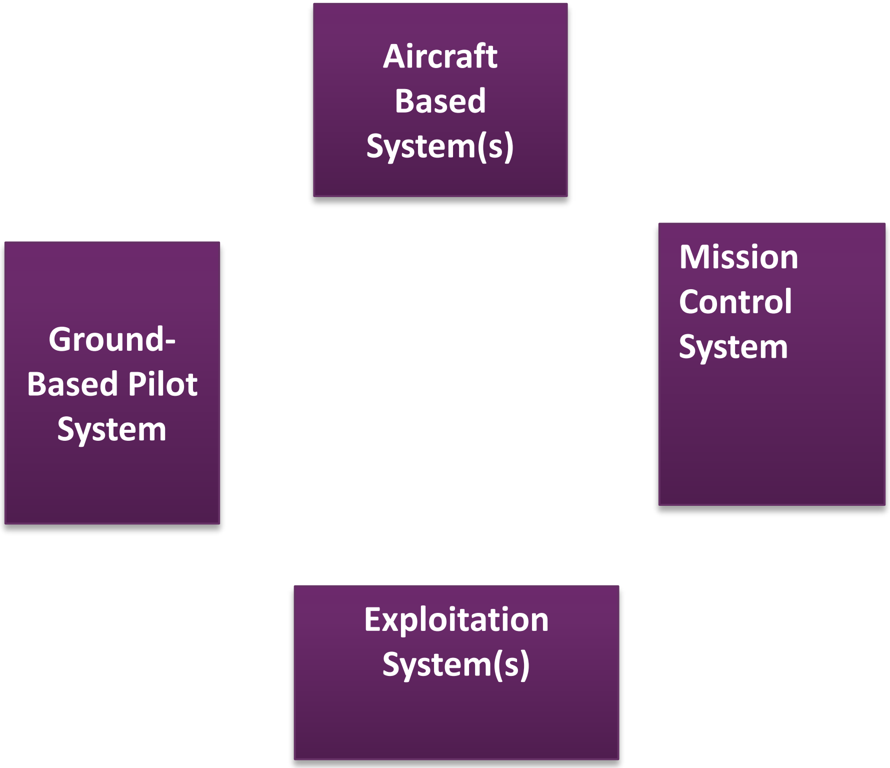
Summary

- The set of policy/process/technology research efforts provides a holistic start to transitioning these concepts to military use
- AF, SiCore, Mitre, Leidos, GTRI, and UVA are all providing resources to advance the project
  - —AF: Funding for SiCore
  - —SiCore: Electronics and training to UVA and GTRI for use of their development kits (FPGA-based development, use of encryption on the board, etc.)
  - —Leidos: Advanced Imagery Exploitation System(AIMES) SW currently licensed to the AF and Army
  - —GTRI: Use of the Outlaw Aircraft
  - —Mitre- Use of REACT Simulation Vehicle

System Aware Cyber Security Publications

- J. L. Bayuk and B. M. Horowitz, An architectural systems engineering methodology for addressing cyber security, Systems Engineering 14 (2011), 294-304.
- R. A. Jones and B. M. Horowitz, A system-aware cyber security architecture, Systems Engineering, Volume 15, No. 2 (2012), 224-240.
- 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, 2013.
- 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, To appear, 2013
- R. A. Jones and B. M. Horowitz, System-Aware cyber security, itng, 2011 Eighth International Conference on Information Technology: New Generations, 2011, pp. 914-917.
- 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.
- 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.

Need for Multiple Interacting Sentinels for Integrated Attacks and Symptom Sharing



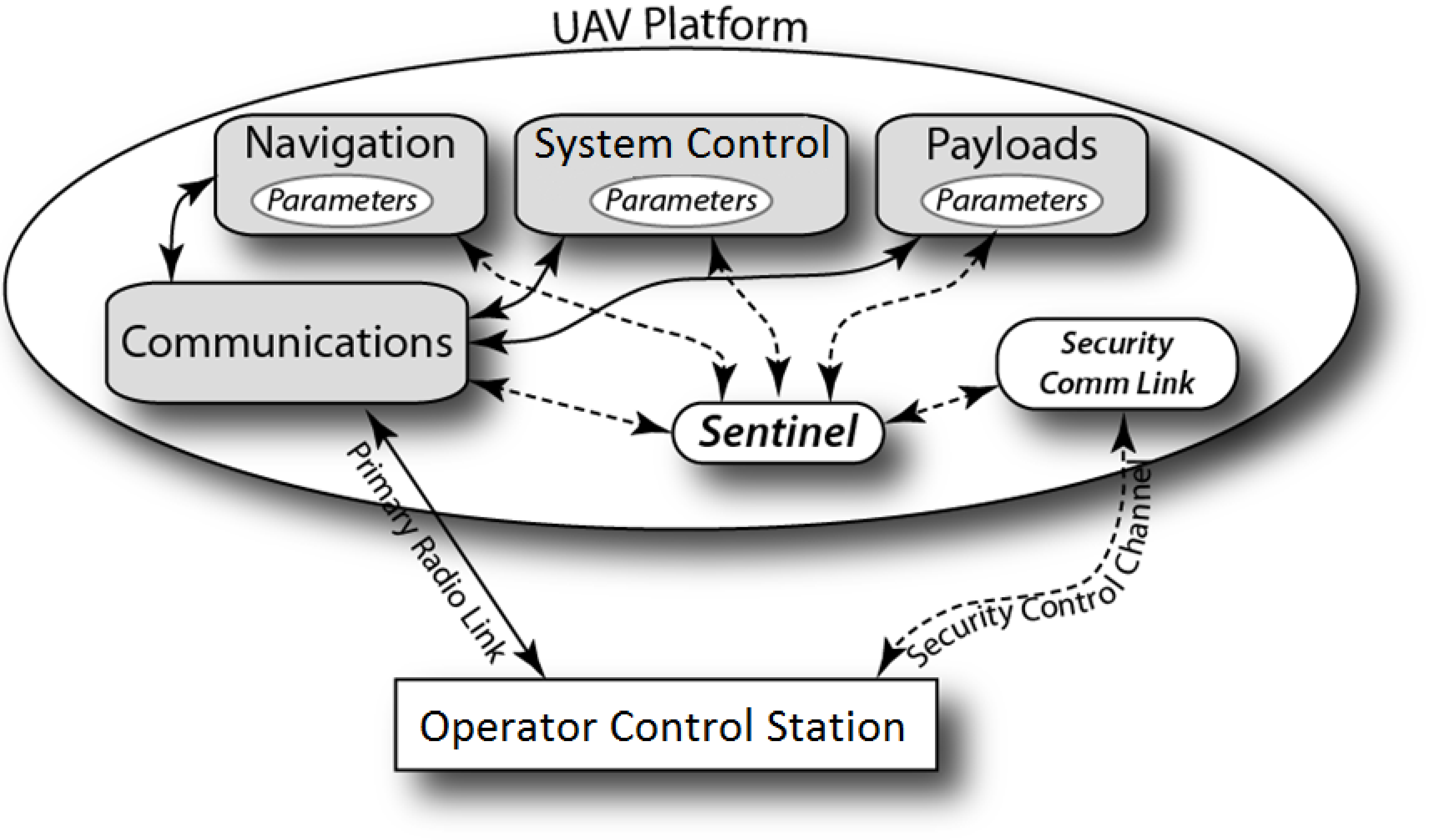
Aircraft Based System(s)

Ground-Based Pilot System

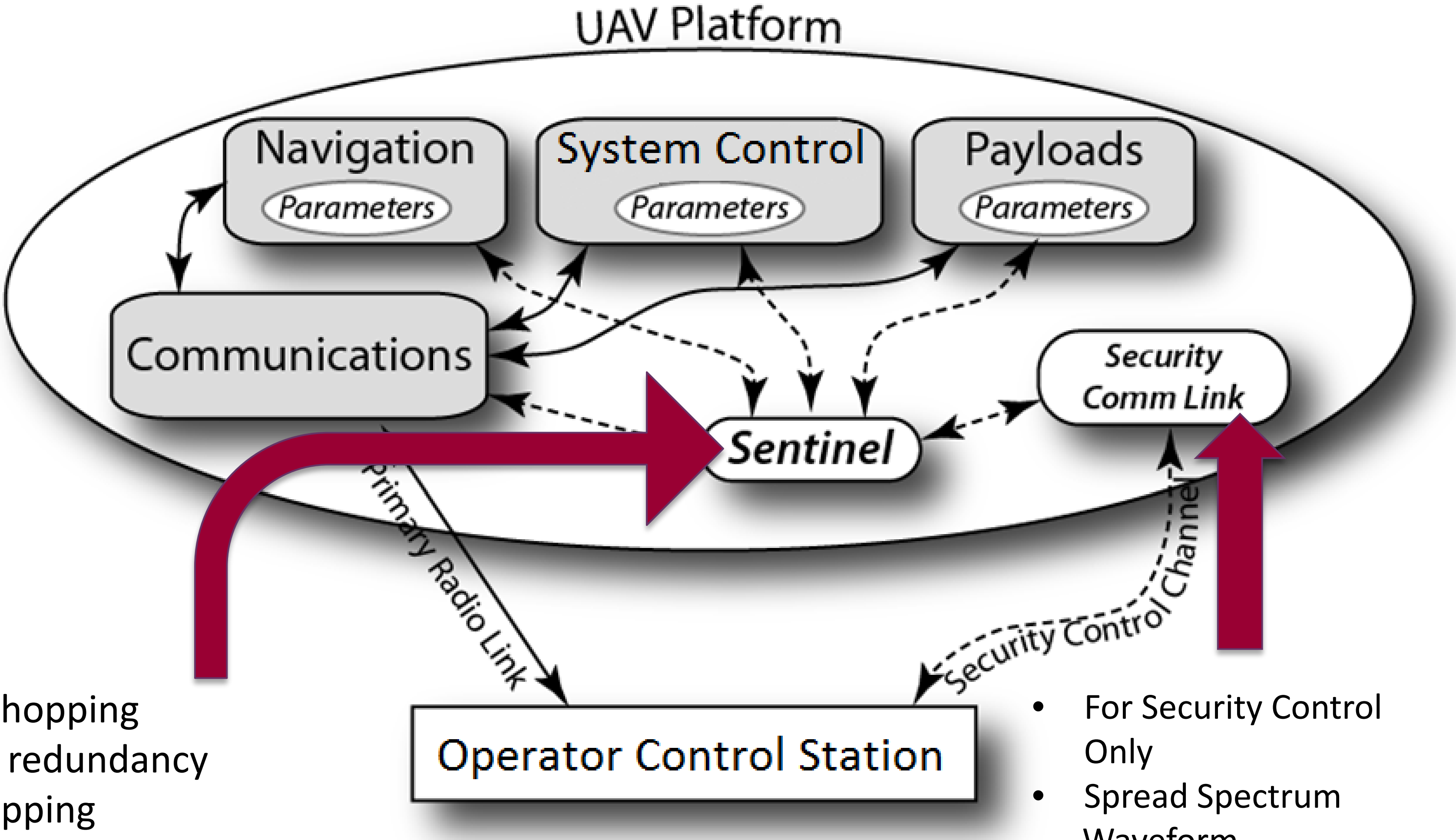
Mission Control System

Exploitation System(s)

Example:
Autonomous Surveillance Platform Protection



Example:
Autonomous Surveillance Platform Protection



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