

# System Aware Cyber Security

Barry M. Horowitz, PI

University of Virginia

November, 2012

# System Aware Cyber Security

- Operates at the system *application-layer*,
  - For *security inside* of the network and perimeter protection provided for the whole system
  - Directly protects the *most critical system functions*
  - Solutions are *embedded within* the protected functions
- Addresses *supply chain* and *insider threats*
- Includes *physical systems* as well as *information systems*
- Solution-space consists of *reusable design patterns*, reducing unnecessary duplications of design and evaluation efforts
- Includes a *scoring framework* for supporting Systems Engineers in evaluating alternative architectures

# System Aware Cyber Security

## Architecture Design Objective

*Reverse cyber security asymmetry  
from favoring offense to favoring  
defense*

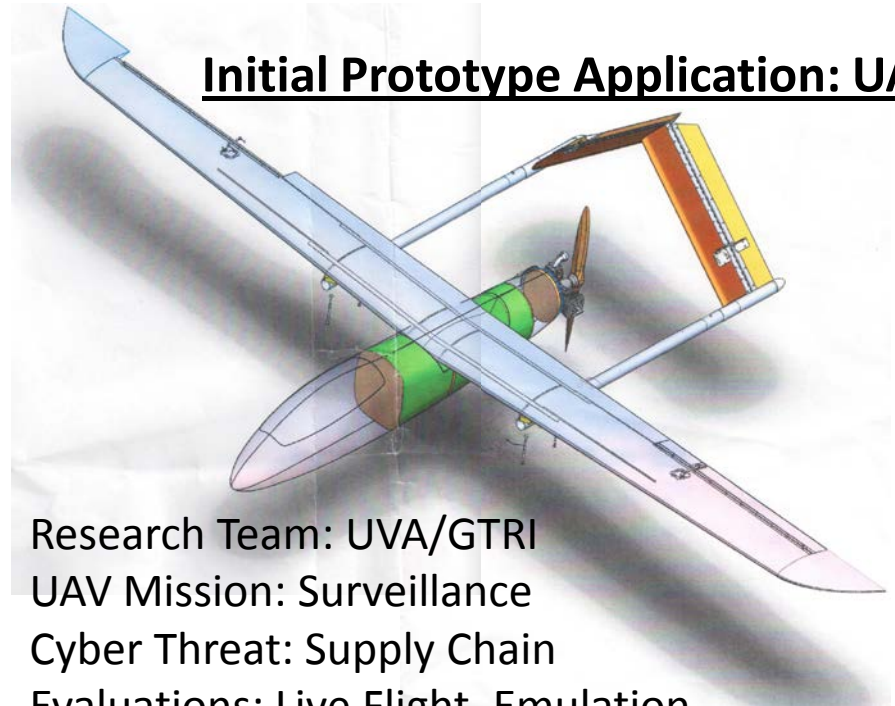
## Design Patterns

- Diverse Redundancy
- Diverse Redundancy + Verifiable Voting
- Physical Configuration Hopping
- Virtual Configuration Hopping
- Data Consistency Checking
- Physical Confirmations of Digital Data
- Use of Analog Components

## Solution Technology Sources

- Fault Tolerant Systems
- Automatic Control Systems
- Information Assurance

## Initial Prototype Application: UAV



- Research Team: UVA/GTRI
- UAV Mission: Surveillance
- Cyber Threat: Supply Chain
- Evaluations: Live Flight, Emulation,  
Simulation