Security Engineering - FY16
System-Aware Cybersecurity

Peter Beling, Barry Horowitz, Cody Fleming
(UVA)
Carl Elks, Georgios Bakirtzis
(VCU)

UNIVERSITY of VIRGINIA ENGINEERING

SYSTEMS ENGINEERING Research Center
A US DoD University Affiliated Research Center

VCU
VIRGINIA COMMONWEALTH UNIVERSITY
School of Engineering

System-Aware Cybersecurity: An Approach to Resiliency for Physical Systems (1 of 2)

- Response to attacks that penetrate network and perimeter security defenses
- Also insider and supply chain attacks
- Application domains:
  - Weapon Systems
  - C2 Systems
  - Sensor Systems
  - Logistics Systems
  - Computer Controlled Physical Systems (Engines, Electrical Power, Rudder Control)
  - Etc.

System-Aware Cybersecurity: An Approach to Resiliency for Cyber Physical Systems(2 of 2)

- Securely monitor physical systems for illogical control system behaviors (Secure Sentinel technology)
- For detected attacks:
  - Inform system operators
  - When possible, provide decision support for reconfiguration

- Developed, and currently developing, a number of prototype solutions including evaluations of responses to cyber attacks during system operation

  Completed Efforts:
  - UAV Surveillance system (DoD)
  - 3D Printer (NIST)
  - State Police cars (Virginia)

  Ongoing Efforts:
  - Radar (DoD)
  - Tank Fire Control System (Picatinny Arsenal)
  - Navy Ship (SBIR Partnership)

Illustrative Examples of Illogical Control

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

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

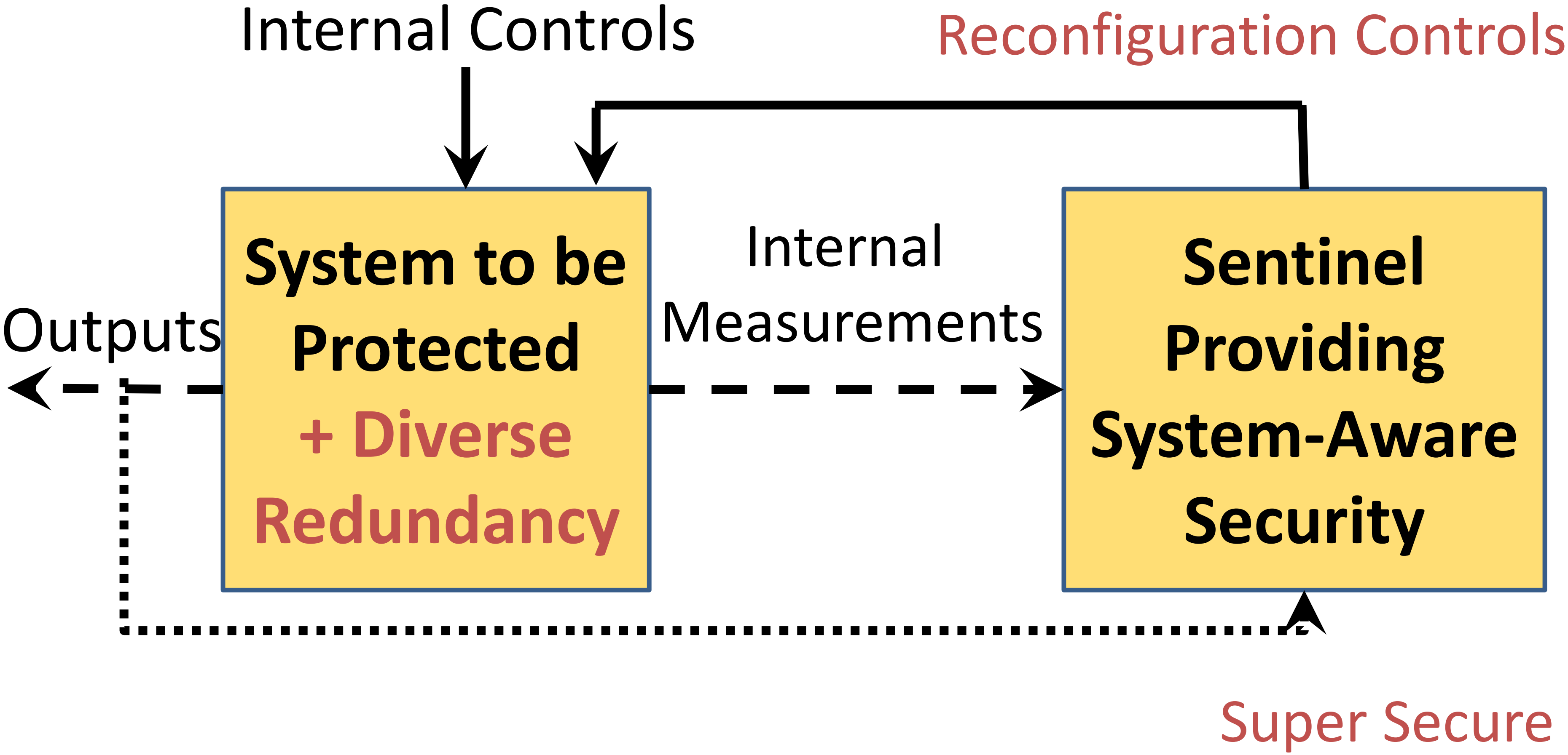
  (Data Integrity)
* System Identification

  (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

High Level Architectural Overview



Mission-Aware Cybersecurity

Human/System Interface

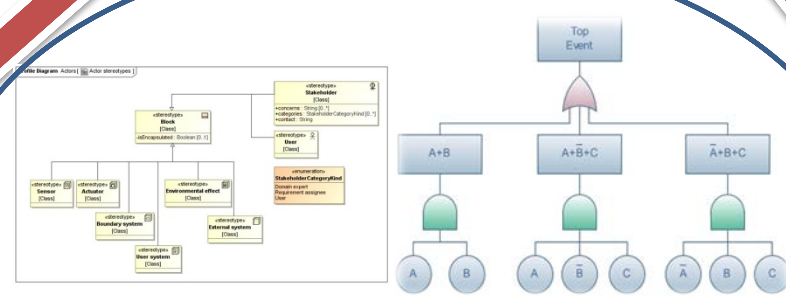
Mission Aware Cyber Security

- **Understanding the Consequences of attacks to Mission integrity**
- **Multidisciplinary modeling**
- **Systems of System Perspective**
- **Model Driven Approach to Vulnerability/Consequence Assessment**

Critical Assets

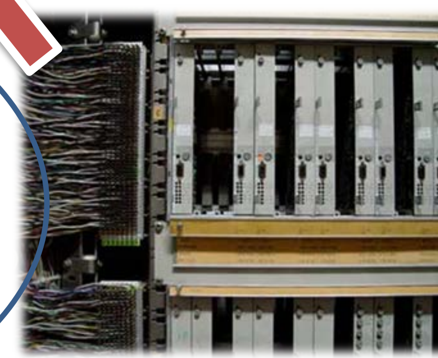
DETECTION AND MITIGATION STRATEGIES TO PROTECT CRITICAL ASSETS

Mission Context



Security / Vulnerability Modeling Methods

System of Systems Perspective



2016 Focus

1. Transition of System-Aware technology into practice on Army tank fire control system
2. Human factors of sentinel alerts and system reconfiguration
3. Decision support tools for selection of resilient architectures

Focus 1: Advanced Lethality and Accuracy System for Medium Caliber (ALAS-MC) with Picatinny Arsenal

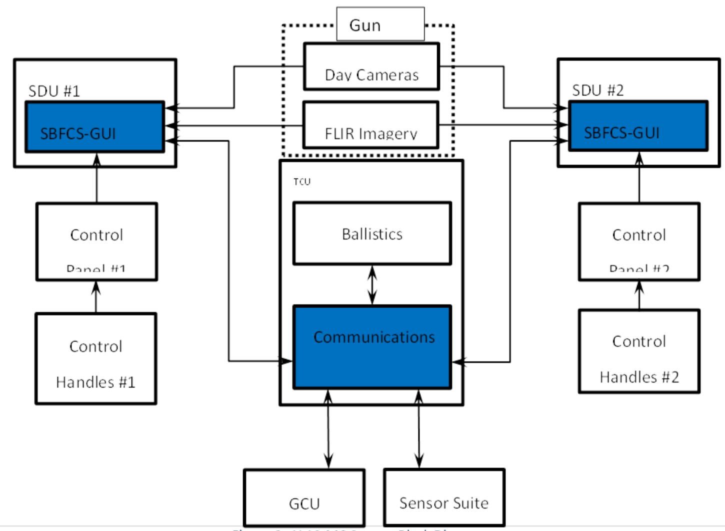


Figure 2: ALAS-MC System Block Diagram

Focus 2: Human Factors Experiments

- UAV Control at Creech AFB
- Cyber Attacks
- Operators receiving inputs from Sentinel
- Operators preferring human-in-the loop decision process
- Unanticipated Outcomes
  - Not sure how they should respond
  - How do they know Sentinel is not under attack
  - How about aircraft in hanger readying for later missions
  - Can they have as needed access to cyber expert when a situation occurs
- Stimulated initiation of new questions and a more substantial concept for experimentation

Suspicion

- Prior AF research activity to characterize a person's level of suspicion
  - Uncertainty
  - Potential for Malicious Intent
  - Consequences
  - Cognitive Capabilities
- 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?

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 consequence
  - System decision support performance including decision-making time
- 8 experimental scenarios ranging from US-based training mission to Middle East-based conflict situation, examples of cyber attacks/no attack, Sentinel missed detections and false alarms

Early Findings Related to Roles and Selection of Operators

- As operator suspicion increased, important HMT performance metrics decreased (more false alarms, more missed detections).
- Sentinel alerts serve as a catalyst for wider spread information searches by the operator, whose results may lead to increased operator suspicion.
- Operator response time increases as suspicion levels increase.

Focus 3: Architectural Selection Problem

- What to protect and why?
- Which combination of design patterns to employ in which mission subsystems?
- How to measure the benefits achieved from implementation choices?
- Process for decision making
  - Who to involve?
  - What information to provide for decision support?
  - How to manage sequential upgrades over time?

Architectural Assessment & Selection Process

- **Identify Relationships between sub-systems, functions and variables**

  What is critical to protect?

- **Recognize the Possible Paths an Attacker Could Take to Exploit critical sub-systems.**.

  What are the opportunities for and consequences of attacks?

- **Determine the Subset of Attack Actions Most Desirable to an Attacker.**

  What is exploitable and by whom?

- **Identify appropriate defensive actions and their impacts on the attacker**

  Pre-selection of cyber defenses

- **Evaluate the impacts of the selected cyber-defensive actions on the system**.

  What does this cost me and can I afford it?

- **Weigh the Security Trade-offs to Determine Which Architectural Solutions Best Reverse the Asymmetry of a Potential Attack.**

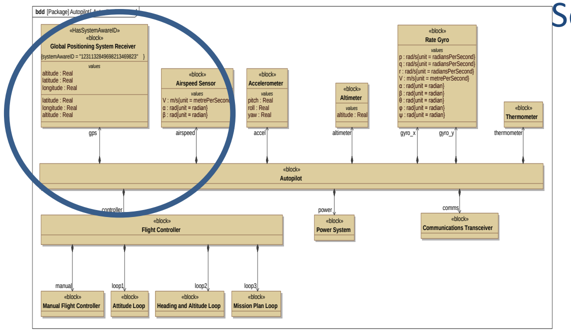
  Effectiveness of best solutions

Architecture Selection Teams

- Blue Team 1 – Identifies and prioritizes critical system functions
- Red Team – Identifies most desirable/lowest cost attacks (cost measured in effectiveness, 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

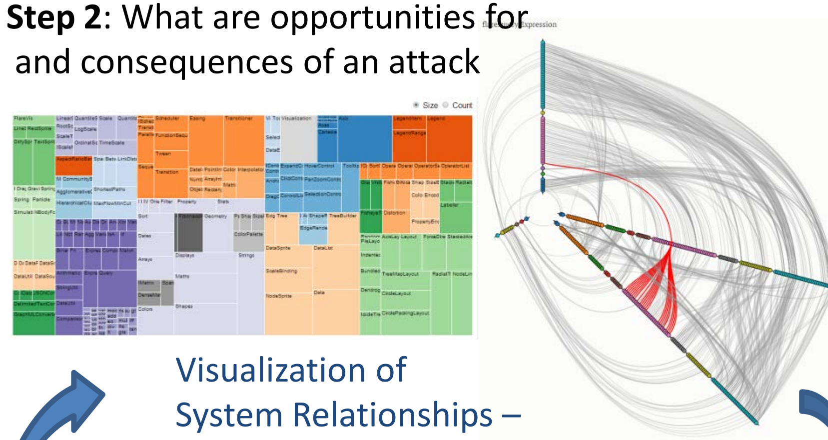
Architectural Selection Framework: Early Version

Step 1: Identify Critical Assets



SysML models of UAV (High fidelity Model Semantics)

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

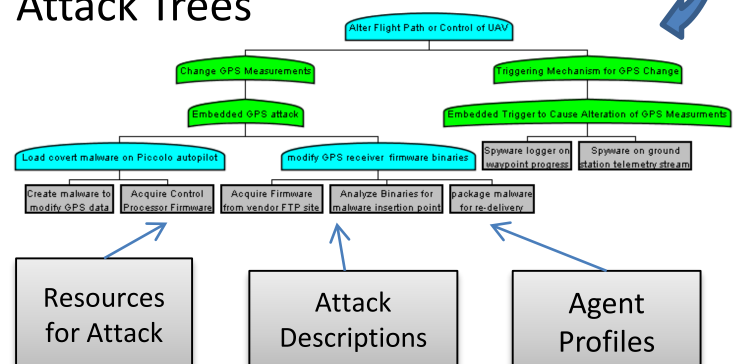


Visualization of System Relationships – Better Coverage of Attack Surfaces

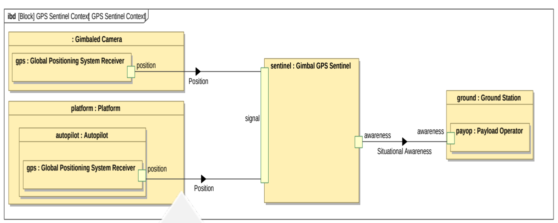
Explicit information exchange- Information from SysML models helps create Attack Trees closer to reality

Step 3: What is exploitable and by whom

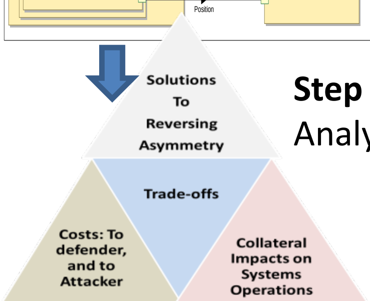
Attack Trees



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

Output:

- Ease of Attack
- Propensity
- Relative Risk

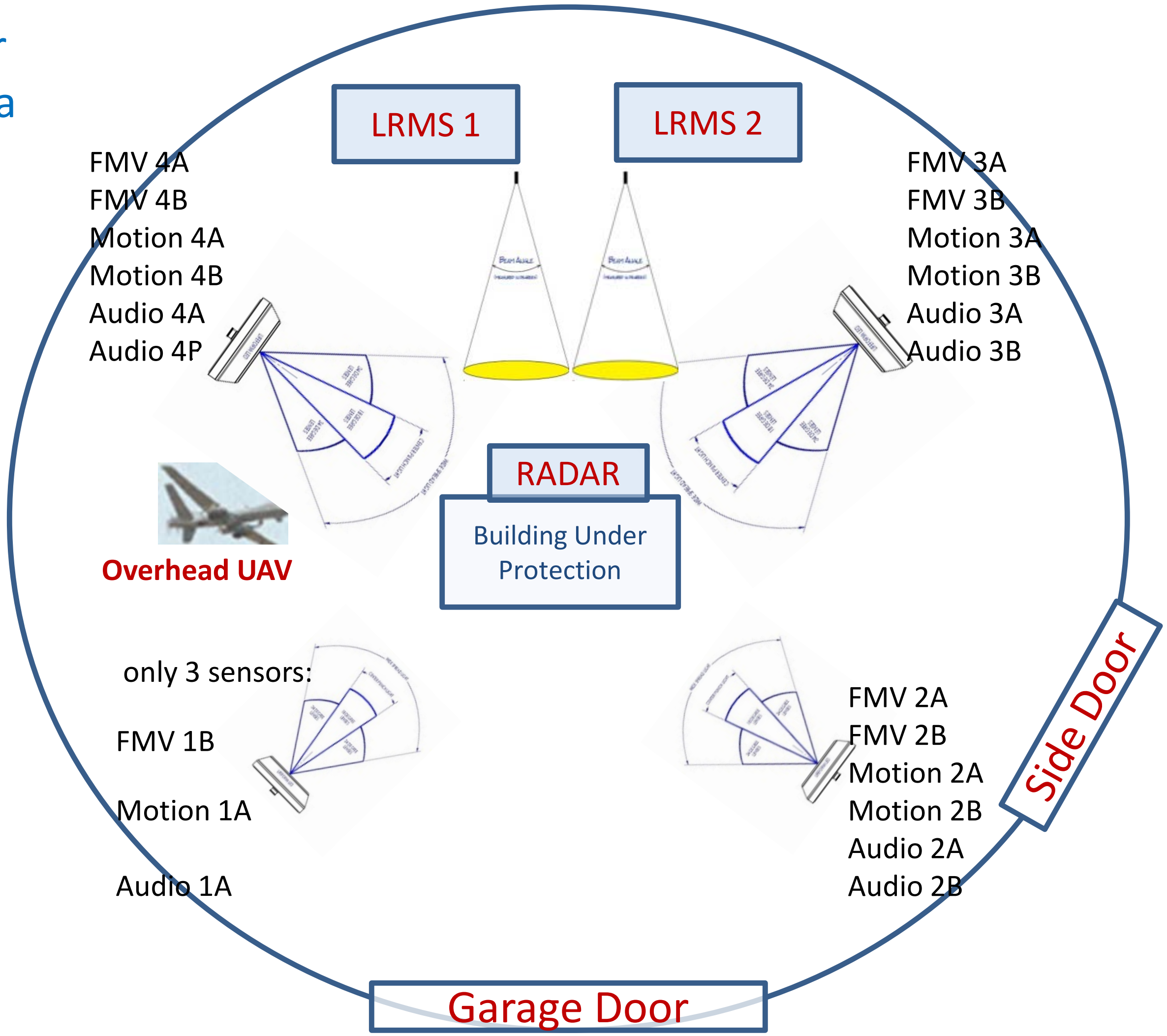
Decision making now aided with Easy to use Data Analysis/Visualization Tools

Modeling Tools for Accuracy at Scale

- **Systems Models** to capture the relationships between functional system entities and to recognize patterns (data, dependence, control) within the system.
  - Be able to represent the system attack surface (danger of under modeling) .
  - Represent the initial system "as-is" with minimal defense and again with possible security solutions implemented.
  - Value in showing solutions integrated into the holistic system for context.
  - Used to model an understanding of the complexity added to an attack by particular defenses.
  - Initial approach used influence diagrams. Currently developing a suite of tools in SysML.
- **Attack Trees** to identify possible paths an attacker could take to exploit the system.
  - Uses assessments of the attack actions and the attackers' capabilities to determine the subset of most preferable actions.

System-of-Systems Demo in UVA Reactor Building

Each Sensor Pod covers a portion of the room and reports on detections within its sphere of detection



Issues Considered 2015

- SoS assessment that addresses cyber attacks from a more strategic perspective regarding military outcomes
- Managing the trade-off between the complexity of analysis and the value of results
- Defining and gaining military organization participation in the research effort

Lessons Learned 2015

1. More systematic methods for accounting for historical attack information in the vulnerability assessment process
2. Need methods to support information gathering from operational community and semi-automatically convert into SysML models

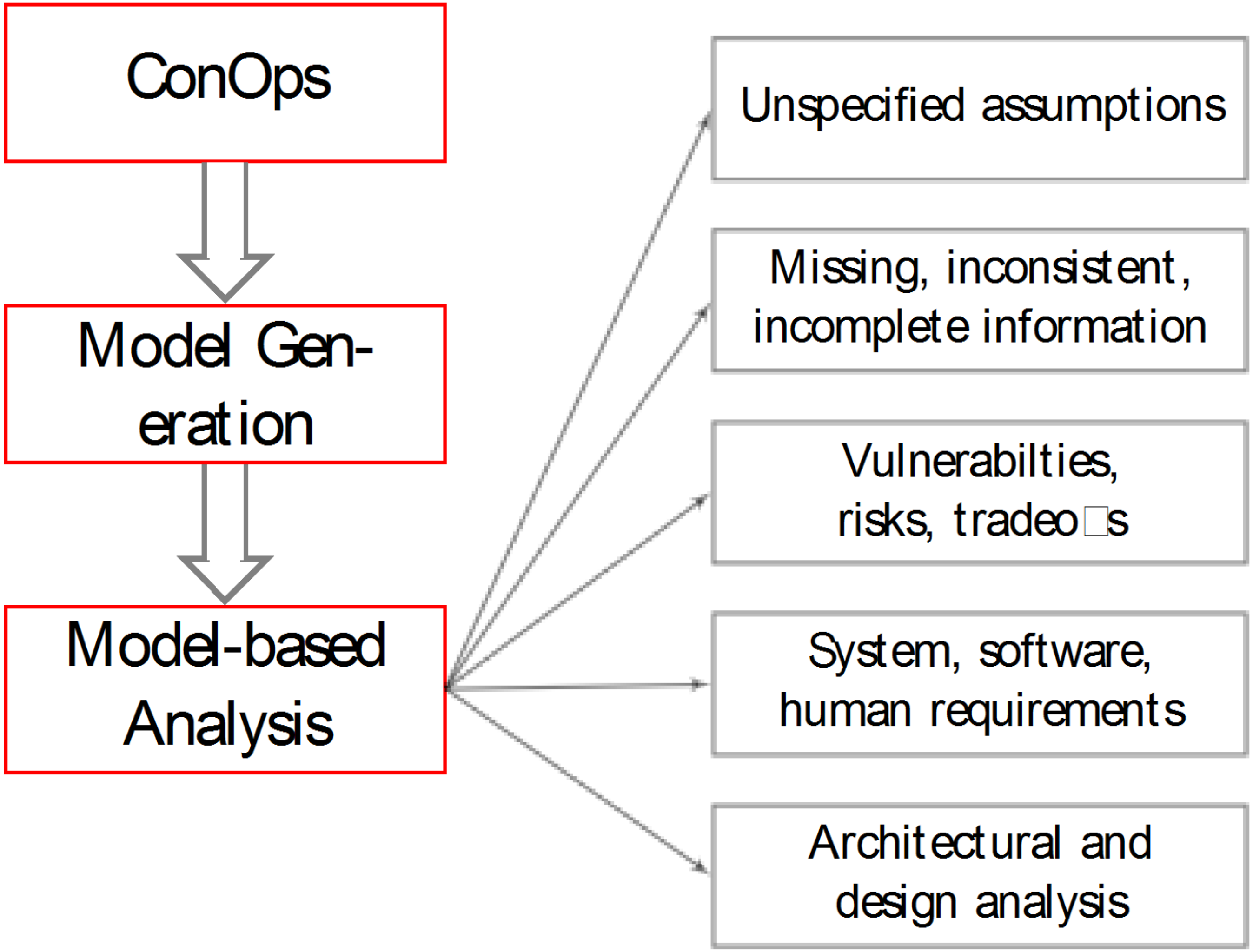
Outcomes and Objectives

- Need methods to support information gathering from operational community and semi-automatically convert into SysML models
- More systematic methods for accounting for historical attack information in the vulnerability assessment process

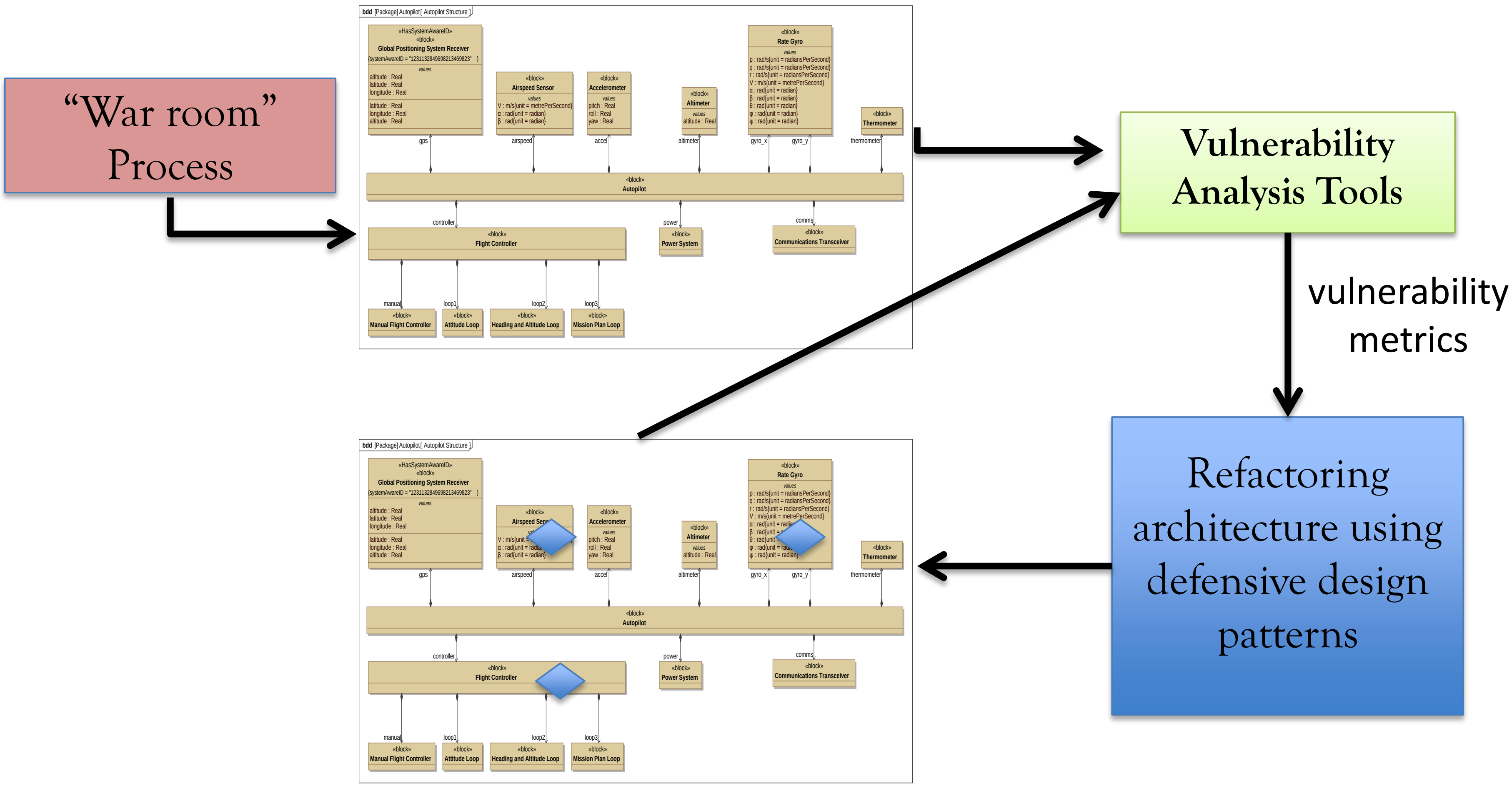
Towards Automation Support for Vulnerability Assessment

- Expressing mission requirements in terms of low level requirement properties (e.g. platform security properties)
- Gathering pertinent threat and historical attack information (special databases, CAPEC)
- Finding attack patterns that are potentially “productive” against our system … Difficult search problem

Approach


ConOps
Model Gen-
eration
Model-based
Analysis
Unspecified assumptions
Missing, inconsistent,
incomplete information
Vulnerabilties,
risks, tradeo□s
System, software,
human requirements
Architectural and
design analysis

Mission-Aware Architectural Selection



Model-based Analysis: Separation of Concerns

Compartmentalization

Modeling | **Extraction** | **Analysis**

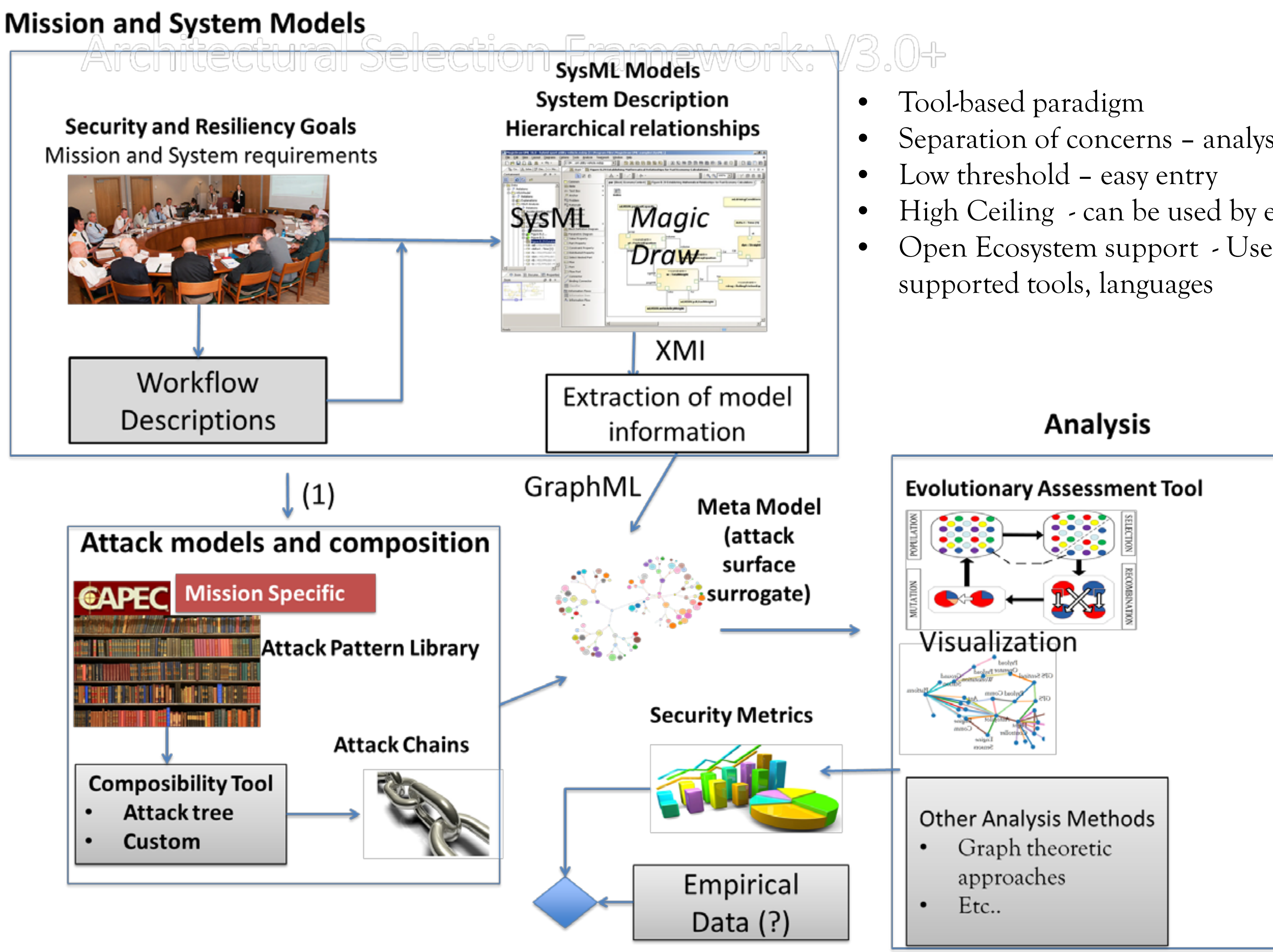
SysML → (OpenAPI / BS Python) → GraphML → (igraph) → jupyter

Meta-model Representation

- Modeling of Mission Oriented Systems
- MagicDraw (SysML)
- Requirements overlays
- Mission Workflows

- Visualization (igraph)
- Attack trees (SecurITree
- Graph theoretic approaches (igraph)
- Genetic algorithm (DEAP)
- Game theoretic approaches (DEAP) (?)
- Linear logic (?)

Mission-Aware Tool Framework 2.0



- Tool-based paradigm
- Separation of concerns – analysis vs modeling
- Low threshold – easy entry
- High Ceiling - can be used by experts
- Open Ecosystem support - Use community supported tools, languages

Current Focus – The War Room

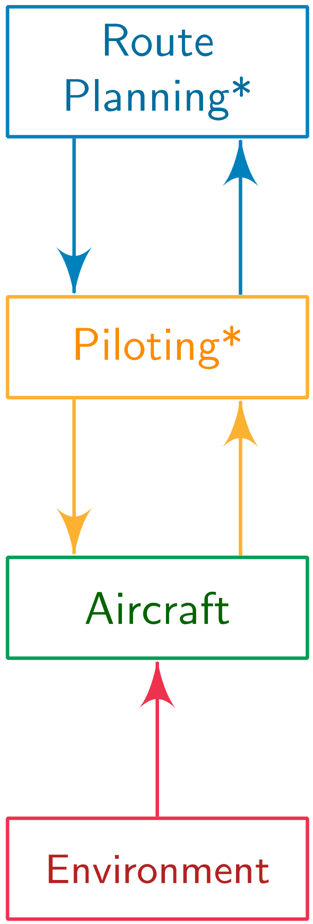
- Adapting tools applied to similar problems in aviation safety
  - Generating a model from high-level, informal descriptions
  - Identifying key requirements, assumptions, and constraints
  - Towards a system, mission-level architecture

Tools for War Rooming

- Guiding concept for modeling
- Grounded in general systems theory and control theory
- Heuristics and guidance for identifying
  - Safety-related factors
  - Requirements
  - Operational assumptions

Hierarchical Control Model

Function



Responsibilities

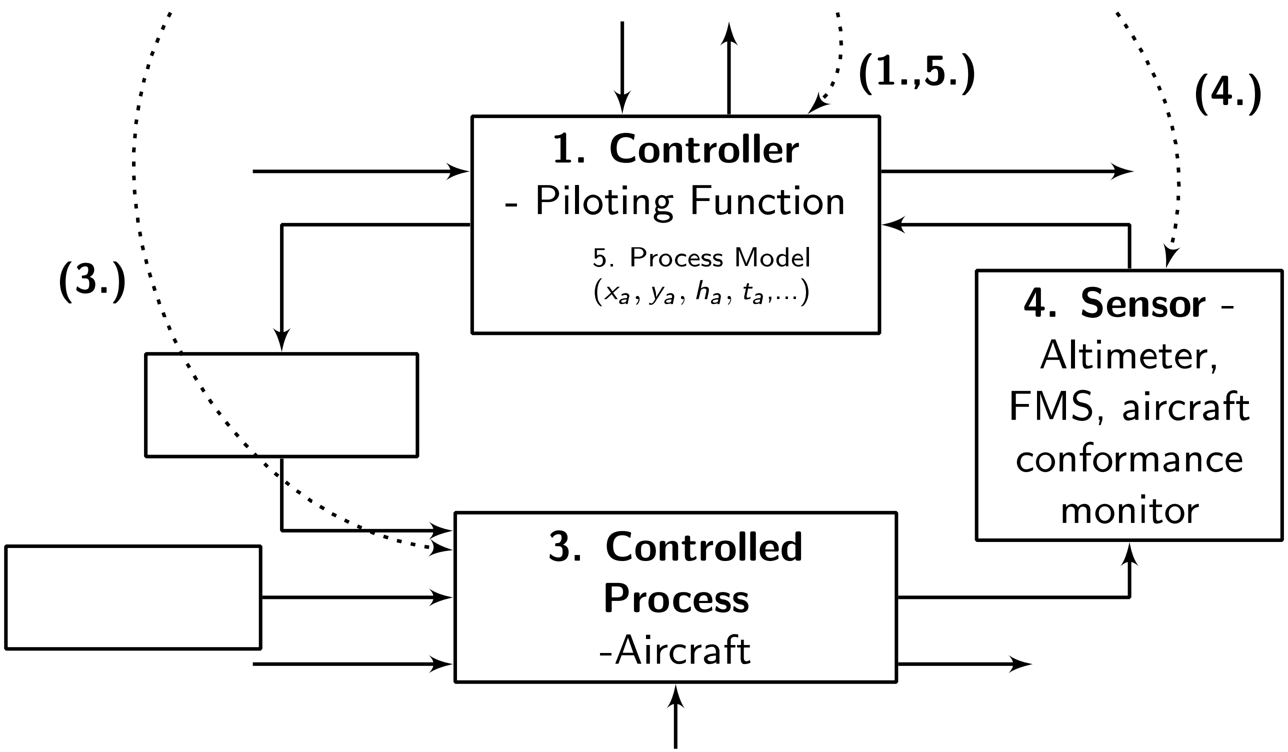
- Provide conflict-free clearances & trajectories
- Merge, sequence, space the flow of aircraft

- Navigate the aircraft
- Provide aircraft state information to rte planner
- Avoid conflicts with other aircraft, terrain, weather
- Ensure that trajectory is within aircraft flight envelope

- Provide lift
- Provide propulsion (thrust)
- Orient and maintain control surfaces

Mapping to Formalized Model

TBO conformance is monitored both in the **aircraft** *and on the* **ground** *against the agreed-upon 4DT. In the* **air**, *this monitoring (and alerting) includes lateral deviations based on RNP..., longitudinal ..., vertical..., and time from the FMS or other "time to go" aids. [JPDO, 2011]*



Thank you!

Questions?