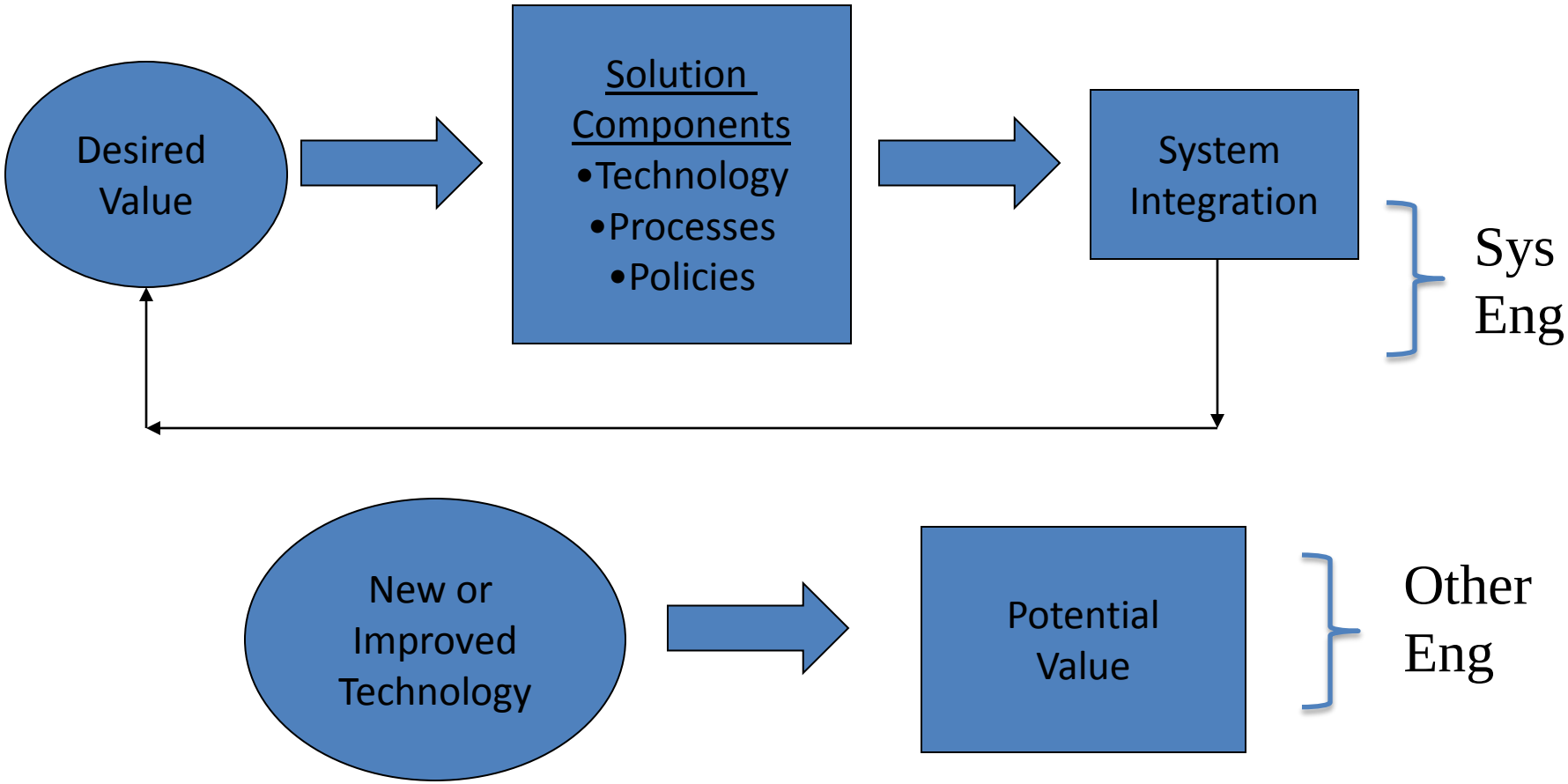
Transitioning Systems Engineering Research Results into Use

Barry Horowitz
University of Virginia
October 2014

Systems Engineering vs Other Engineering Departments



Transition Requirements

- Policy, Process and Technology Integration and Buy-in (3 Consumer Orientations, not 1)
- Harmonizing each of the 3 elements
- Managing and coordinating the sequencing of the transition process
- Managing the learning process and the needed modifications of the early ideas from 3 perspectives

Transition Requirements

- Policy, Process and Technology Integration and Buy-in (3 Consumer Orientations, not 1)
- Harmonizing each of the 3 elements
- Managing and coordinating the sequencing of the transition process
- From 3 perspectives, managing the learning process and the needed modifications of the early ideas

Usually Not Done

Instead Treated like Transitioning of Enabling Technology

Historical Examples

- Ada SW Std – Policy enacted before the technology was ready
- Fixed Price Contacting for Complex Systems – Frequently not well matched to technology/process
- Orange Book for Cyber Security – Transitioned well. But incompatible with the fast moving pace of SW technology

Hand-off Process for Transition

- Need the initial researchers to be sensitive to 3 dimensions of SE from the start, not only one.
- Need a continuous relationship manager to address the communities surrounding the 3 components of transition until the idea is transitioned - the entrepreneur for the SE solution
- Need a budget to support 3 transitions (policy/process/technology), not 1.

Current Emerging Example Related to Cyber Security

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)

Architecture Selection/Attack Trees

- Blue Team – 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 – 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

Process Implications

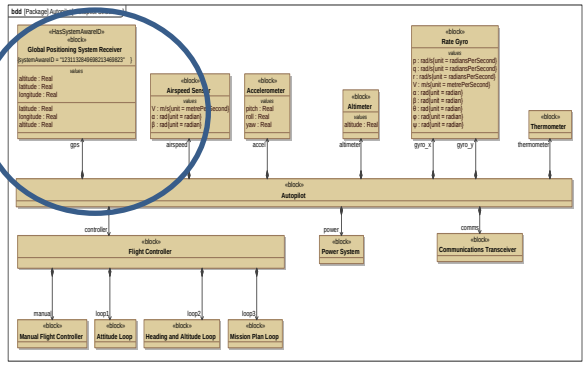
- Prioritizing system functions implies a mission focused approach to security vice a widget or subsystem approach
- Integrates red team attack assessments with blue team priority and defense solution assessments to derive integrated solution sets
- Brings together a decision team that accounts for Blue financial considerations as well as adversary responsive behaviors

Requires a set of integrated support tools to provide needed high fidelity inputs and supporting analysis

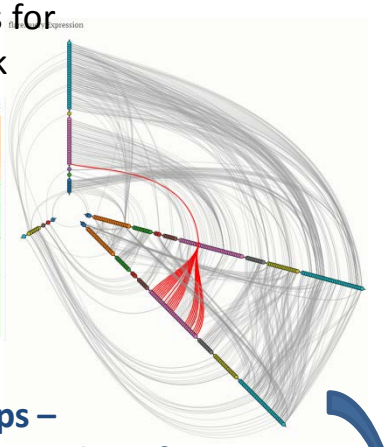
System Aware Cyber Security Framework: Process View 2.0

Step 1: Identify Critical Assets

SysML models of UAV
(High fidelity Model Semantics)



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

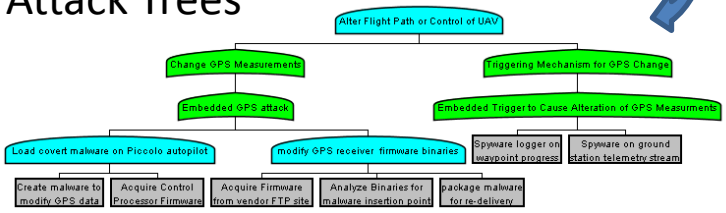


Visualization of System Relationships – Better Coverage of Attack Surfaces

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

Step 3: What is exploitable and by whom

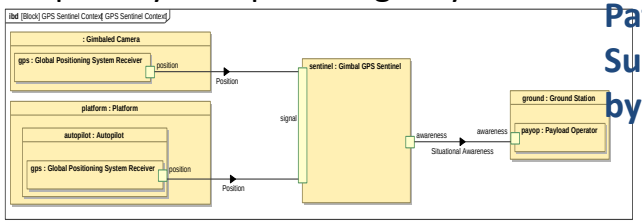
Attack Trees



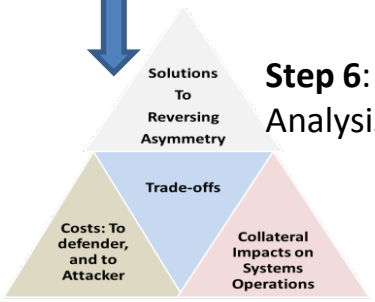
Output:
- Ease of Attack
- Capabilistic Propensity
- Relative Risk

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



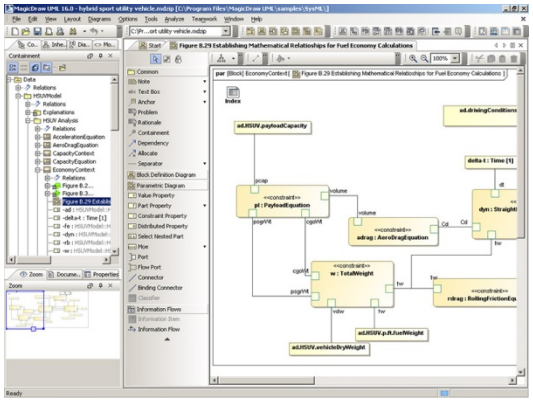
Decision making now aided with Easy to use Data Analysis/Visualization Tools

Architectural Assessment Workbench Concept

Model Creation Input
- Specs (what it does)
- Requirements (what is suppose to do)
- User domain (how people use it)
- Functional
- Use Cases
- Mission Context

Capture system to system interactions, Relationships with respect to different users and threat agents

SysML *MagicDraw*

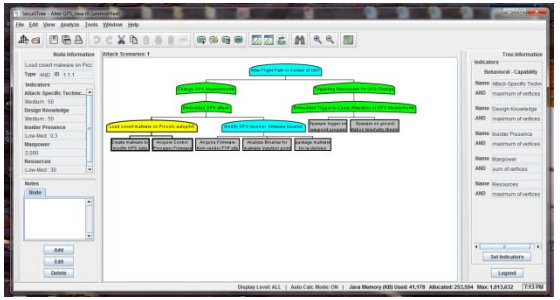


XMI
Extensible Model Interchange

Model Creation Input
- Data on vulnerabilities
- Path analysis
- Sequences
- Component UUID

ATML
Attack Tree Markup Language

Attack Tree *SecureITree*

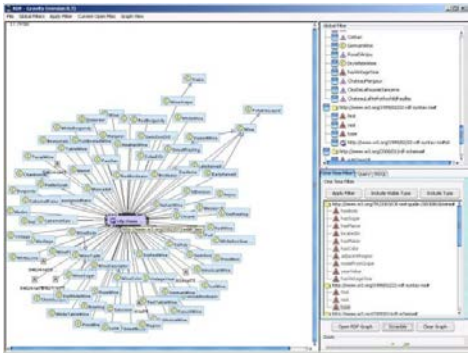


ATML

CSV
Comma Separated Values

Trade-off/Cost benefit Analysis
- Cost of Attack to Attacker
- Cost of Defense
- Collateral Costs
- Lifecycle Costs

Knowledge Graph *RDF*



Visualization *IPython*

CSV

Reports
- Attack trees
- Ease of Attack
- Capabilistic Propensity
- Relative Risk

The Transition Approach is in Motion Before the Proof of Value is Completed

- Policy: Work is funded by OSD, where it has already been exposed to a variety of policy stakeholders
- Process:
  - To minimize user issues, the research project has engaged tool users as prototype developers of the tool integration approach
  - For early feedback, a work shop is being conducted with Navy 10th Fleet (Cyber Command) and Navy Info Ops to expose the concept of tool integration to support decision-making
- Technology:
  - Started engaging with tool vendors to gain interest in tool integration as part of their product lines
  - Started exposing the process approach to cybersecurity service companies to gain their interest and initiative