SYSTEMS ENGINEERING RESEARCH CENTER

Methods to Evaluate Cost/Technical Risk and Opportunity Decisions for Security Assurance in Design

Sponsor: OUSD(R&E)

By
Tom McDermott, Megan Clifford (Stevens)
Cody Fleming, Georgios Bakirtzis, Tim Sherburne (University of Virginia)

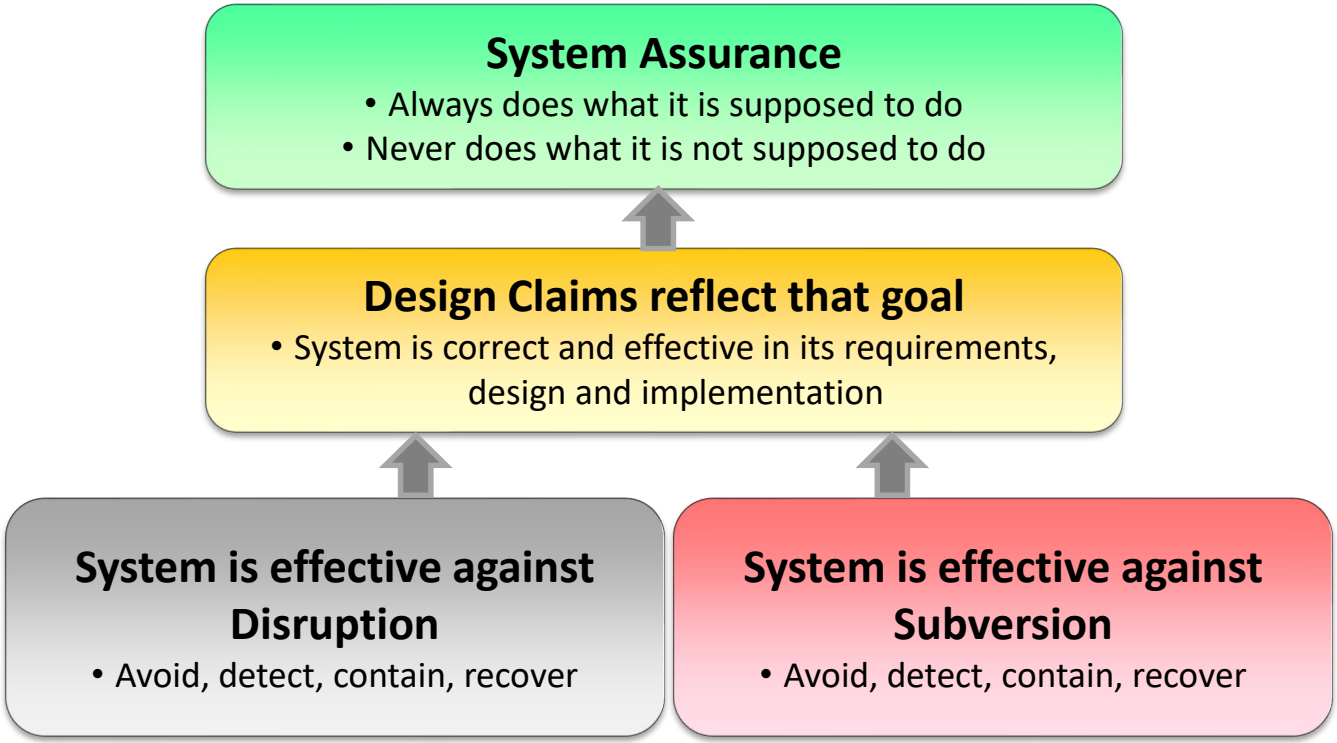
11th Annual SERC Sponsor Research Review
November 19, 2019
FHI 360 CONFERENCE CENTER
1825 Connecticut Avenue NW, 8th Floor
Washington, DC 20009

www.sercuarc.org

SYSTEMS ENGINEERING RESEARCH CENTER

Need the capability to formally assess security in the assurance design process

What is the risk/likelihood/cost of the attack?



How does the CPS design assure acceptable risk?
And at what Cost/Effort?

Expand System Aware: Rigorous Functional Security Analysis and Modeling Process

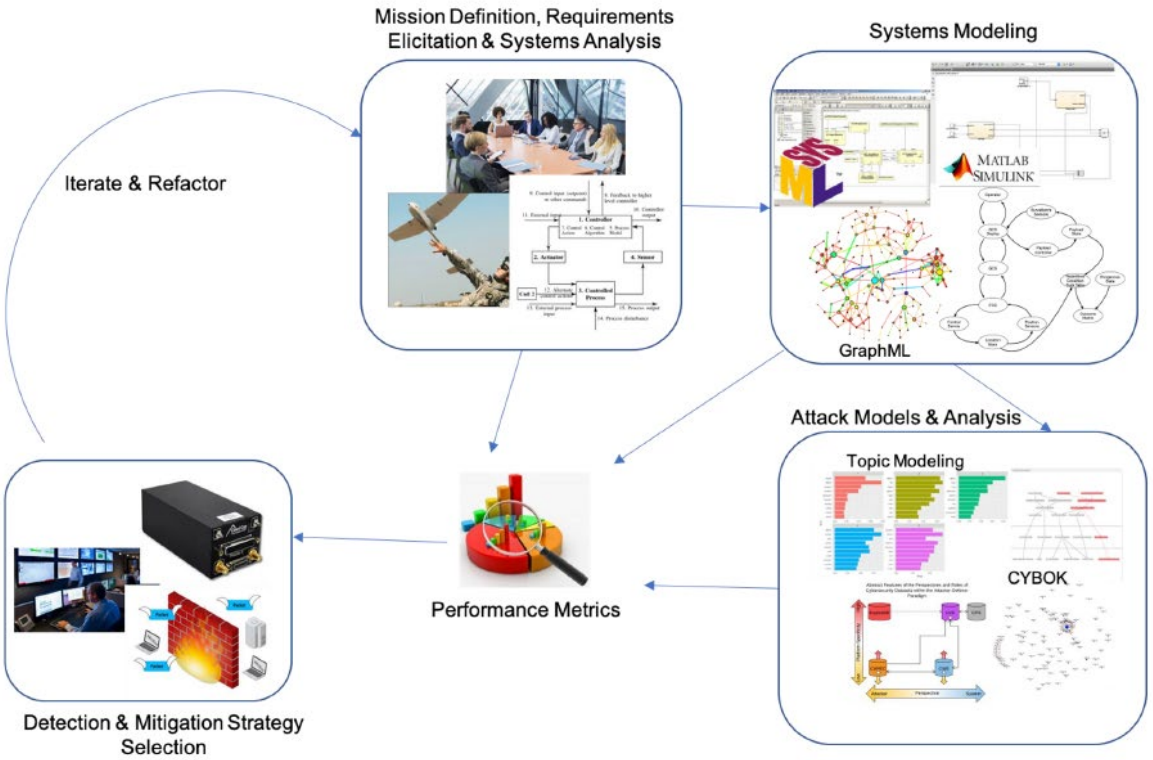
Standardize System Assurance Case Development and Analysis across safety/reliability/security design

Further explore system & threat models related to assurance case language

Create reference threat descriptions in engineering terms (Conops)

Evaluate useable cost/risk metrics that bridge system and threat Conops

Develop quantitative approaches and metrics to trade design versus “acceptable risk”

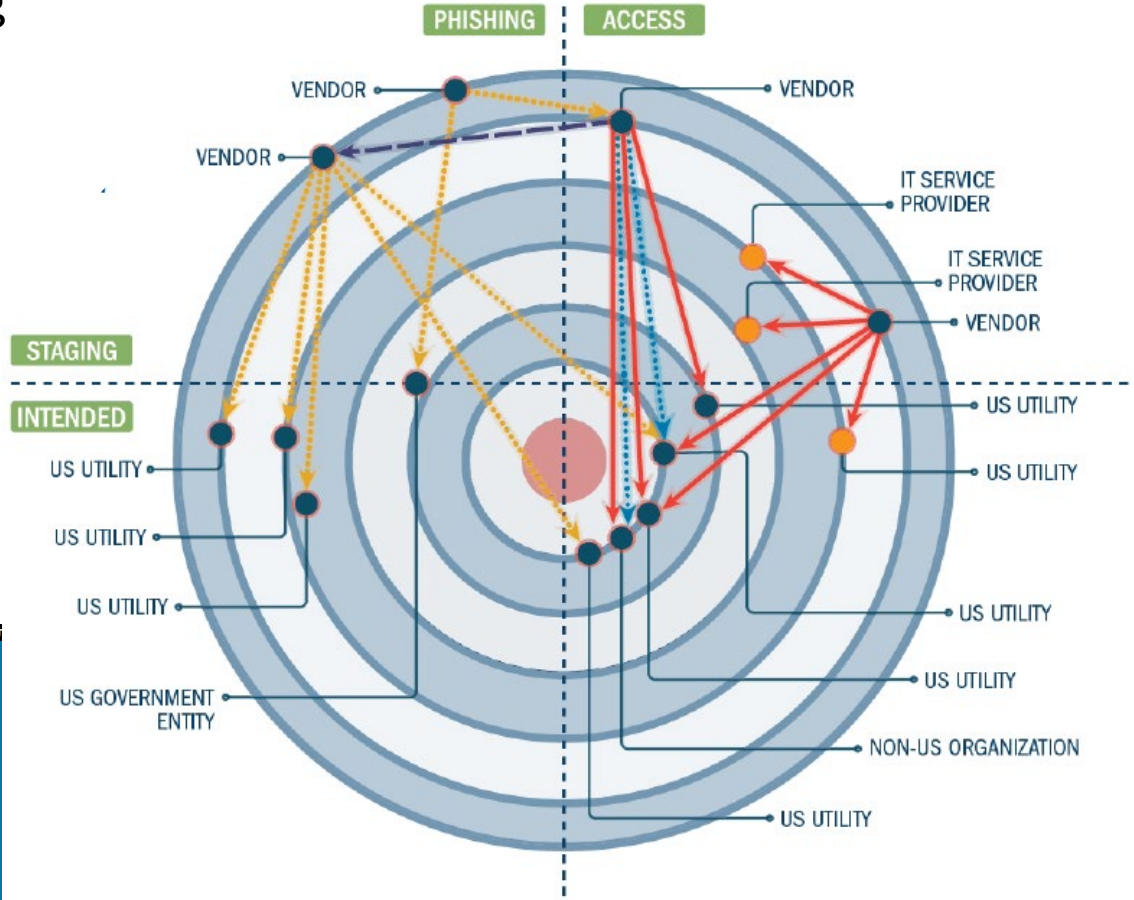


ART-004 Security Assurance in Design Research Goals

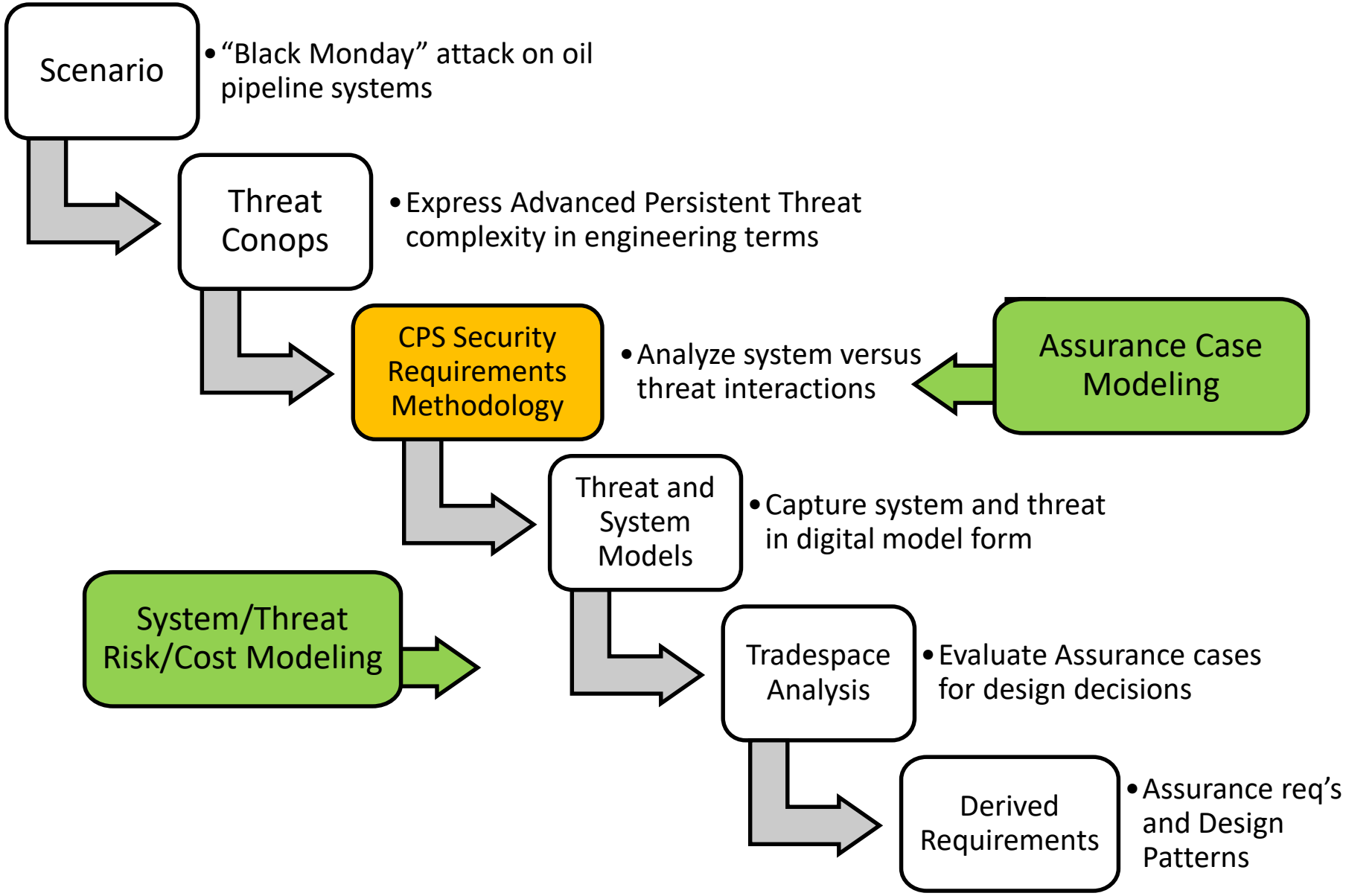
- Assess current research and tools supporting system hazard/risk, vulnerability, security, and cost analysis approaches to inform candidate evaluation methods and models.
- Select and/or develop candidate system assurance methods that can be integrated into the systems engineering process that meets the necessary evidence building and decision structures for critical systems. The methods and tools should be based on existing MBSE frameworks.
- Develop candidate metrics that effectively represent system vulnerabilities, costs to mitigate those vulnerabilities, costs to the attacker to exploit system vulnerabilities, and the overall impact on systems performance goals. Evaluate these metrics for effectiveness and decision support in a sample design case, taking into account risk and overall impact on mission resilience goals.
- Develop a plan for incorporation of the selected metrics and methods into a full-scale pilot on a representative mission critical system.

Advanced Persistent Threat in Critical Systems

- Social Engineering
  - —Research, data harvesting
  - —Credential harvesting
- Physical Engineering
- Vulnerabilities
  - —SCADA zero day
- Push Rogue logic
- Execute outcomes
  - —Lack of predictive models



ART-004 Security Assurance in Design Project Activities



Black Monday Scenario

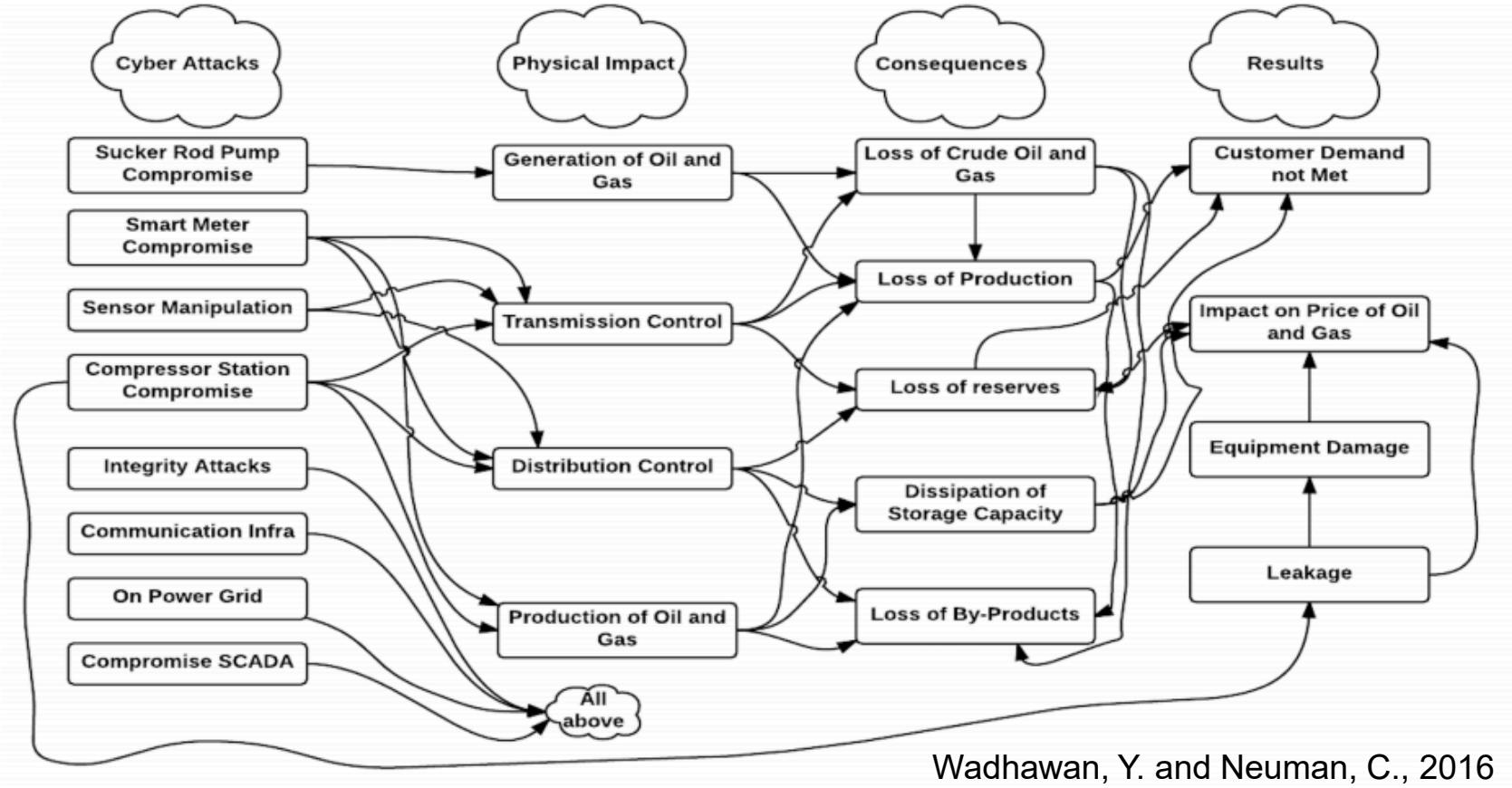
Developed by students in Ga Tech Sam Nunn School of International Affairs, Scenario Building class

- Posited cyber attack on Saudi Aramco Riyadh & Yanbu, Baiji (Iraq), and SPC refineries
- Fancy Bear (Russian hacker group) gains remote access to refinery controls
- Report false flow rates, pressure, temperature of trunk lines
- Russian refineries report “similar spills” as time goes on, and come out with malicious code “found” in their own refineries, solving the irritation plaguing the three countries
- Russia offers world-class cyber security services to all three countries - but also installs backdoor measures to take control in future
- Used to manipulate critical pipeline pumping stations to refineries, attacks degrade flow
- Causes yield of oil decreases by 6.2m barrels/day (Overall 10% decrease in global oil availability)
- 50% price of oil increase for 30 days estimated at $31B market price impact
- Significant profits in oil futures

Complexity of the Attack Scenario

The Modern oil and gas cyber-physical systems incorporate information and communication technologies for improving wide area control, maintaining situational awareness and controlling physical processes remotely.

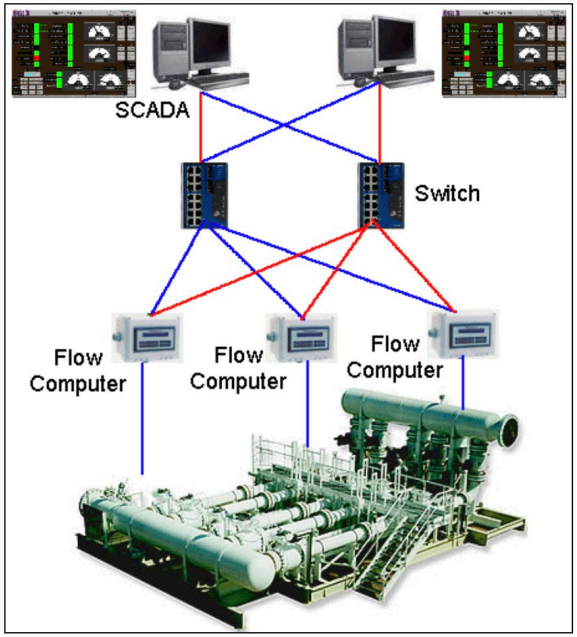
A multilevel attack incorporating numerous segments with persistent threat on SCADA and ICS is most feasible for scenario.



Wadhawan, Y. and Neuman, C., 2016

Oil Pumping Network Scenario

- Coordinated attack on multiple stations
  - Pump control
  - Pipeline monitoring
  - Distributed control system
  - Leak detection systems
  - Control centers
  - Maintenance operations



Metering System

- When and where is critical (APT)
  - Pump location and maintenance cycles
- Distributed stakeholder set, lack of System-of-systems view
- Developing Conops document format to capture complexity of the SoS and threat in systems engineering terms

Assurance Methods and Cases

- Verification and validation of mission-critical systems through test and evaluation has historically been the gold standard for assurance
  - Significantly expensive and increasingly fraught with difficulty as systems become more complex, more expansive, and more inter-dependent on other systems to realize their intended capabilities.
- Assurance cases capture subjective judgment through *claims* supported by evidence, and make explicit the context, including:
  1. System architecture
  2. System environment
  3. System expected service
- Largely informal, with purpose to not replace methods and tools from reliability, dependability, and safety, but rather to reveal the relationship of such analyses with their higher level claims within design and acquisition process.
- Ineffective when used as check lists to adhere to safety standards.

The current state of practice in system assurance is in need of a paradigm change.

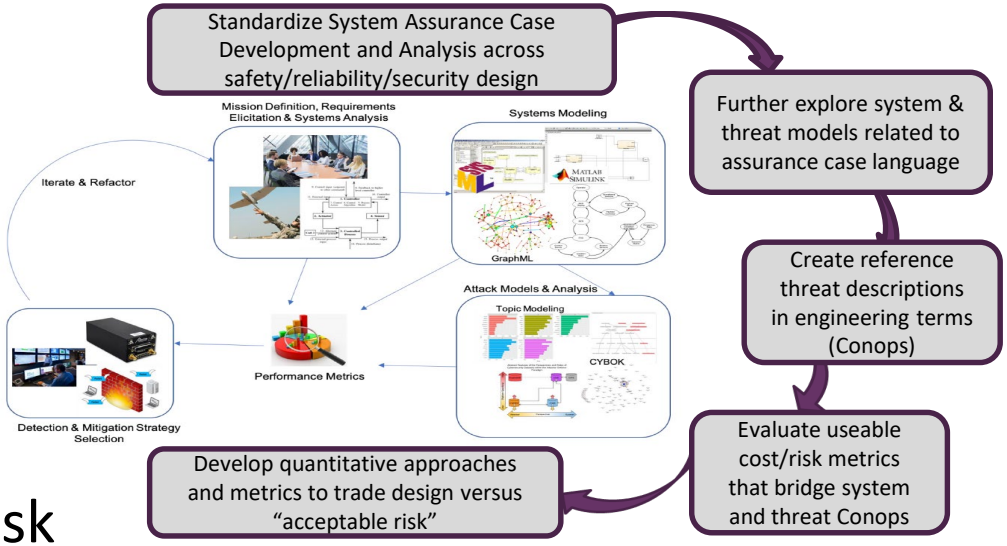
Assurance Case Modeling

Model-Based Assurance Methods for Cyber Test and Evaluation

System-Theoretic Accident Model and Process (STAMP) & System Theoretic Process Analysis – Security (STPA-Sec)
Addresses shortcomings of linear failure models. Applied to accident analysis and prevention as well as general dependability and security design of CPS with STPA-Sec.
Fault and Attack Trees/Graphs
Graphical representation of various parallel and sequential combinations of errors.
Architecture Analysis and Design Language (AADL) and Resolute Case Language
Model-based assurance leveraging AADL to capture system architecture to be processed and validated against system requirements. Developed Resolute assurance case modeling tool for formal cases.
ModelPlex
Formal verification and validation providing correctness guarantees for CPS executions at runtimes.
Six-Step Model (SSM) and SSM with Informational Flow Diagrams (IFDs)
Created for CPS safety and security analysis incorporating six hierarchies of CPS. Integration with IFDs for modeling, but prove inefficient for identification of failures and attacks.
Formal Methods transfer to CPS
Field of its own, but rapid integration currently occurring between formal methods and the control engineering communities.

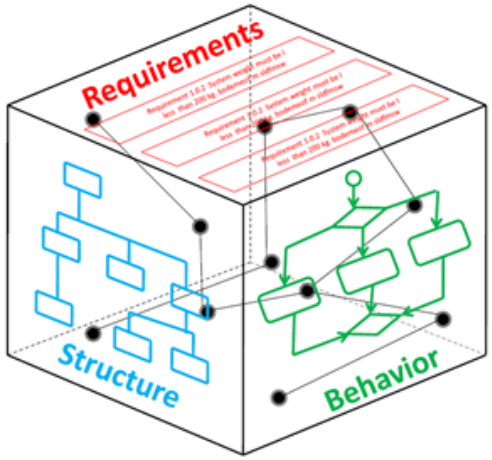
Integrating Assurance into the Analysis

- Improvement through integrating functional and formal design methods with consideration for advanced persistent threat.
- The model, with all levels of abstraction, represents accurate system functional performance and characteristics up to the mission operational level.
  - —Bridging system and threat Conops to create and evaluate useable cost/risk metrics
- Reveal better integration into assurance case arguments and documentation with quantitative approach to tradespace vs. acceptable risk



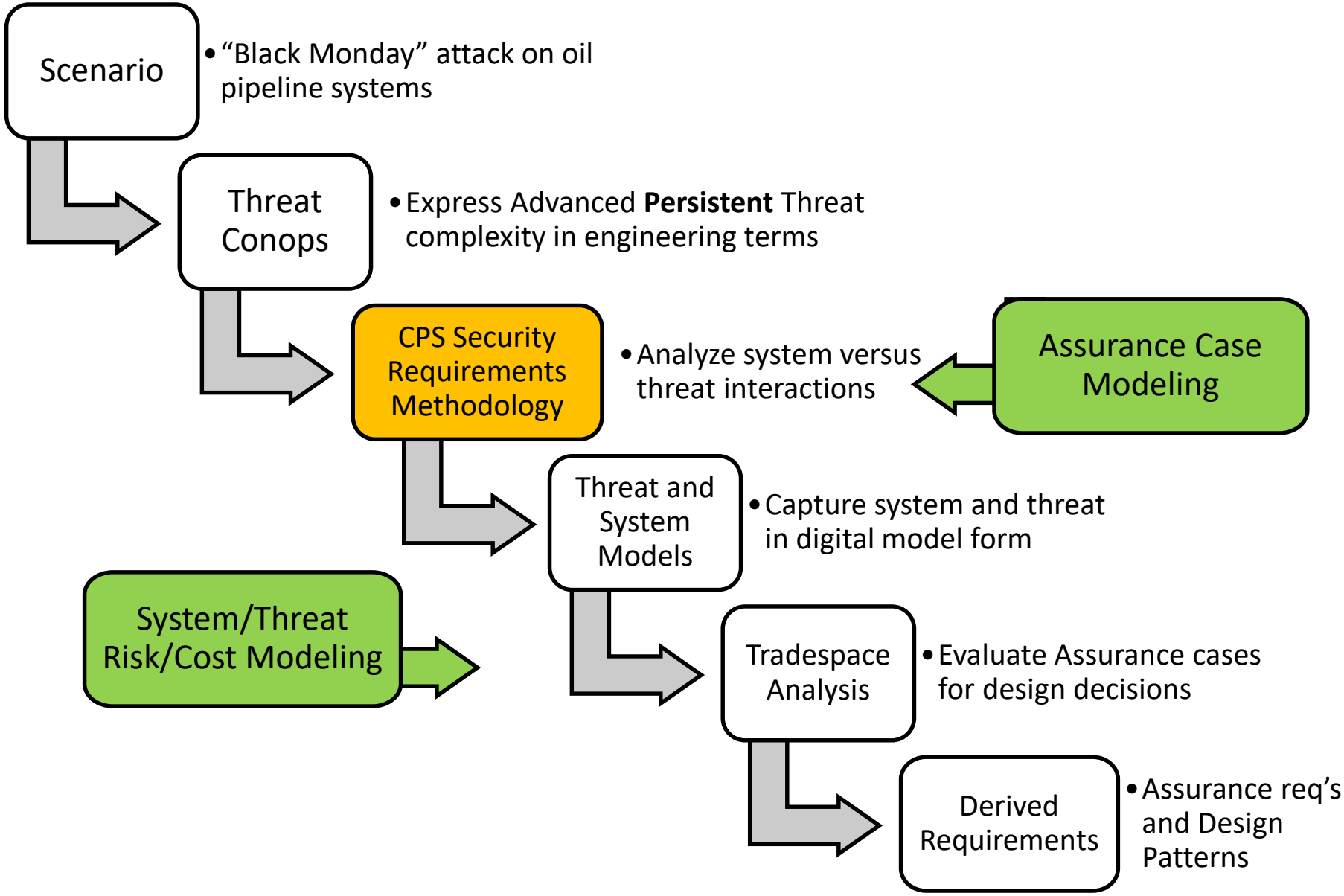
Linking system cost/risk to threat benefit/opportunity

- We need relevant scenarios
  - Relevant, interesting geo-political-conflict opportunities
  - With thought to the complexity of how they will be conducted
  - With a perspective and top level analysis of cost-benefit to the attacker



- What cost formalisms / best practices within do we need to specify for this approach to work?
  - Cost-benefit analysis
  - Loss cases, vulnerability cases, probability of attack
  - Countermeasure cost estimating relationships
  - Game theoretic simulations for predictive modeling

Continuing Efforts



Questions?

Thank you!