RT-196:

Peter Beling[1] (PI), Cody Fleming[1], Barry Horowitz[1], Bryan Carter[1],
Stephen Adams[1], Carl Elks[2], Georgios Bakirtzis[2]
[1]Department of Engineering Systems and Environment, University of Virginia
[2]College of Engineering, Virginia Commonwealth University

Research Task / Overview

- We aim to develop a top-down analysis and modeling methodology that takes a mission-centric viewpoint to cyber resiliency of cyber-physical systems. This work extends RT-172 [1]. The proposed approach combines (a) stakeholder inputs from system experts, (b) models of system architecture and behavior based on those inputs, and (c) attack and vulnerability analysis techniques to identify the most appropriate and effective resiliency solutions to help ensure mission success.
- Identifying appropriate detection and mitigation strategies requires a three-pronged approach that:
  1. Understands the mission goals, requirements, and operational intricacies,
  2. Accurately represents system behavior and architecture to quantify potential pathways to adverse mission outcomes, and
  3. Characterizes the potential threats to the system.

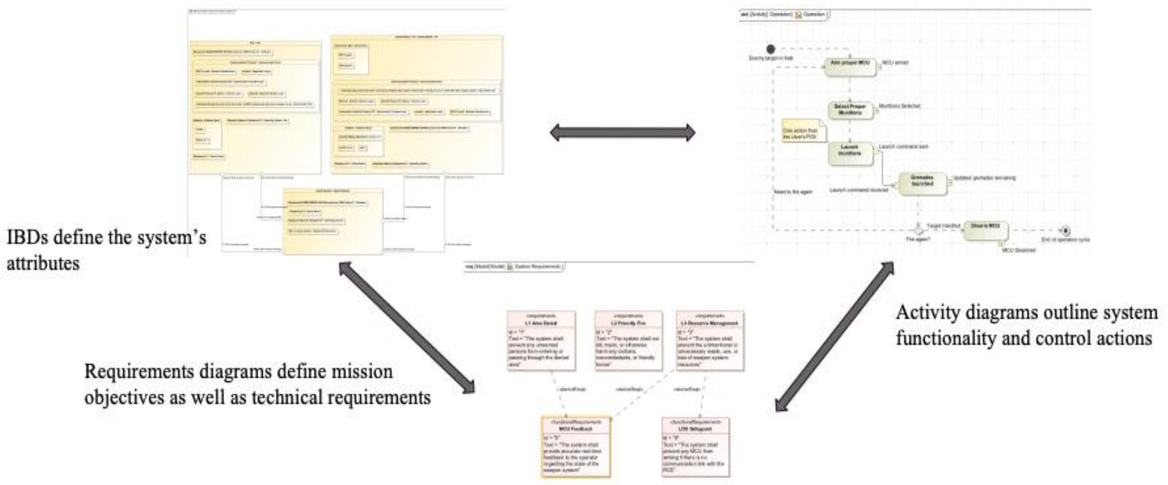
  These components work in concert to motivate the selection of resiliency solutions based on performance, compatibility, and evidence.

Goals & Objectives

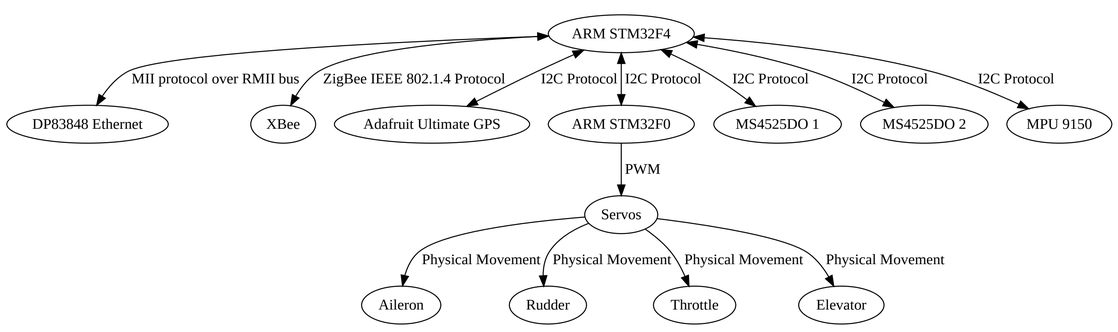
- Explore and develop methods to select and evaluate appropriate cyber defense strategies for Cyber-Physical Systems
- Develop tools to aid system analysis and selection of cyber defense strategies
- Establish protocols and techniques for eliciting relevant mission information from stakeholders
- Understand the consequences of potential attacks on mission integrity
- Develop a model driven approach to vulnerability and consequence assessment
- Formalize modeling techniques and schemas to enable the creation of accurate, precise, and repeatable models
- Develop and identify key performance metrics to motivate the selection of specific detection and mitigation strategies

Data & Analysis

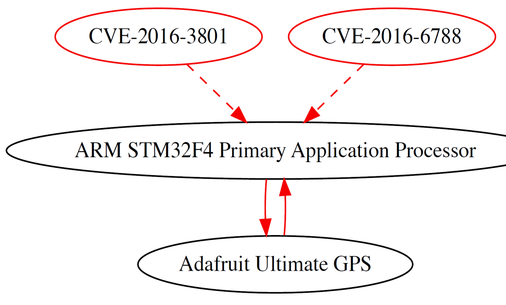
- Various stakeholders work together to define the mission, its requirements, unacceptable outcomes, and relevant operational procedures

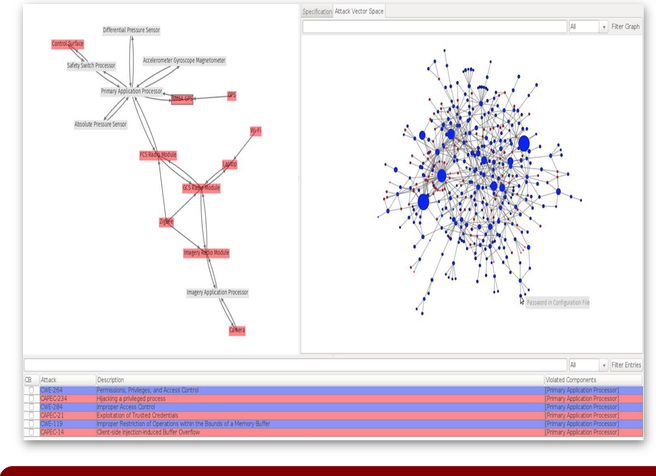


- SysML models encode mission information, requirements, and architectural characteristics in a navigable format
- A SysML to GraphML parser generates a meta-model for input into the CYBOK tool



- Vulnerabilities from CYBOK linked to elements in system architectural model highlight a potential area for implementing defense and mitigation measures
- The requirements graph shows the potential pathways for a vulnerability to create mission-level consequences

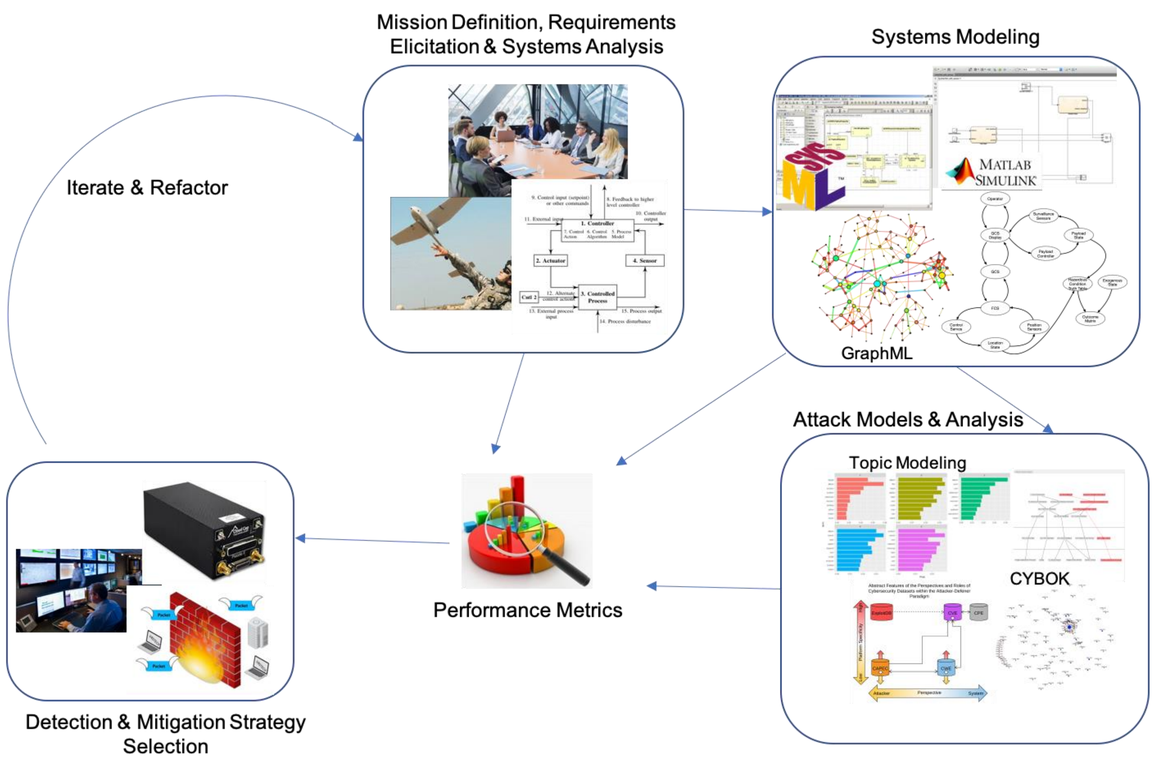




- A visualization environment used to assist cyber analysis from a model based perspective.
- Goal is to provide security engineering feedback early in design and development or procurement cycle

Methodology

1. Engage stakeholders to define, develop, and understand mission requirements, consequences, and operational procedures [2]. Use Systems-Theoretic tools to organize the gathered information into an analyzable format.
2. Take a multi-tool approach to modeling system requirements, behavior, and architecture to create a traceable, holistic model.
3. Analyze the system models using existing attack and vulnerability databases and natural language processing techniques (e.g. topic modeling [3]) to generate an evidence-based cyber-risk profile of the system.
4. Identify and evaluate the requirements, models, and risk profile against a set of performance metrics
5. Select detection and mitigation strategies based on the performance metrics
6. Iterate and refactor using the "new" defended system



Future Research

- Formalization of graph representations of system models
- Algorithms for analysis of system model graphs to identify the mechanisms and pathways for adverse mission outcomes
- Automated tools for analysis and selection of detection and mitigation strategies
- Develop and maintain a repository of detection and mitigation strategies and their associated model representations to streamline future analysis on other systems

References

1. Horowitz, B., Beling, P., Fleming, C., Adams, S., Carter, B., Vemuru, K., ... & Collins, A. (2017). *Security Engineering FY17 Systems Aware Cybersecurity*. Stevens Institute of Technology Hoboken United States.
2. Carter, B. T., Bakirtzis, G., Elks, C. R., & Fleming, C. H. (2018, April). A systems approach for eliciting mission-centric security requirements. In *Systems Conference (SysCon), 2018 Annual IEEE International* (pp. 1-8). IEEE.
3. Adams, S., Carter, B., Fleming, C., & Beling, P. A. (2018, August). Selecting System Specific Cybersecurity Attack Patterns Using Topic Modeling. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 490-497). IEEE.