2025 - AIP - RNC-MJV - Simulating Risks & Impacts of Cyberattacks on Critical Infrastructure - gmaduwub@purdue.edu - Gerald Maduwuba

CERIAS

The Center for Education and Research in Information Assurance and Security

Simulating Risks & Impacts of Cyberattacks on Critical Infrastructure

Aashi Agarwal, Kanari Hirano, Gerald Maduwuba, Courtney Falk, Rick Kennell

MOTIVATION

The Cyber Adversary Likelihood project has the goal of identifying methods for modeling adversaries in attacks on critical infrastructure, using those models to help determine the likelihood of various adversary actions. Specifically, the project will examine threat actors in the context of cyber systems (including information systems and control networks) and propose modeling approaches to approximate their behaviors. The project will develop a method to estimate likelihoods of various adversary actions in relevant contexts and then characterize and demonstrate that method. The ultimate use case of the model(s) and tool(s) is to estimate likelihood parameters in a broader model that will be used to assess risk to critical infrastructure from malicious and natural hazards.

Critical Infrastructures Overview

- DHS identifies 16 critical infrastructure sectors that are vital to national security, economy, and public health and safety
- To help develop effective cyber defenses and mitigations, we estimated potential risks associated with cyberattacks within three of these sectors:
  - ➢Healthcare
  - ➢Energy
  - ➢Water and Wastewater
- We developed models using an object-oriented programming approach (Java) in the AnyLogic software package
- To run simulations of cyberattacks on our models, we configured parameters for systems and adversaries and measured associated risks
- Due to the dependencies between sectors, we also analyzed the cascading impacts of attacks in one sector on others by building a combined unified model

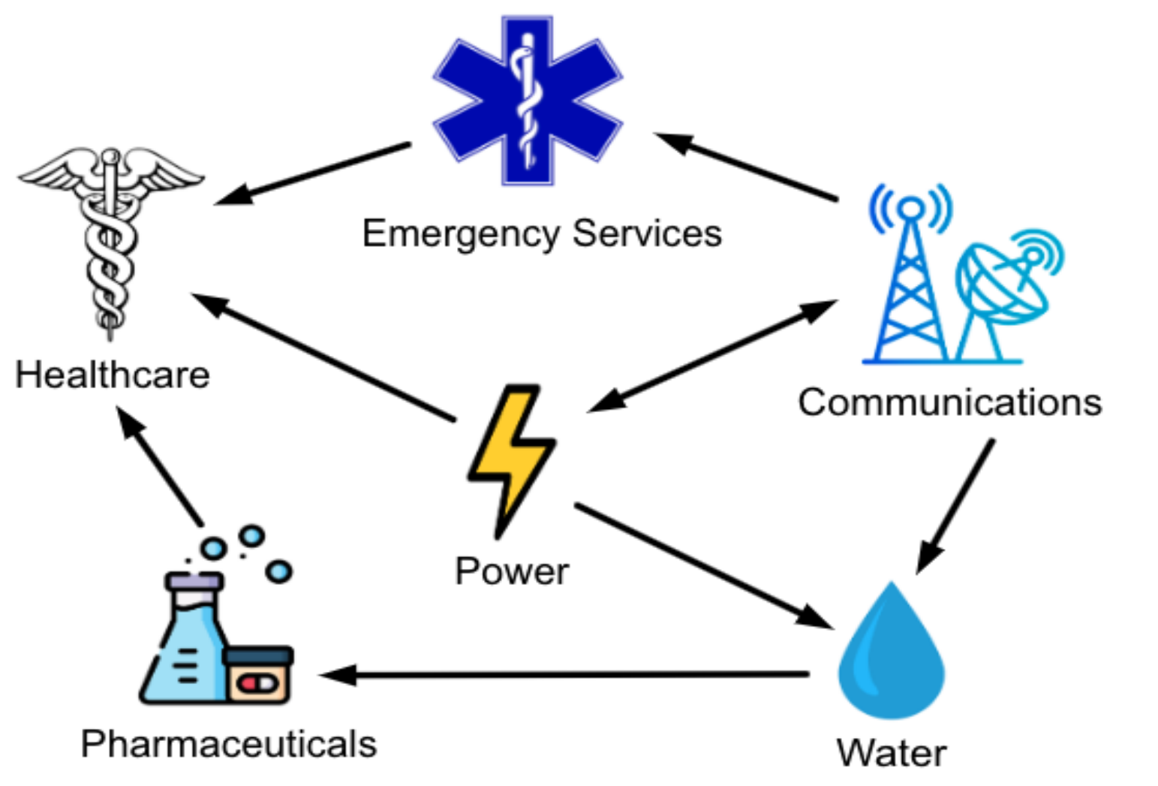

Figure 1: Dependencies between the Power, Healthcare, and Water Sectors.

Energy Sector

- Electric power plays a central role in modern life
- Foreign nation-state hackers are targeting power generator stations (e.g., Ukraine, 2015)
- Power generation facilities and the power grid rely on ICS
- Electric power sector relies on a combination of legacy systems like Modbus and DNP3, and newer principles such as Network Segmentation and Secure-by-design principles
- Difficult implementation due to increased latency, system requirements, and cost of maintenance downtime.

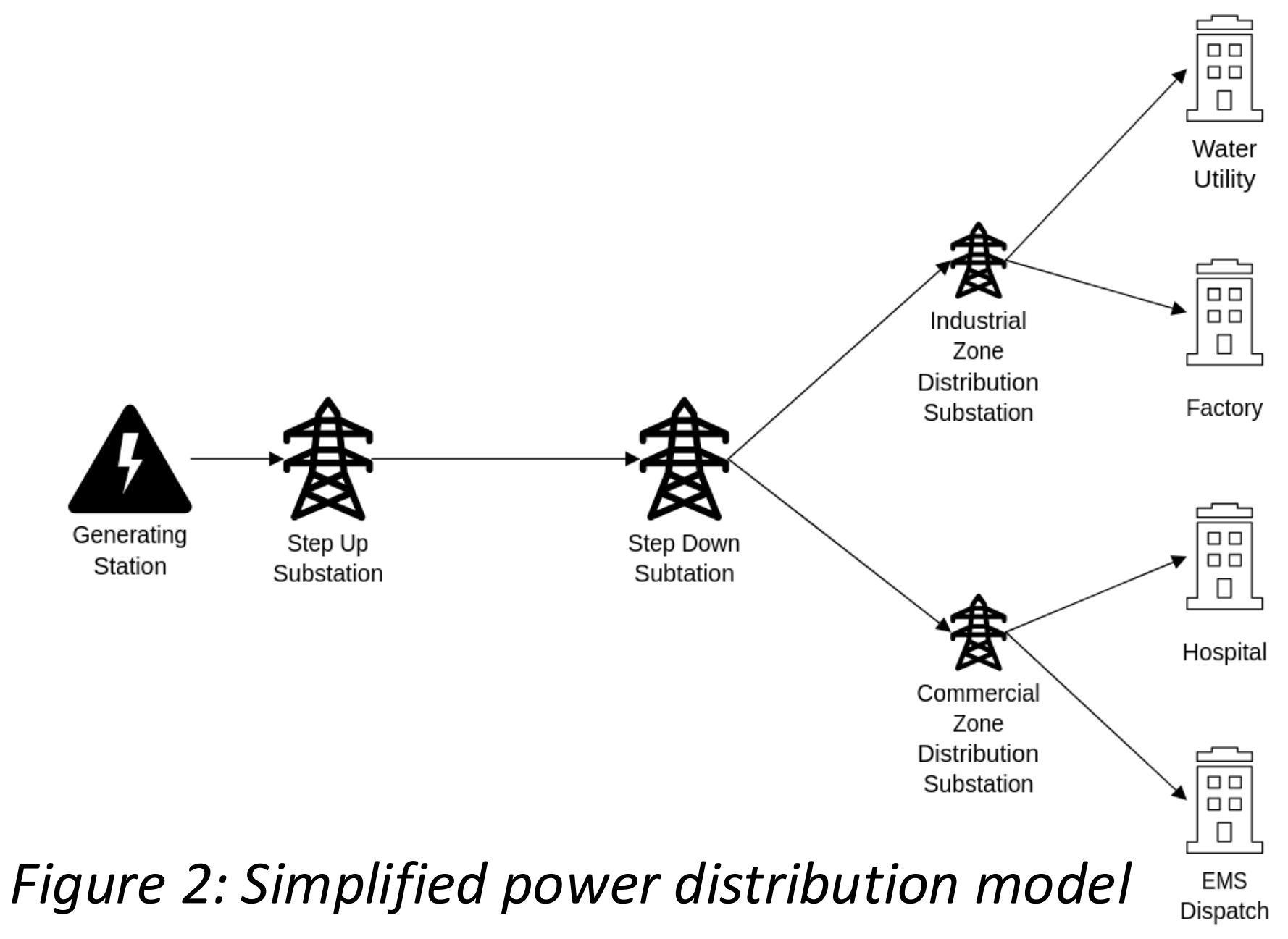

Figure 2: Simplified power distribution model

Water and Wastewater Systems

- Access to a reliable supply of clean water is essential for public health
- Foreign nation-state hackers are increasingly targeting water and wastewater treatment (WWS) facilities (e.g., Texas, 2024)
- WWS treatment facilities and transportation infrastructure rely on ICS to control OT such as sensors, valves, and pumps
- Typical WWS network architectures still overlap IT and OT networks, posing security risks for legacy ICS devices
- Our model measures multiple risk factors including water quality, flow rate, and overflow

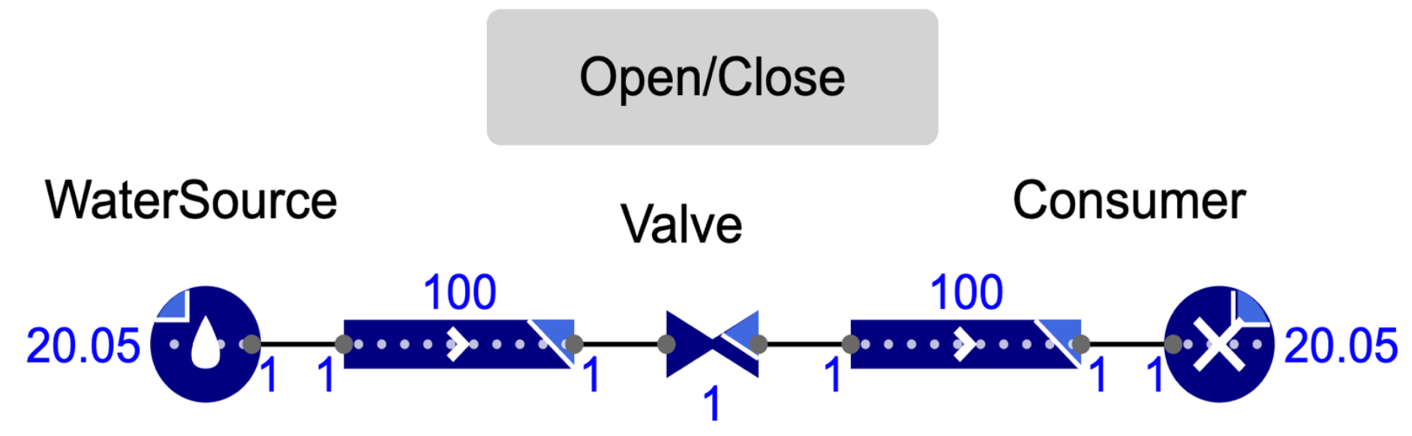

Figure 3: Simplified water system model on AnyLogic software which features a single valve controlled by a switch.

Healthcare Sector

- The Healthcare and Public Health (HPH) sector leverages technology to store medical and patient information like personally identifiable information (PII) to properly care and communicate with their people (e.g., CISA, 2025)
- Smaller hospitals are an even bigger target for cyberattacks as they lack the resources, systems, and staffing to build an effective security posture to protects themselves as larger hospitals can
- Cybersecurity awareness and safety protects a patient's safety

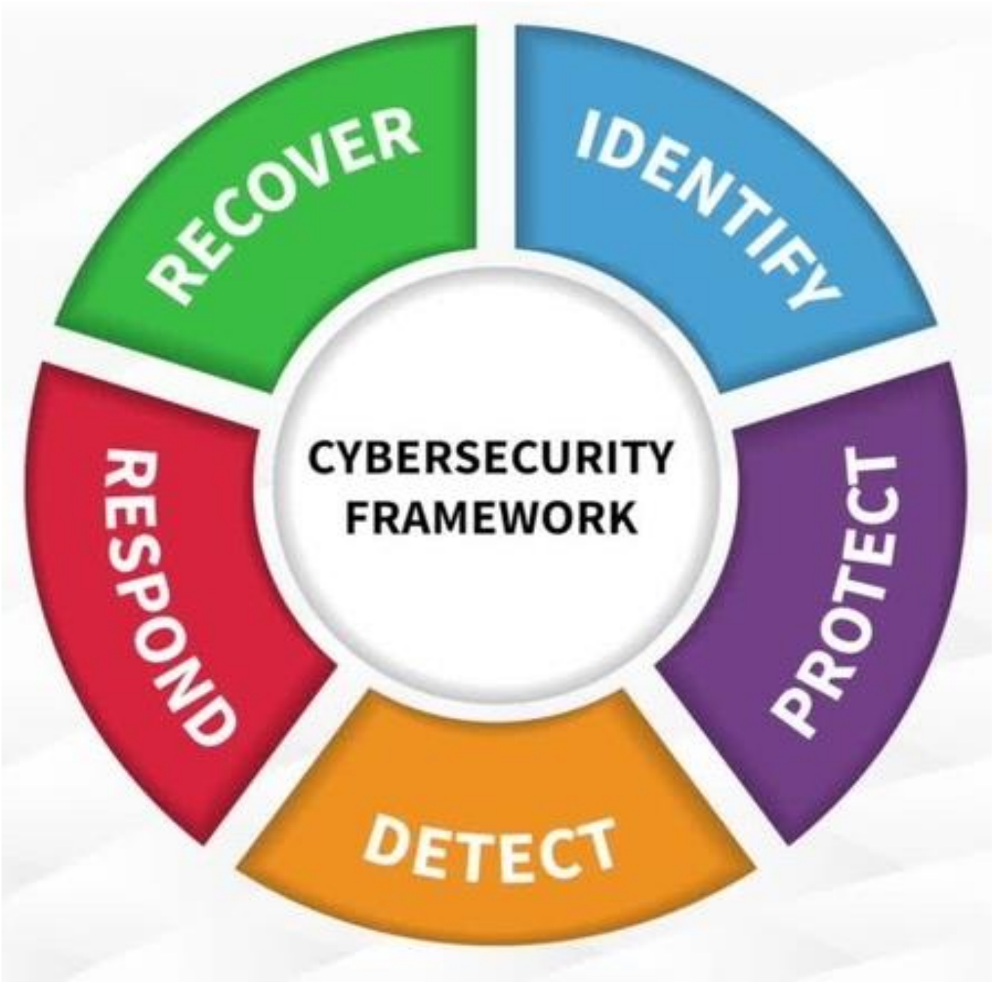

Figure 4: NIST's Cybersecurity Healthcare Industry Framework

- Disorders in the basic operations of a hospital will impact:
  - ➢ Loss of PII, endangering patient safety & confidentiality
  - ➢ Patient's overall health, as care for them will be delayed
  - ➢ Reputation, paints a negative image for the hospitals

PURDUE UNIVERSITY

CERIAS