Severe Impact Resilience: Assessment Framework for Compound Threats

Presenter: Dr. Amy Babay, University of Pittsburgh

Project PI: Dr. Imes Chiu, USACE–ERDC—CERL

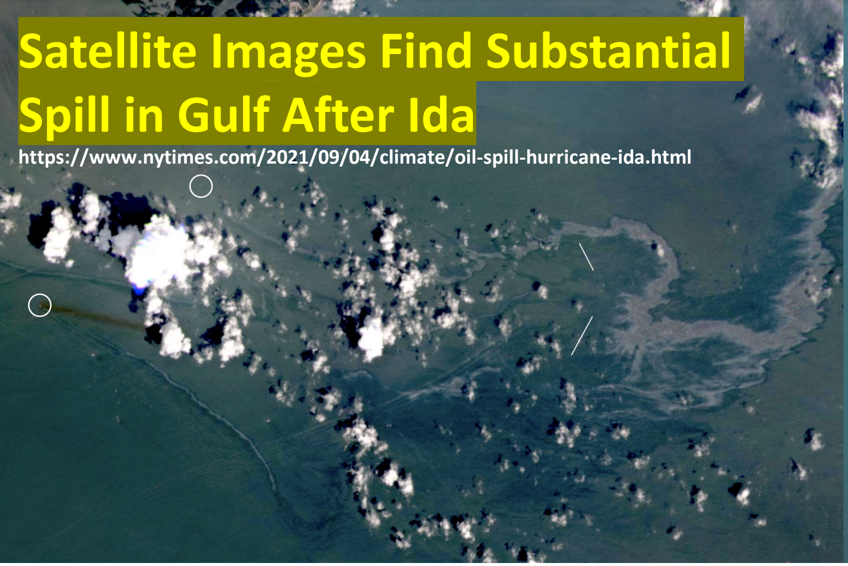
SERDP•ESTCP SYMPOSIUM
2021 • Enhancing DoD's Mission Effectiveness

Project Team

- PI: Dr. Imes Chiu, US Army Corps of Engineers—Engineer Research and Development Center—Construction Engineering Research Lab
- Co-PIs: Dr. Amy Babay[1], Dr. Yair Amir[2], Dr. John van de Lindt[3], Dr. Mathaios Panteli[4], Dr. Linton Wells II
- Students: Benjamin Gilby[1], Maher Khan[1], Sahiti Bommareddy[2]
- [1]University of Pittsburgh, [2]Johns Hopkins University, [3]VDL Risk Solutions LLC, [4]University of Cyprus

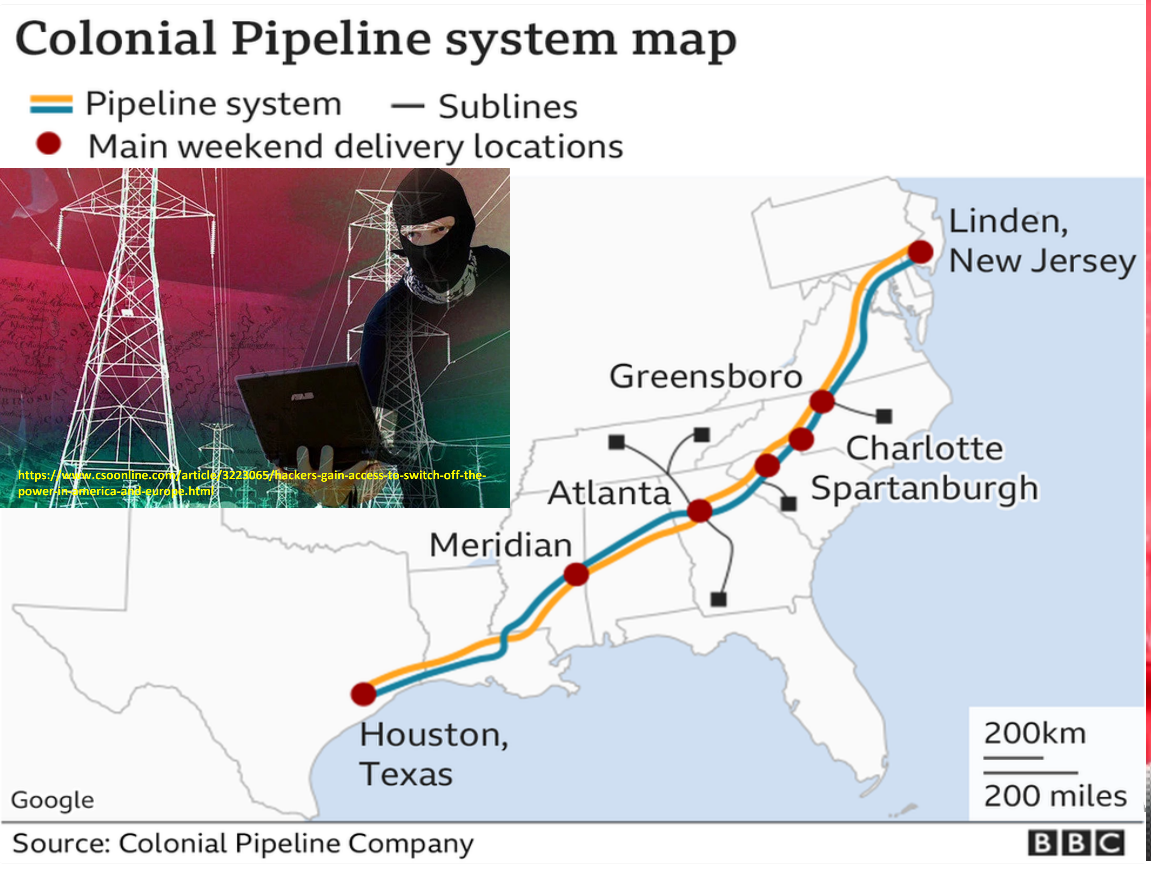
Motivation

- The joint threats of increasingly frequent and severe **natural disasters** and increasingly sophisticated **malicious cyberattacks** pose a serious threat to US **critical infrastructure systems**
- **Compound threats**, involving both natural hazards and cyberattacks (which may exploit hazard conditions to cause further infrastructure damage or prolong recovery) are not well understood today
  - impact on control systems (micro-level)
  - impact on surrounding communities (macro-level)
- As these threats become increasingly realistic, it is crucial to build infrastructure systems that can withstand them with minimal disruption


Satellite Images Find Substantial Spill in Gulf After Ida
https://www.nytimes.com/2021/09/04/climate/oil-spill-hurricane-ida.html


https://www.nytimes.com/2021/09/04/climate/oil-spill-hurricane-ida.html


BP oil spill led to baby dolphin deaths and diseases along the Gulf Coast. Truth Wire


Colonial Pipeline system map
Pipeline system
Sublines
Main weekend delivery locations
Linden, New Jersey
Greensboro
Charlotte
Spartanburgh
Atlanta
Meridian
Houston, Texas
200km
200 miles
Google
Source: Colonial Pipeline Company
BBC
https://www.csoonline.com/article/3223065/hackers-gain-access-to-switch-off-the-power-in-america-and-europe.html

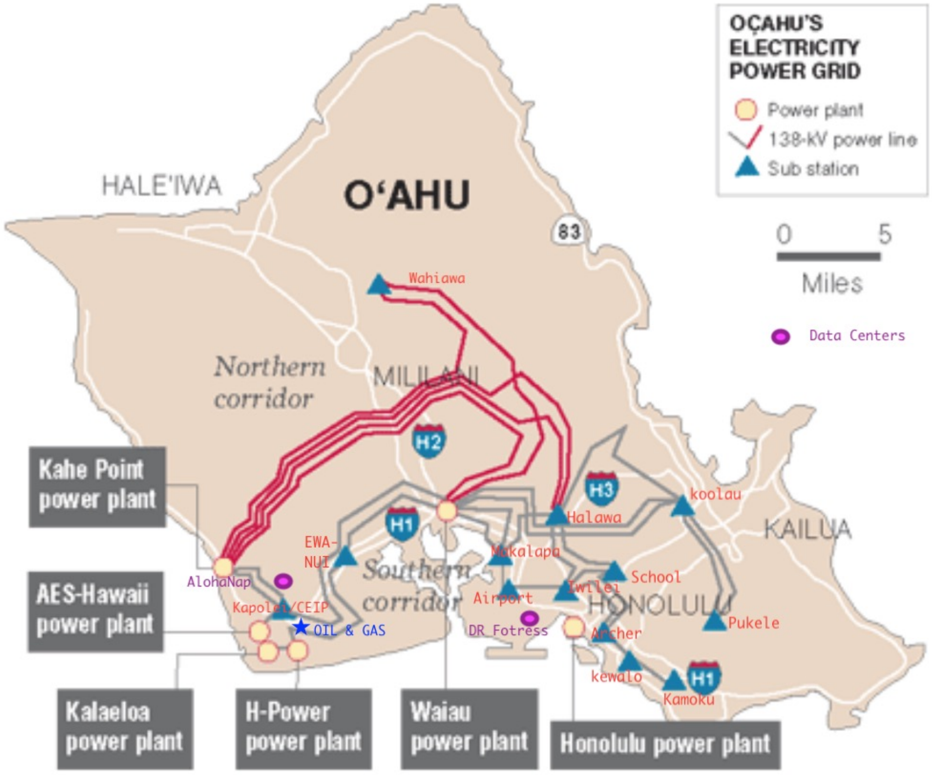

https://www.ft.com/content/0afb53f0-f382-442a-9a32-02824ce8bb70
COLONIAL PIPELINE CO.

Project Objectives

- Develop a realistic compound threat scenario relevant to USINDOPACIFIC Command (case study)
- Develop a framework to model resilience to compound threats in the context of the (generalizable) scenario
- Develop architectures and recommendations for the design of critical infrastructure control systems that can improve resilience under the compound threat model
- Validate the framework in a testbed environment

Case Study

- We have developed a scenario representing a **hurricane** strike on **Oahu, Hawaii** that impacts the **electrical power grid** and **pipeline** systems on the island
- Our preliminary results consider:
  - a Category 2 hurricane and associated flooding impact on the power grid
  - 3 different architectures for power grid Supervisory Control and Data Acquisition (SCADA)
  - Cyberattacks including *network attacks* and *intrusions*
    - network attack: disconnects a site
    - intrusion: attacker gains access to a control server



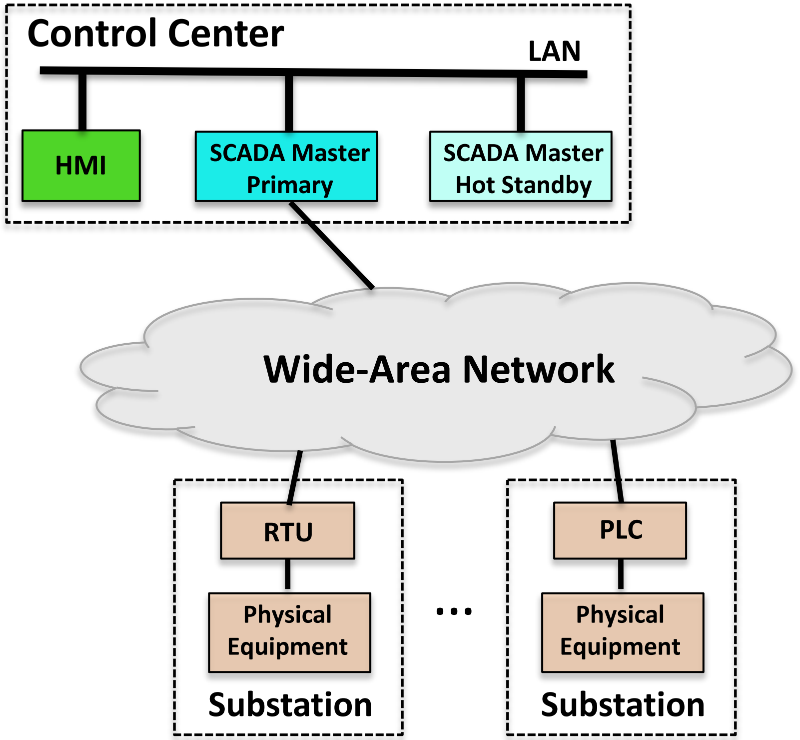
Electricity power grid topology

(https://www.kalanienglish.com/news_advertiser_061017.php, augmented with data center locations)

Case Study: Traditional Single-Control-Center Architecture

- **One control center**, located at Waiau power plant

- This architecture is vulnerable to:
  - **Flooding** at the Waiau power plant
  - **Network attack** that disconnects the Waiau control center
  - **Intrusion attack** that compromises a SCADA Master

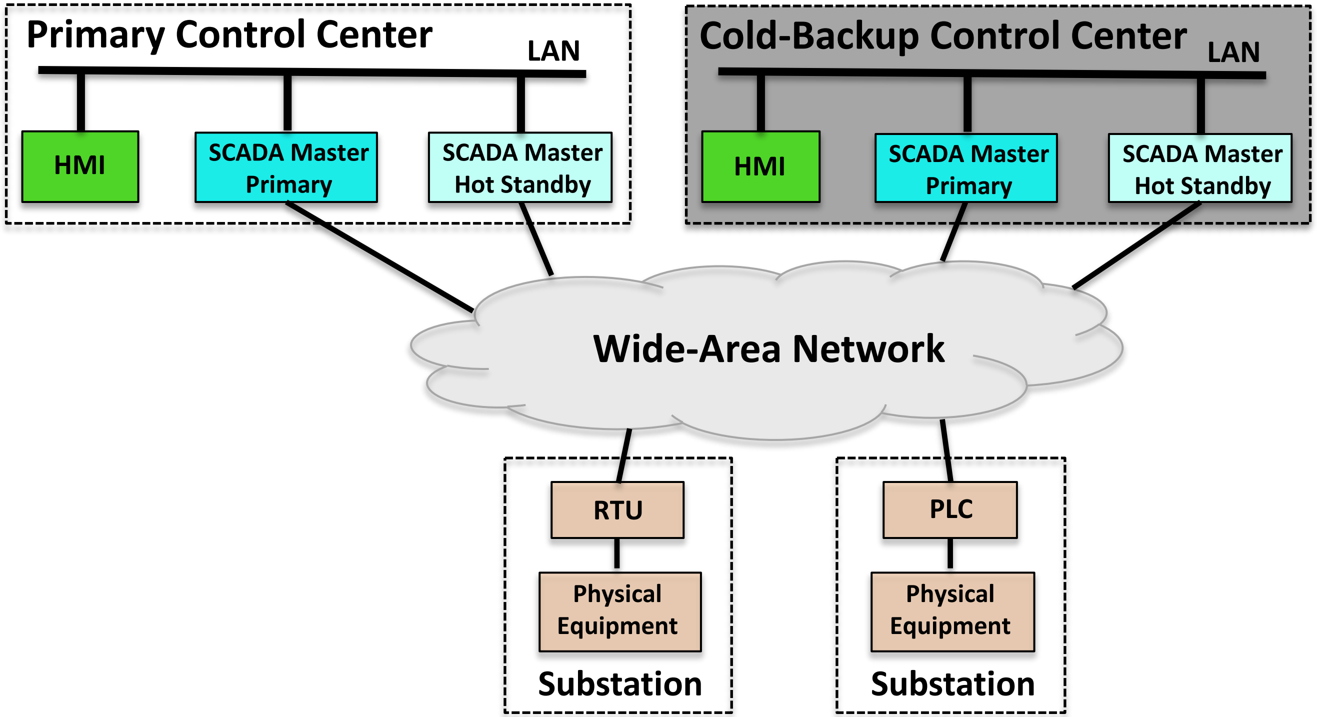


Traditional single-control-center architecture

Case Study: Modern Primary-Backup Architecture

- Backup control center can take over if primary fails
- Primary located at Waiau power plant, backup at Honolulu power plant

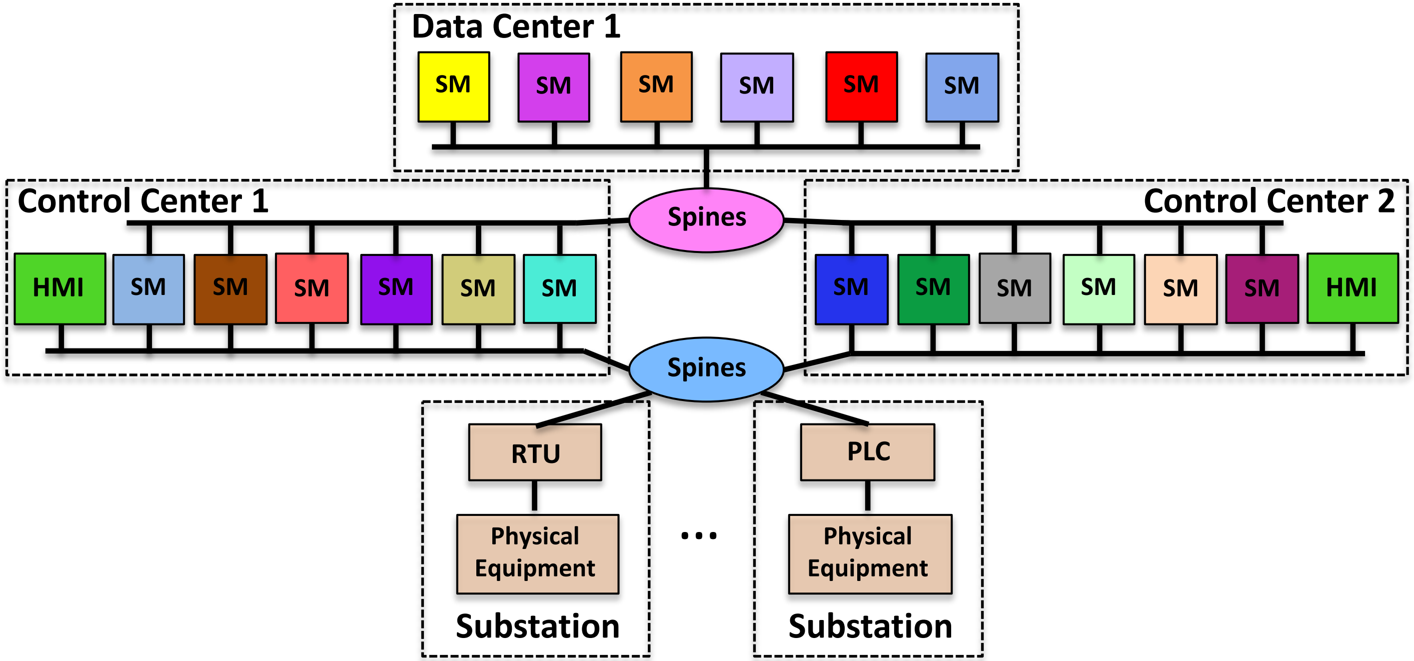
- This architecture can recover from:
  - Flooding or network attack at Waiau power plant
- This architecture is still vulnerable to:
  - Combinations of flooding and network attacks that affect **both** sites
  - Intrusion attack that compromises a SCADA Master



Modern primary backup architecture

Case Study: Intrusion-Tolerant Architecture

- Designed to **withstand** a compromised SCADA control server, **and** a network attack that succeeds in disconnecting a control center
- Waiau and Honolulu control centers are simultaneously active, with additional data center support from AlohaNap or DCFortress
- This architecture can seamlessly withstand:
  - Flooding or network attack at any **one** site + intrusion that compromises a SCADA master
- This architecture is still vulnerable to:
  - Combinations of flooding and network attacks that affect **two or more** sites



Intrusion-tolerant architecture [BTAPA18]

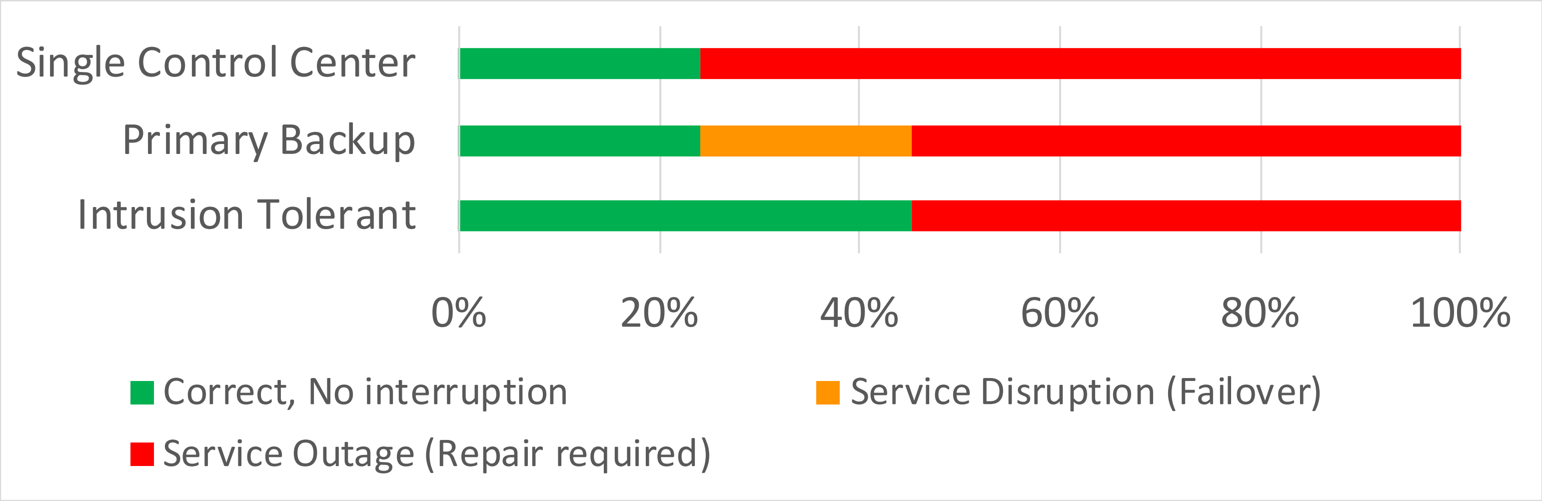
Initial Modeling Approach

- We model:
  - The probability of each site (control center, power plant, substation, data center) becoming non-operational due to **flooding** from hurricane storm surge
    - Initial modeling is somewhat limited, providing independent probabilities for site flooding across the system topology
  - **Operational status** of the overall SCADA system post-hurricane
  - Effects of **cyber-intrusion or network attack** on post-hurricane status:
    - **Fully correct, no service disruption**
    - **Temporary service disruption to fail over to backup control center**
    - **Service outage requiring (at a minimum) repairs to correct**
    - **Compromised and able to be controlled by a malicious cyber-attacker**

Preliminary Findings: Hurricane Impact

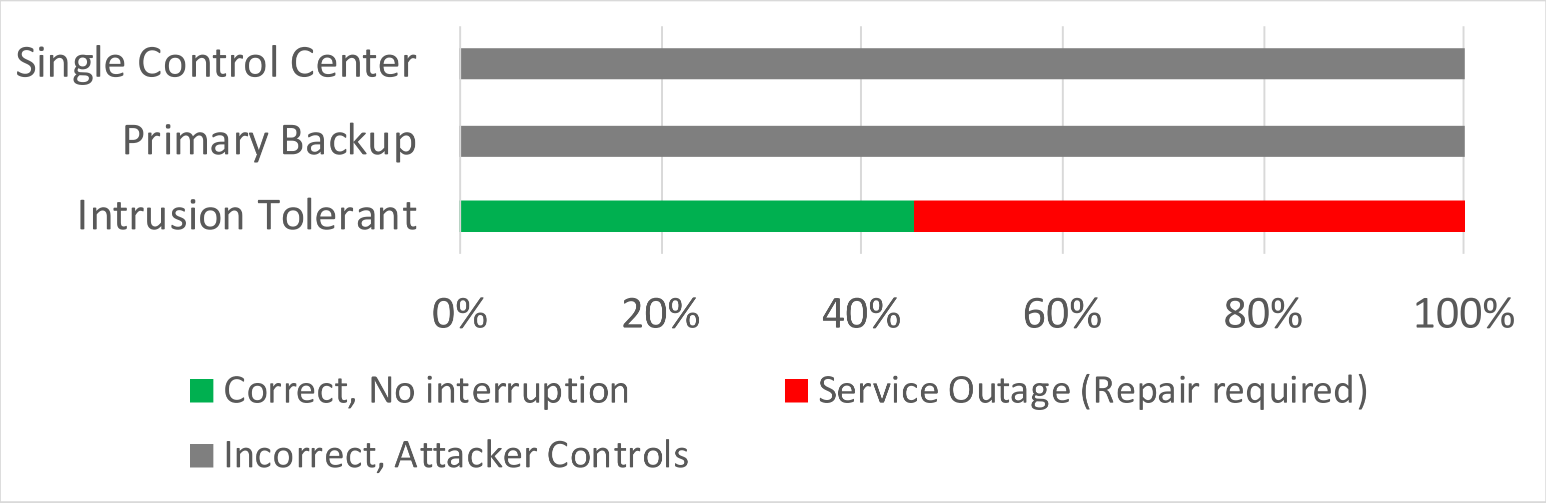
- Initial results suggest hurricane has high probability of flooding each control center (> 70%)
- This leads to a high probability of overall system outage post-hurricane, (> 50%) for all architectures

- Primary-Backup architecture improves resilience by failing over to backup if primary control center is flooded
- Intrusion-Tolerant architecture avoids service disruption due to failover, as additional sites are already active



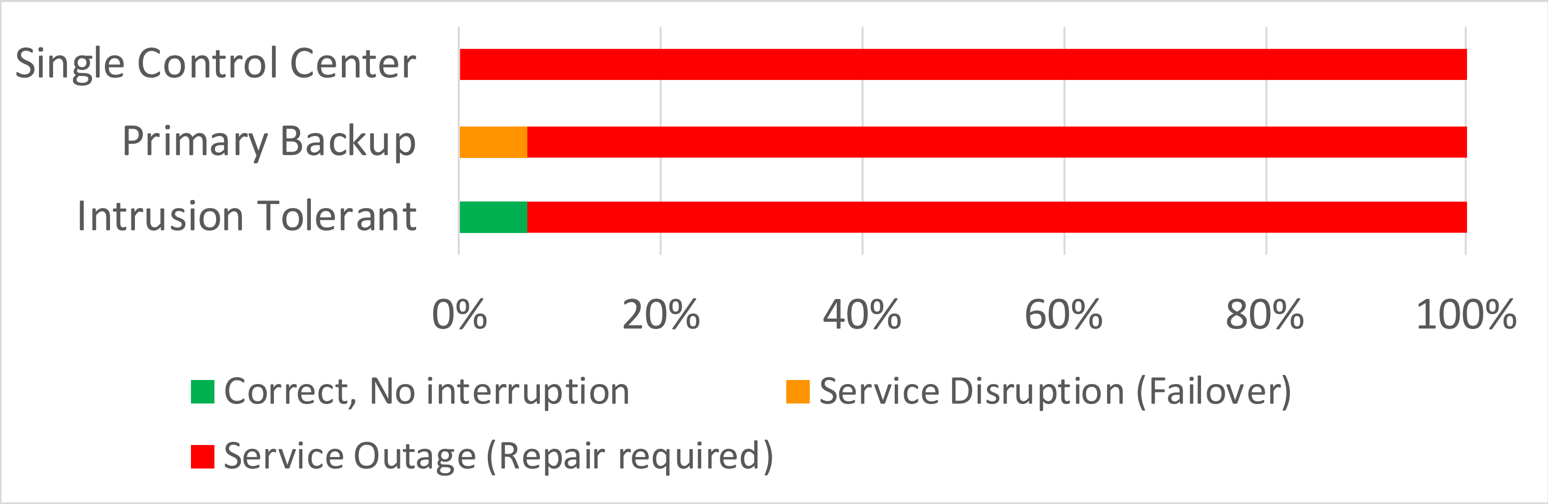
Preliminary Findings: Compound Impact Hurricane + Intrusion

- Only the intrusion-tolerant system can remain correct during a successful cyber-intrusion occurring post-hurricane
- In all other architectures, an attacker can gain control of the SCADA system and cause damage



Preliminary Findings: Compound Impact Hurricane + Network Attack

- Outage probability if a network denial-of-service attack succeeds in disconnecting a control center post-hurricane is extremely high for all architectures (> 90%)
- Intuition: with each control center having > 70% probability to be flooded by the hurricane, it is highly likely that at least one of them **will be flooded**. A sophisticated attacker can then target the other control center to cause an outage.
- Worst-case analysis with powerful, know-all attacker



Preliminary Findings: Takeaways

- Preliminary findings show extremely high outage likelihoods for all existing architectures.
- This project aims to improve this situation. We plan to:
  - Refine our modeling approach
  - Develop new design recommendations and system architectures to improve resilience
  - Expand analysis to consider effects on gas pipeline SCADA system, recovery timelines, and effects on surrounding communities

Next Steps: Modeling

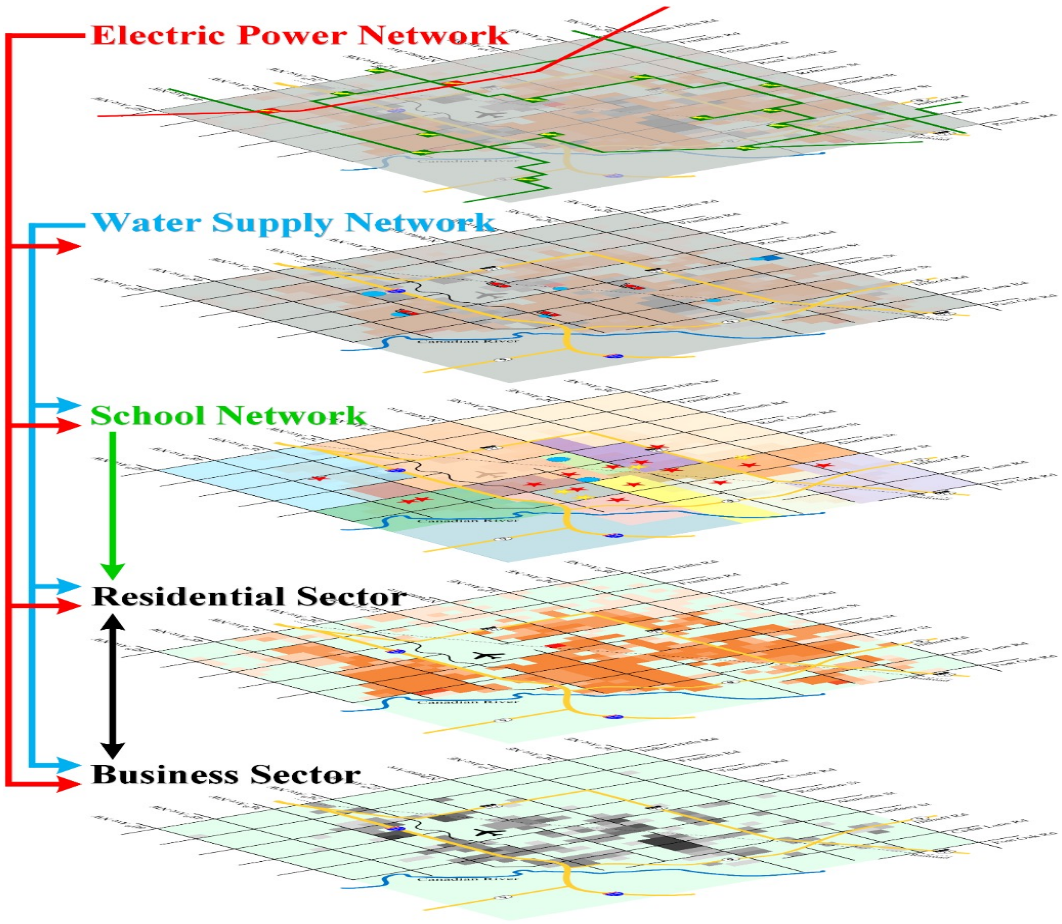
- We plan to refine our modeling approach with respect to:
  - Hurricane effects: we plan to model a suite of specific hurricane scenarios that capture correlations in failure likelihood across sites
  - Attacker power: in addition to the worst-case analysis with powerful know-all attacker considered so far, we plan to develop more realistic probabilistic models of the attacker's ability to target specific sites and servers

Next Steps: System Design

- We plan to:
  - Develop **design recommendations** for improved resilience to hurricane-related flooding and cyberattacks within current system architectures
    - Can alternative control center locations support higher resilience? (currently, only network-resilience considerations are taken into account)
  - Develop **alternative architectures** that can improve overall system resilience to the compound threats we consider, especially in the presence of sophisticated network attacks
    - Currently investigating **reconfigurable** system architectures (this includes in-band and out-of-band reconfigurations)

Next Steps: Expanding the Analysis

- Physical infrastructure systems support social and economic institutions within communities and regions
  - Schools, healthcare
- Resilience metrics include a number of different areas such as
  - Population dislocation by race/ethnicity, income, tenancy status
  - Economic changes – local gross product, household income, tax revenue
  - Building functionality
  - Functionality of critical services, for example electricity and water supply
- Interdependencies must be accounted for between critical systems and sectors



Next Steps: Expanding the Analysis

- Analyze the full "skeleton" version of the community to
  - Assess community resilience metrics for baseline case
  - Assess community resilience for alternative architectures highlighted earlier
- Discuss need for additional physical systems