Intrusion-Tolerant Power Grid Infrastructure

Amy Babay

University of Pittsburgh School of Computing and Information

Department of Informatics and Networked Systems

Department of Computer Science

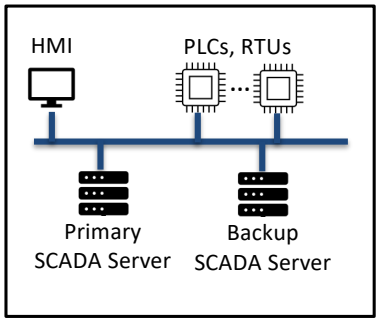
University of Pittsburgh

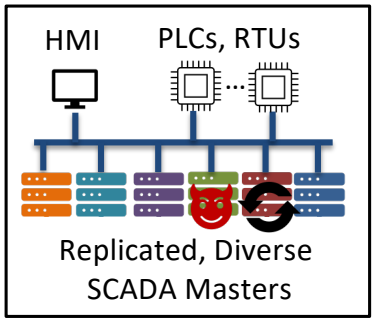
Intrusion-Tolerant Power Grid Infrastructure

- How can we ensure the systems that control our **power grids** continue to **work correctly** (and meet performance requirements), **despite *successful attacks***?
  - Compromises of system components, network attacks that disrupt communication between components

First Steps: Making it Possible

- **Spire** intrusion-tolerant SCADA system (www.spire-sys.org) [DSN 2018]
  - Byzantine fault tolerant replication with latency guarantees under attack (Prime) + diversity + proactive recovery

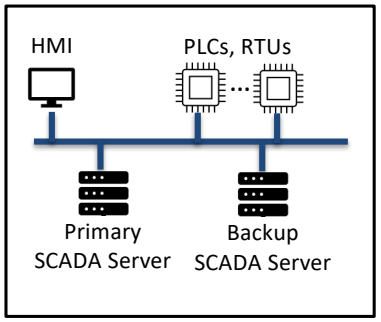


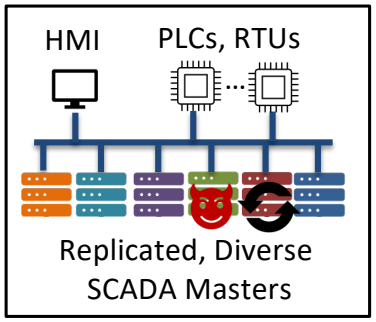


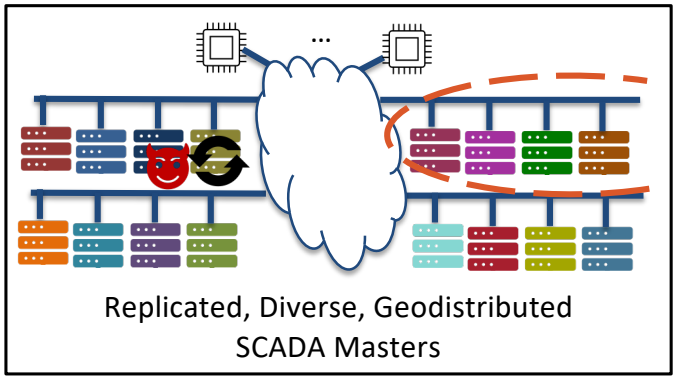
- Validated in red team experiment by Sandia National Labs at PNNL and test deployment at Hawaiian Electric [DSN 2019]

First Steps: Making it Possible

- **Spire** intrusion-tolerant SCADA system (www.spire-sys.org) [DSN 2018]
  - Byzantine fault tolerant replication with latency guarantees under attack (Prime) + diversity + proactive recovery
  - Framework for distributing replicas across multiple sites to tolerate network DoS attacks that can isolate a site







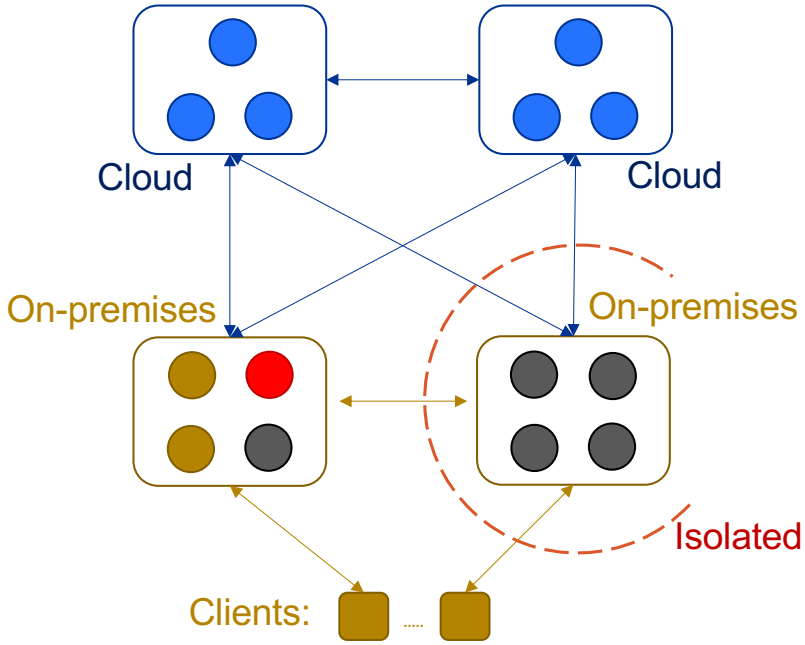
- Validated in red team experiment by Sandia National Labs at PNNL and test deployment at Hawaiian Electric [DSN 2019]

Making it Practical

- How can we make it feasible for (every) utility to deploy such a multi-site, diverse, intrusion-tolerant architecture?

Making it Practical

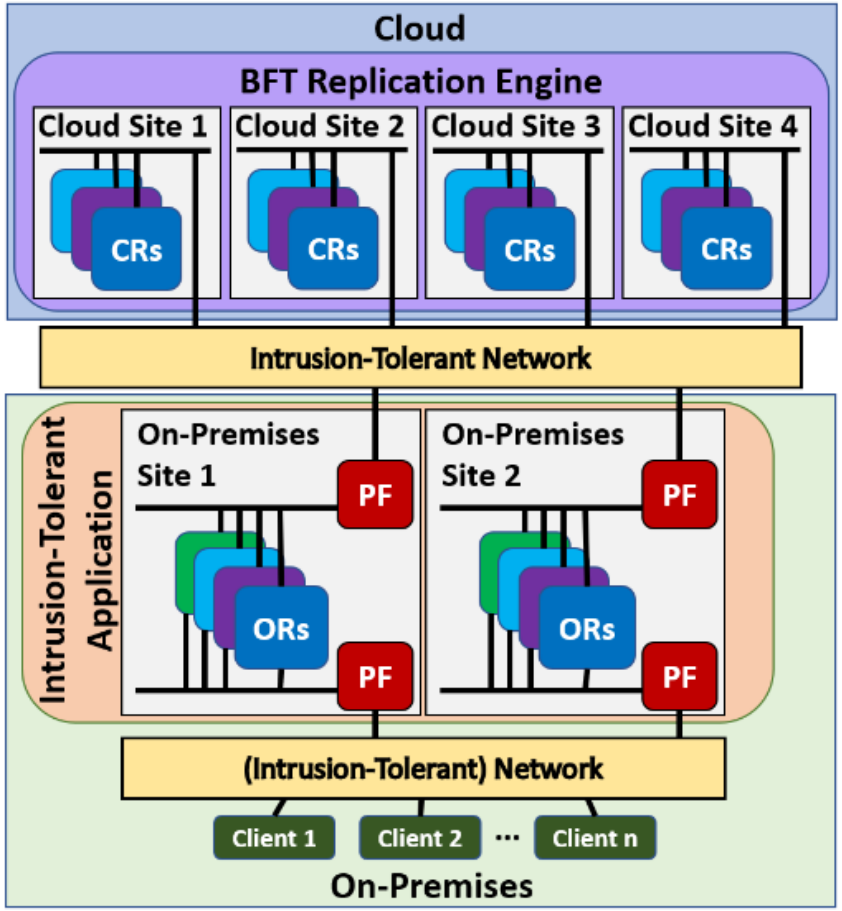
- **Cloud-based i**ntrusion-tolerant SCADA systems reduce the cost of resilience, **without exposing sensitive data to cloud providers**



- ***f+1* on-premises replicas** can encrypt client requests, cooperate with **cloud replicas** to establish ordering, then decrypt, execute, and generate (threshold-signed) client response
- Requires *2f+2* on-premises replicas per control center to tolerate *f* intrusions, 1 proactive recovery, 1 site isolation

[DSN 2021, Best paper runner-up]

Making it Practical



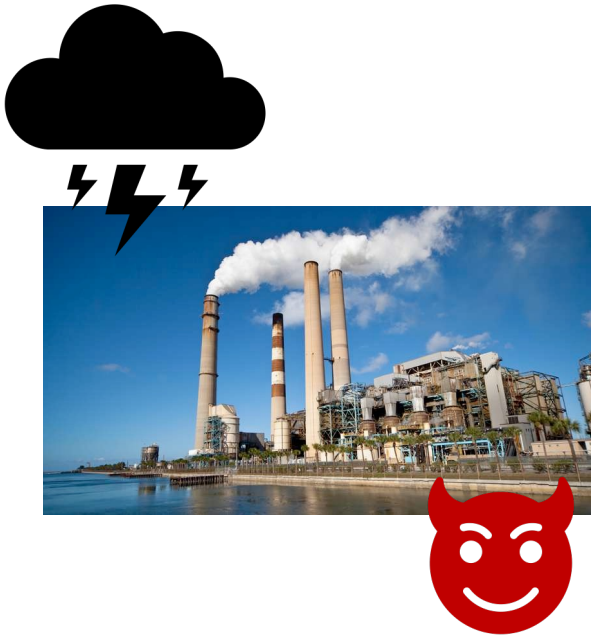
- **Separating responsibilities** of cloud replicas and on-premises replicas can allow **service providers** to invest in creating highly resilient **BFT engines**

[SRDS 2023]

Addressing Emerging Threats

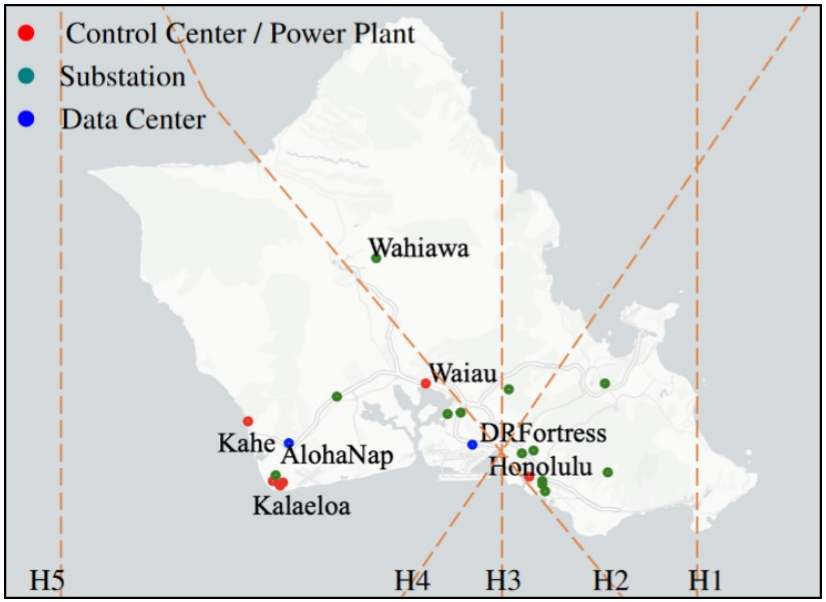
- Even this threat model is no longer enough…
- Natural hazards are becoming more frequent and more severe
- **Compound threats** are emerging, where cyberattacks are targeted in the aftermath of a natural hazard
- First question: can existing system architectures withstand such threats?
  - Unfortunately, no…

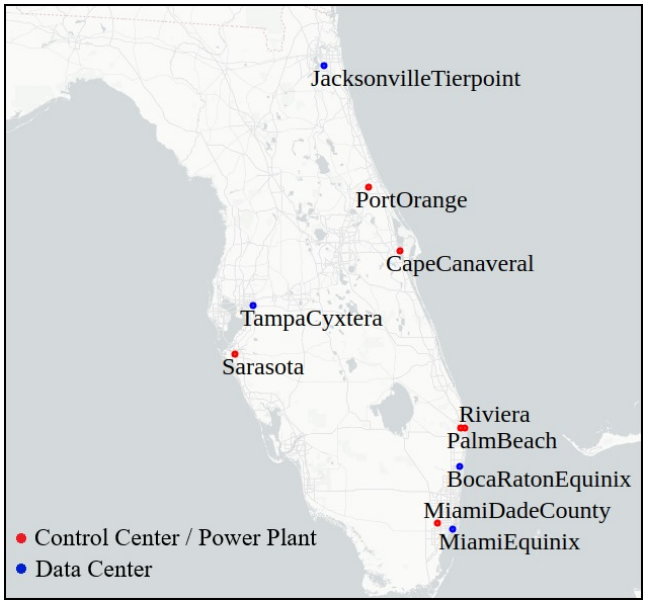
[SRDS 2024, Best Paper Award]



Addressing Emerging Threats

- Worked with civil engineers to model hurricane impacts in Hawaii and Florida



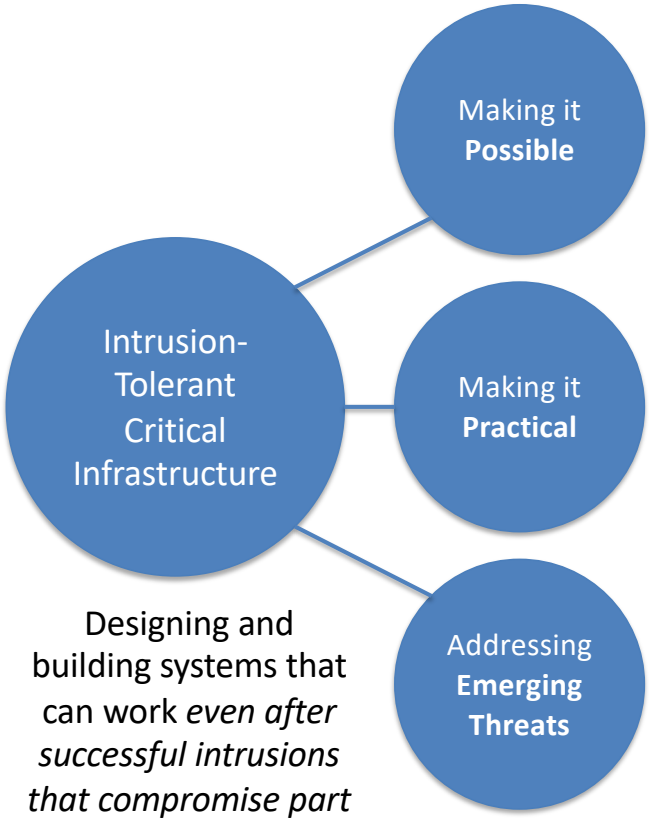


Addressing Emerging Threats

- Outcomes:
  - Compound threats have a high probability to make **multiple sites unavailable simultaneously** (via flooding that affects multiple sites, or combination of flooding and network attacks)
  - Building a static system that withstands multiple site failures becomes extremely **expensive**
  - **Reconfiguration** can help
    - If at least one control center survives, can reconfigure to run the system from that site
    - May be possible to integrate a **mobile control center** to restore operations as part of disaster recovery

Resilient Systems and Societies Lab

www.rsslab.io - Amy Babay



Designing and building systems that can work *even after successful intrusions that compromise part of the system*

- **Spire** intrusion-tolerant SCADA for the power grid
- **Spines** intrusion-tolerant network

www.spire-sys.org
www.spines-org.github.io

- **Cloud-based** intrusion-tolerant SCADA systems reduce the cost of resilience, without exposing sensitive data to cloud providers

DSN 2021 (Best paper runner-up), SRDS 2023, Maher Khan PhD thesis (2024)

- **Digital twins** can provide a transition path to intrusion-tolerant architectures

DOE-funded Cyber Energy Center project

- **Seamless intrusion-tolerant networks** support legacy applications without changes

Defense Logistics Agency funded project

- **Compound threats** involve natural hazards combined with cyberattacks

DoD/DOE funded SERDP project, SRDS 2024 (Best paper)

- **Integrated architecture** for power grid systems, provides intrusion tolerance from substation to control center