The Spire System: Toward an Intrusion-Tolerant Power Grid

Amy Babay, John Schultz,
Thomas Tantillo, and Yair Amir

Johns Hopkins University, Spread Concepts LLC

Spread Concepts

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Distributed Systems
and Networks Lab
www.dsn.jhu.edu

Importance of SCADA for the Power Grid

- Supervisory Control and Data Acquisition (SCADA) systems form the backbone of critical infrastructure services
- To preserve control and monitoring capabilities, SCADA systems must be constantly available and run at their expected level of performance (able to react within 100-200ms)
- SCADA system failures and downtime can cause catastrophic consequences, such as equipment damage, blackouts, and human casualties

Emerging Power Grid Threats

- Traditional SCADA systems ran on proprietary networks
  - Created air gap from outside world and attackers
- Cost benefits and ubiquity of IP networks are driving SCADA to use IP networks
  - Exposes SCADA to hostile environments, removing the air gap
- Raises additional concerns because SCADA systems are:
  - In service for decades
  - Running legacy code with well-known exploits

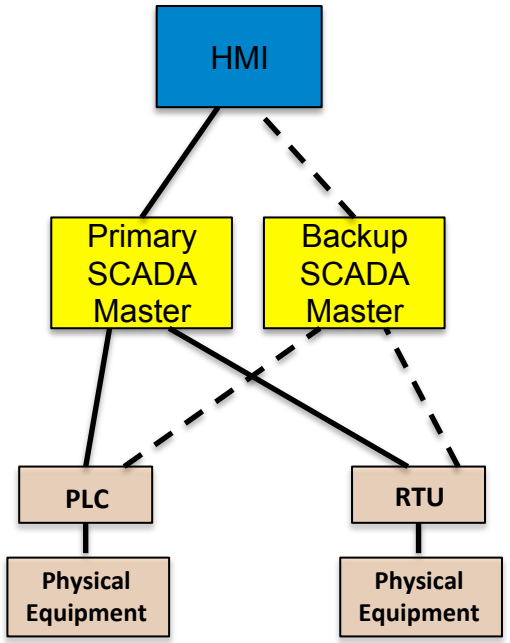
Emerging Power Grid Threats

- Perimeter defenses are not sufficient against determined attackers
  - Stuxnet, Dragonfly/Energetic Bear, Black energy (Ukraine 2015), Crashoverride (Ukraine 2016)
  - Becoming a target for nation-state attackers

SCADA Vulnerability

The move to IP makes SCADA vulnerable on several fronts:

- SCADA system compromises
  - SCADA Master – system-wide damage
  - RTUs, PLCs – limited local effects
  - HMIs
- Network level attacks
  - Routing attacks that disrupt or delay communication
  - Isolating critical components from the rest of the network



Roadmap

- The Spire System
- Red Team Experiment at Pacific Northwest National Labs (PNNL)
- Power Plant Deployment at Hawaiian Electric Company (HECO)
- Toward an Intrusion Tolerant US Power Grid

Spire: Network-Attack Resilient Intrusion-Tolerant SCADA for the Power Grid

The Spire System

- Spire is an intrusion-tolerant SCADA system for the power grid: it continues to work correctly even if some critical components have been compromised
- Intrusion tolerance as the core design principle:
  - Intrusion-tolerant network
  - Intrusion-tolerant consistent state
  - Intrusion-tolerant SCADA Master
- Open Source - http://dsn.jhu.edu/spire

The Spire System: Defense across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
  - Prime protocol – latency guarantees under attack [ACKL11]

The Spire System: Defense across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
  - Prime protocol – latency guarantees under attack [ACKL11]
- What prevents an attacker from reusing the same exploit to compromise more than f replicas?

The Spire System: Defense across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
  - Prime protocol – latency guarantees under attack [ACKL11]
- Diversity
  - Present a different attack surface so that an adversary cannot exploit a single vulnerability to compromise all replicas
  - Multicompiler from UC Irvine [HNLBF13]

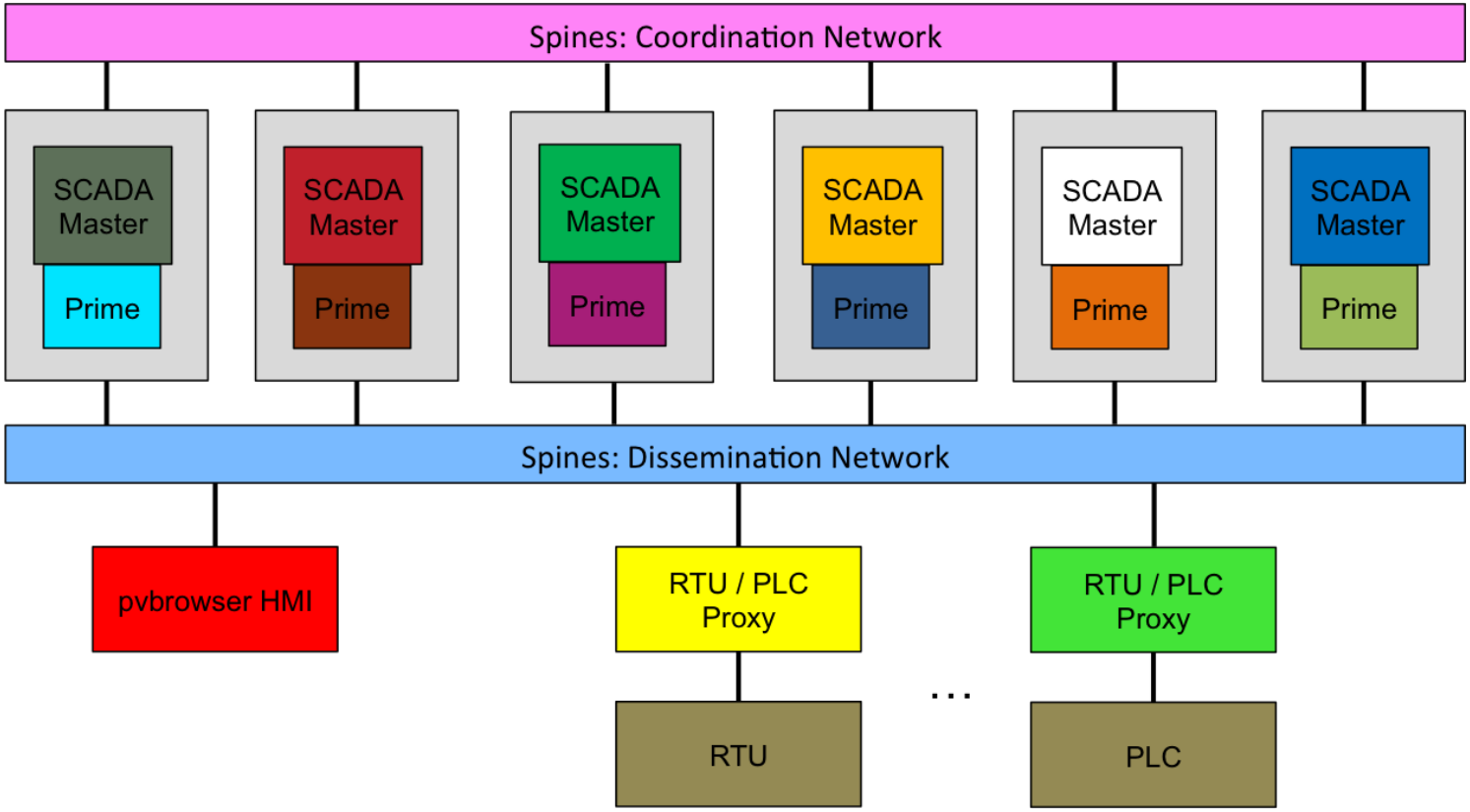
The Spire System: Defense across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
  - Prime protocol – latency guarantees under attack [ACKL11]
- Diversity
  - Present a different attack surface so that an adversary cannot exploit a single vulnerability to compromise all replicas
  - Multicompiler from UC Irvine [HNLBF13]
- What prevents an attacker from compromising more than f replicas over time?

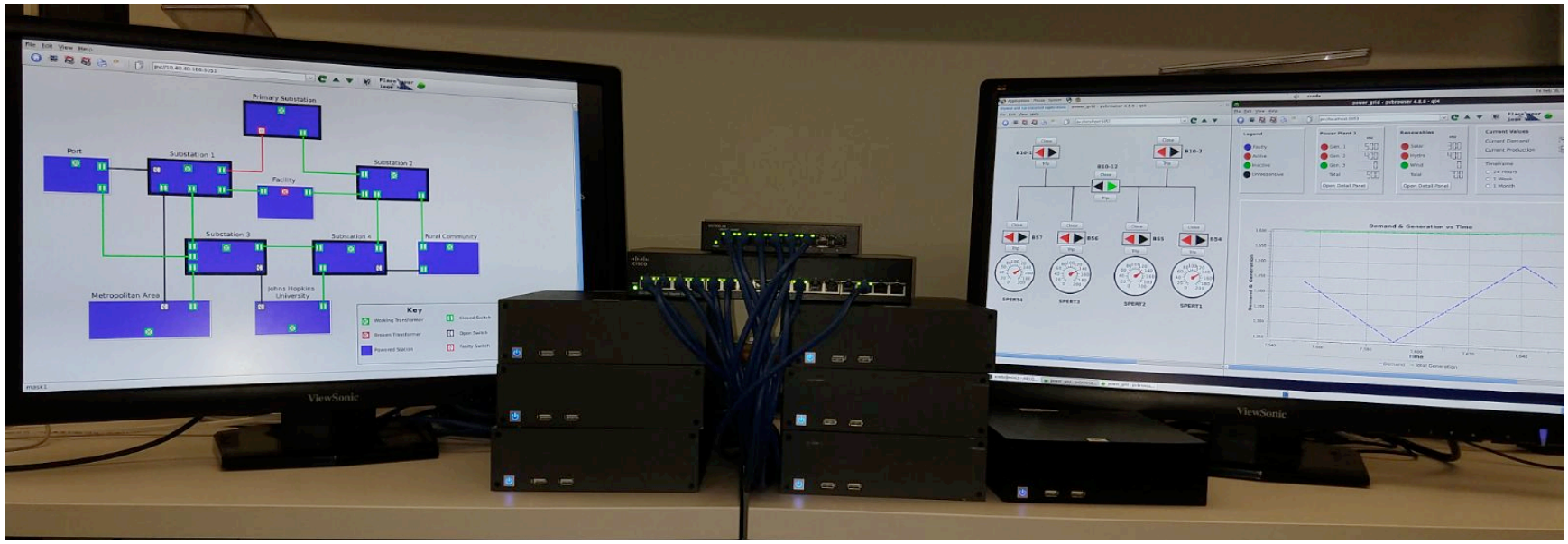
The Spire System: Defense across Space and Time

- Byzantine Fault Tolerant Replication (BFT)
  - Correctly maintains state in the presence of compromises
  - 3f+1 replicas needed to tolerate up to f intrusions
  - 2f+1 connected correct replicas required to make progress
  - Prime protocol – latency guarantees under attack [ACKL11]
- Diversity
  - Present a different attack surface so that an adversary cannot exploit a single vulnerability to compromise all replicas
  - Multicompiler from UC Irvine [HNLBF13]
- Proactive Recovery
  - Periodically rejuvenate replicas to a known good state to cleanse any potentially undetected intrusions
  - 3f+2k+1 replicas needed to simultaneously tolerate up to f intrusions and k recovering replicas [SBCNV10]
  - 2f+k+1 connected correct replicas required to make progress

The Spire System: Single Control Center



The Spire System: Single Control Center



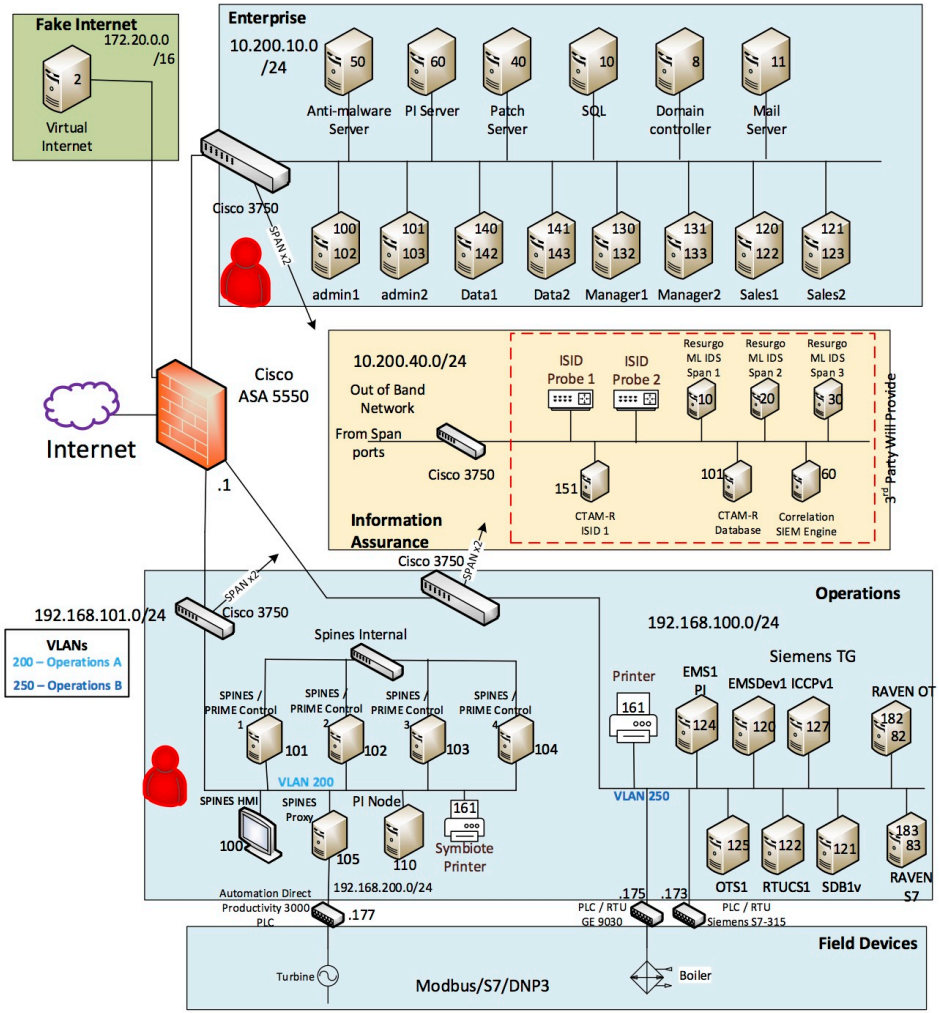
Six Spire replicas, monitoring and controlling three power grid scenarios (two distribution, one generation)

Red Team Experiment

March 27 – April 7, 2017

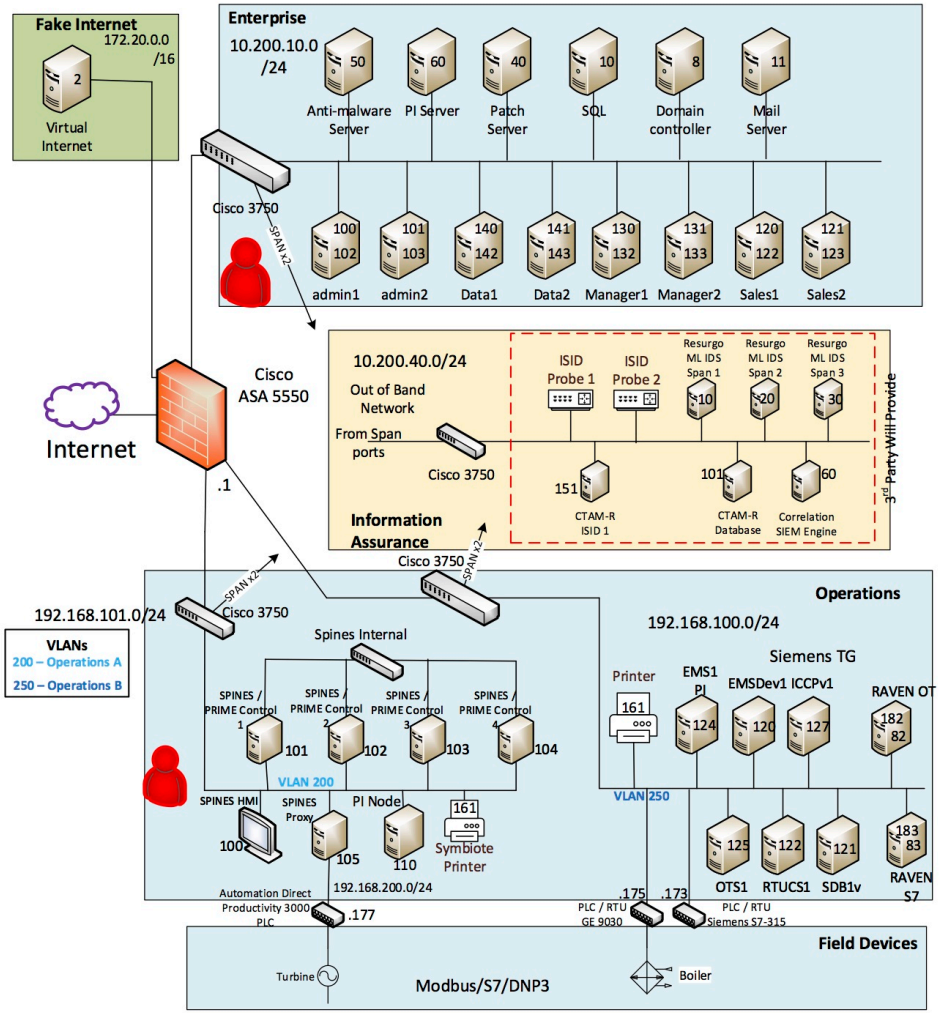
DoD ESTCP Red Team Experiment

- DoD ESTCP experiment at Pacific Northwest National Labs
  - Conducted by Resurgo with JHU DSN lab and Spread Concepts LLC participation
- Evaluated NIST-compliant commercial SCADA architecture and Spire
  - Each attacked by Sandia National Labs red team



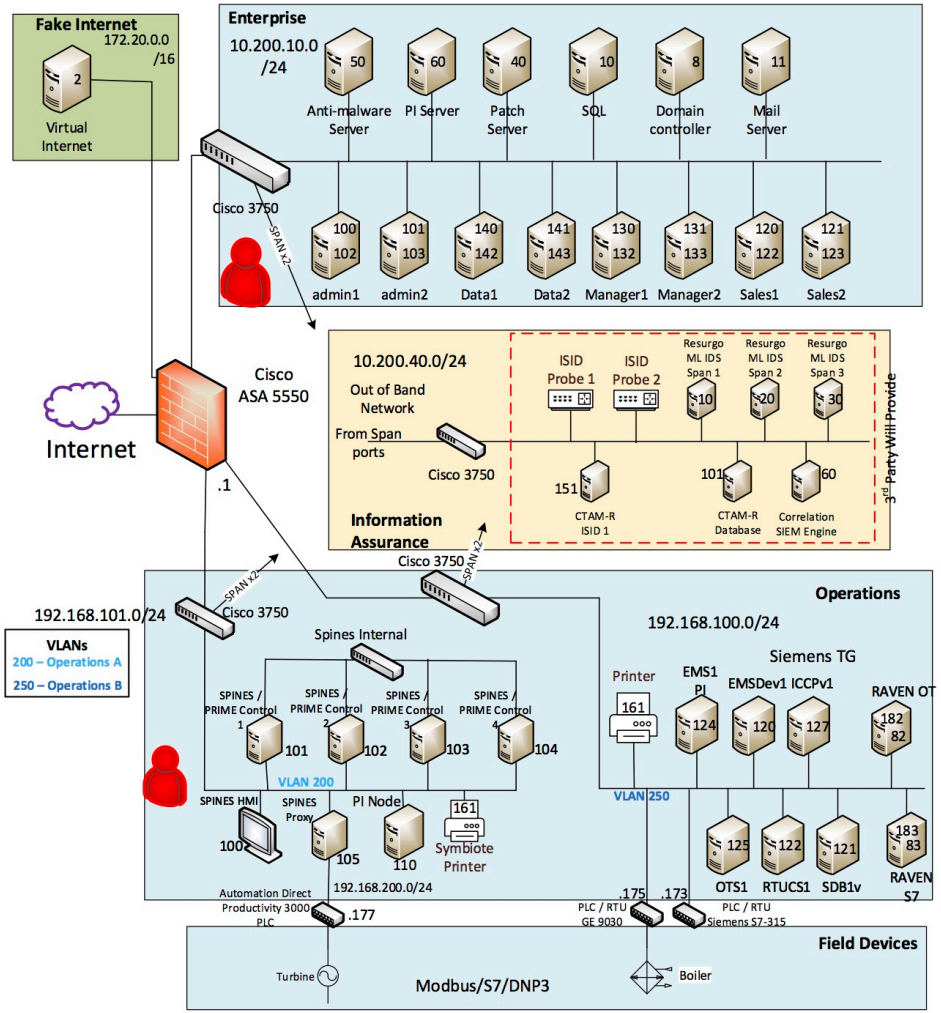
DoD ESTCP Red Team Results

- NIST-compliant system completely taken over
  - MITM attack from corporate network
  - Direct access to PLC from operational network
- Spire completely unaffected
  - Attacks in corporate and operational network
  - Given complete access to a replica and code
  - Red team gave up after several days



DoD ESTCP Red Team Takeaways

- Today's power grid is vulnerable
- There is a difference between current best practices and state-of-the-art research-based solutions
- Secure network setup using cloud expertise (protected the system for two days)
- Customized intrusion-tolerant protocols (defended the system in the presence of an intrusion on the third day)



Hawaiian Electric Company
Power Plant Deployment

January 22 – February 2, 2018

DoD ESTCP Hawaiian Electric Company Deployment Setup

- Spire test deployment at HECO
  - "Mothballed" Honolulu plant
  - Managed small power topology, controlling 3 physical breakers via a Modbus PLC
- Deployment goals
  - Operate correctly in real environment without adverse effects
  - Meet performance requirements

DoD ESTCP Hawaiian Electric Company Deployment Results

- Ran continuously for 6 days without adverse effects on other plant systems
- Timing experiment using sensor to measure HMI reaction time showed that Spire met latency requirements

Toward an Intrusion-Tolerant Power Grid

Encouraging Adoption through Open Source

- Challenge
  - Legacy, proprietary software is difficult to modernize
  - Strict reliability requirements and result in highly conservative ecosystem
- Open-source ecosystem
  - Educate power companies, SCADA vendors, and regulators about new solutions
  - Prove that new technology is effective before it is adopted/ adapted

Spire

pvb

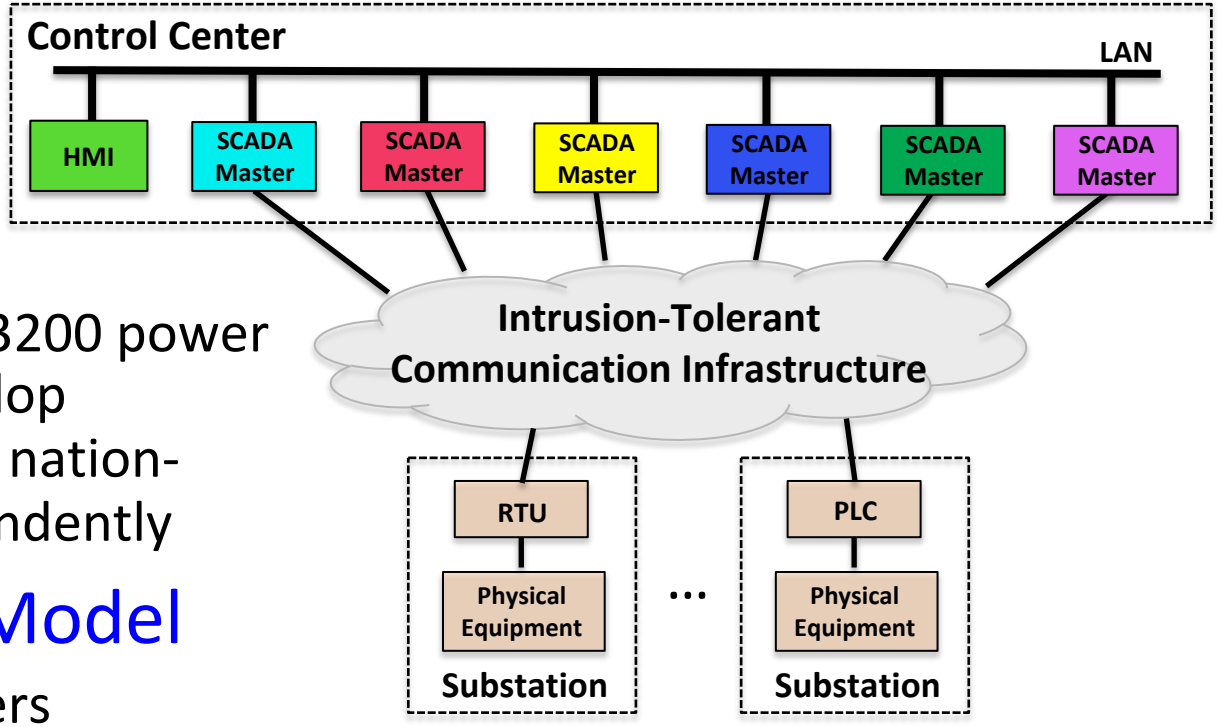
TANGO

GSF

openPLC

Systemic Resilience through a Service Provider Model

- Challenge
  - Interconnection leads to “weakest link” problem
  - Difficult for each of 3200 power installations to develop expertise to counter nation-state attacks independently
- Service Provider Model
  - Service provider offers intrusion-tolerant state maintenance service
  - Power companies customize system and endpoints



Spire: Toward Deployment

- Seeking industry partners / relevant projects
- Spire forum focused on open source intrusion-tolerant control systems for the power grid
- http://dsn.jhu.edu/spire
- http://www.spreadconcepts.com

Spread Concepts

Johns Hopkins
Whiting School
of Engineering

Distributed Systems
and Networks Lab
www.dsn.jhu.edu