Developing, Red-Teaming, and Test-Deploying Spire: Intrusion-Tolerant SCADA for the Power Grid

Yair Amir
yairamir@cs.jhu.edu
Johns Hopkins University
Department of Computer Science

Acknowledgement

- Yair Amir is a Professor of Computer Science and the Director of the Distributed Systems and Networks lab (www.dsn.jhu.edu) at Johns Hopkins University
- Yair is also a co-founder and member of and holds equity in Spread Concepts LLC (www.spreadconcepts.com), as well as a co-founder and Chief Science Officer of and holds equity in LTN Global Communications (www.ltnglobal.com). The results discussed in this presentation could affect the value of Spread Concepts LLC and LTN Global Communications. This arrangement has been reviewed and approved by the Johns Hopkins University in accordance with its conflict of interest policies

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

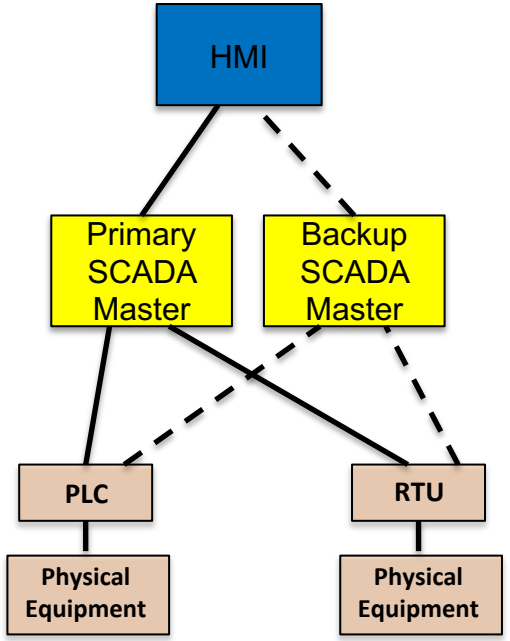
Emerging Power Grid Threats

- 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 Vulnerabilities

SCADA systems are 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



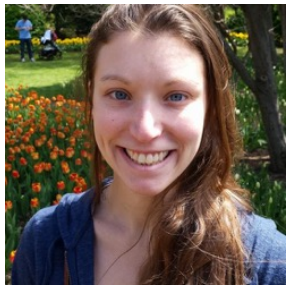
The Spire System

- 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://www.dsn.jhu.edu/spire

The Spire Story

- Distributed Systems and Networks Lab (DSN), Johns Hopkins University
  www.dsn.jhu.edu
  - DARPA Resilient Clouds, transition to power grid --> Spire
  - DoD ESTCP project
- Spread Concepts LLC www.spreadconcepts.com
  - Experience running global cloud systems at scale
  - DoD ESTCP project
  - Further development toward practical use

Credits ☺



Dr. Amy Babay

Dr. Thomas Tantillo

Trevor Aron

Sam Beckley

Dr. Marco Platania

John Schultz

Dr. Jonathan Stanton

Roadmap

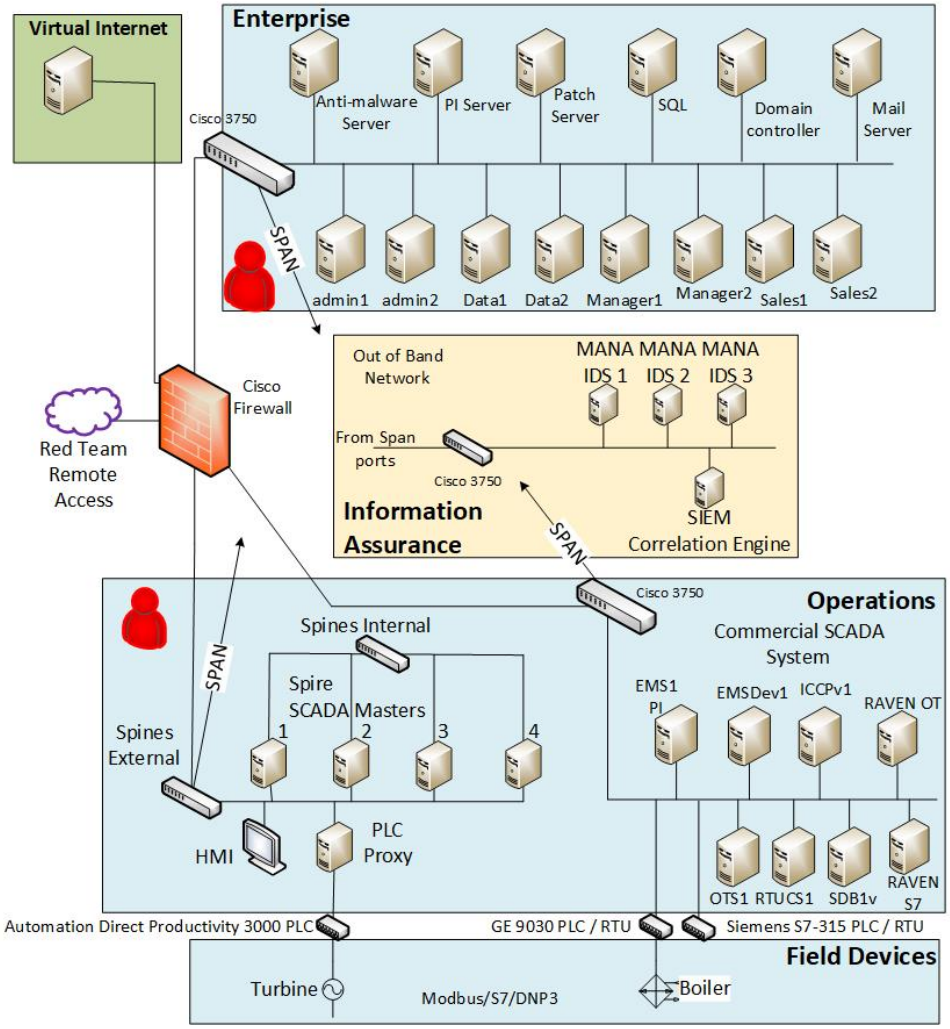
- Demonstrating the problem: Red Team Experiment at Pacific Northwest National Labs (PNNL)
- The Spire System – how it works
- Deployment Scenarios
  - Power Plant Deployment at Hawaiian Electric Company
  - Wide-area Transmission Architecture
- Path to Transition

Red Team Experiment at Pacific Northwest National Labs (PNNL)

March 27 – April 7, 2017

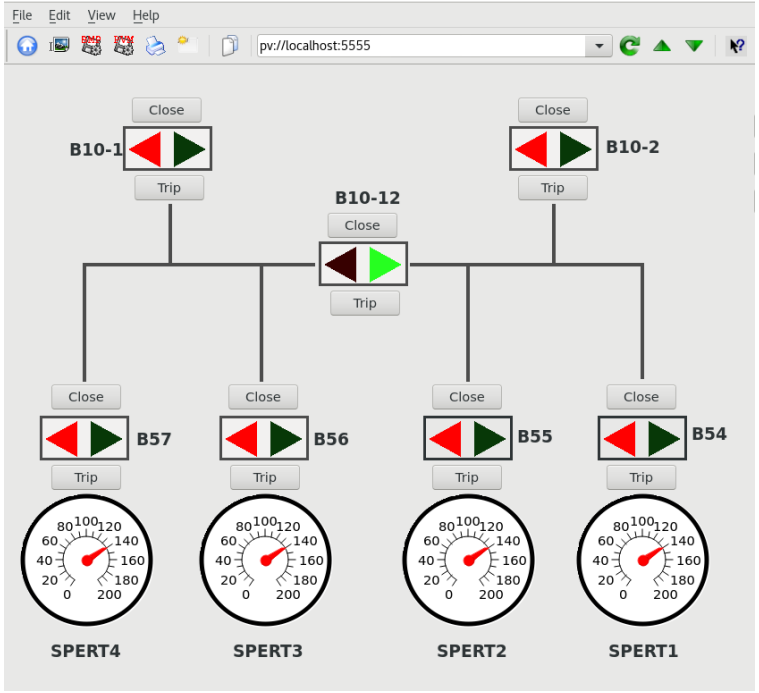
DoD ESTCP Red Team Experiment

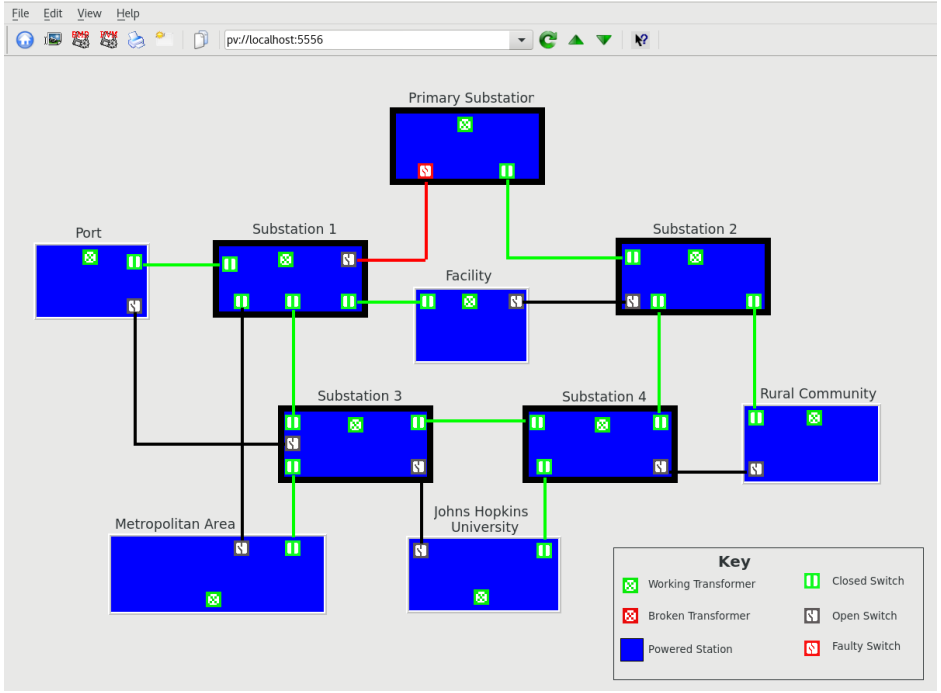
- Conducted at Pacific Northwest National Lab (PNNL)
- Power plant network architecture set up with input from Hawaiian Electric Company
- Parallel operations networks
  - NIST-compliant commercial SCADA system
  - Spire system
- Commercial system and Spire each attacked by Sandia National Labs red team



SCADA System Setup

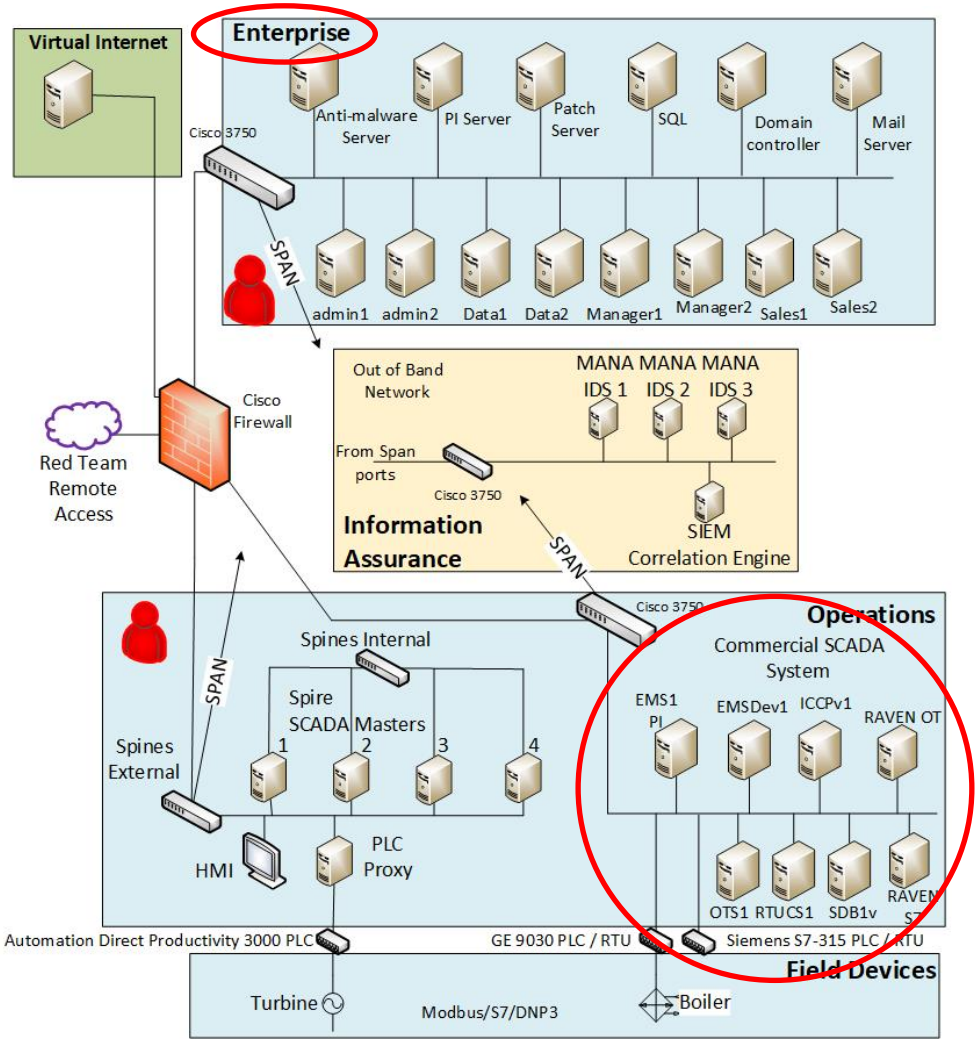
- Scenario 1: 1 real PLC provided by PNNL, representing a field substation feeding power to four buildings
- Scenario 2: 10 PLCs emulated using OpenPLC, power distribution from 5 substations to 5 sites





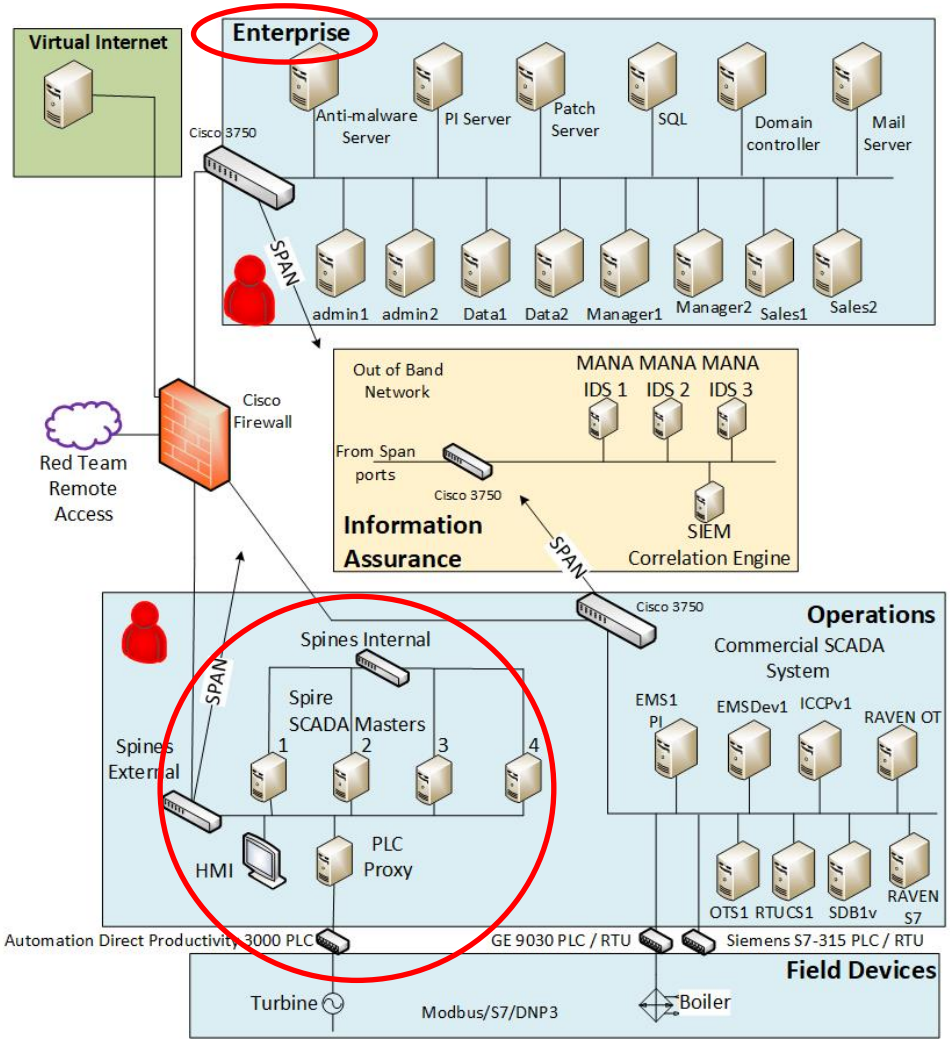
Commercial System Attacks

- Started from enterprise network
  - Goal: Establish baseline
  - Surprising result: access to operations network via MITM attack -> issued direct commands to PLC
  - Full control + damage to PLC: required firmware reinstall
- Given direct access to operations network
  - Disrupted and modified SCADA Master to HMI communication



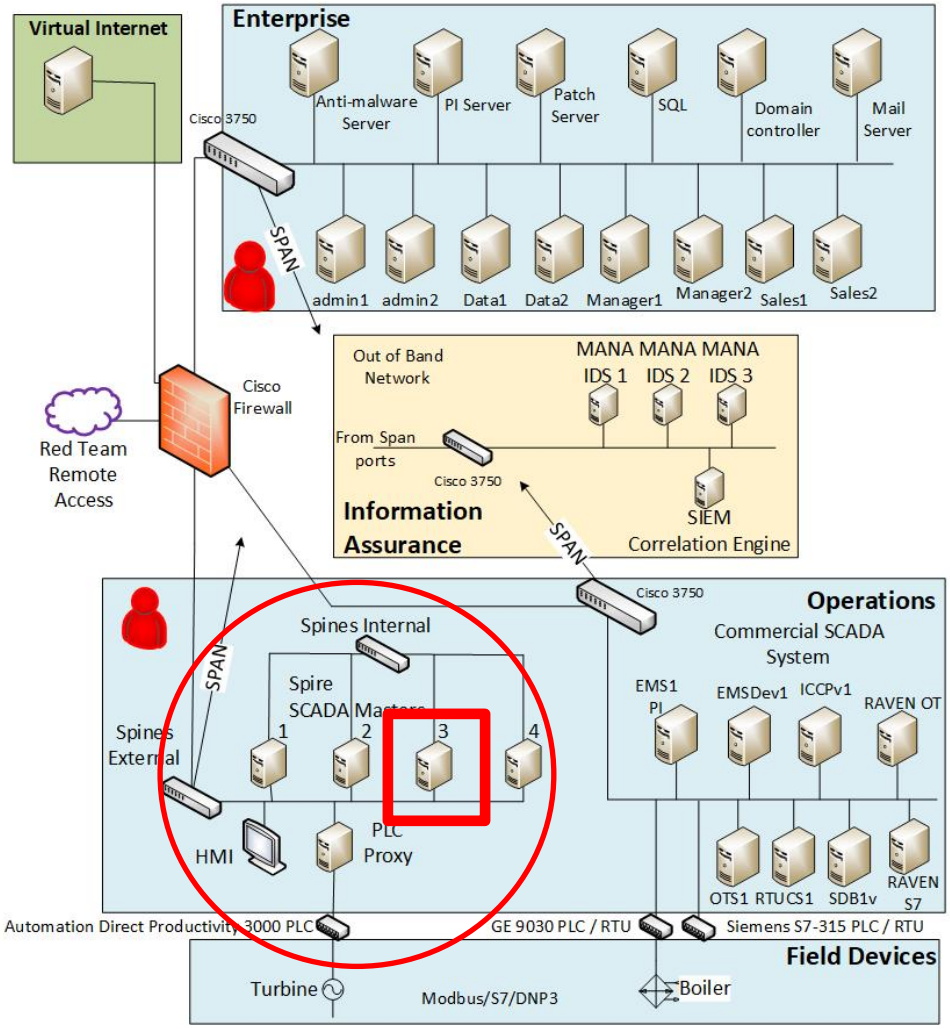
Spire System Attacks

- Started from enterprise network
  - No visibility; gave up after a couple hours
- Given direct access to operations network
  - 2 full days of network attacks (port scanning, ARP poisoning, IP address spoofing, DoS via traffic bursts, …)
- No effect on the system



Spire System Excursion (1)

- Excursion: Red team given access to a SCADA Master replica
- User-level access
- Root access + source code
- No effect on the system



Spire: How it Works

Spire: Addressing System Compromises

- 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]

Spire: Addressing System Compromises

- 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?

Spire: Addressing System Compromises

- 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]

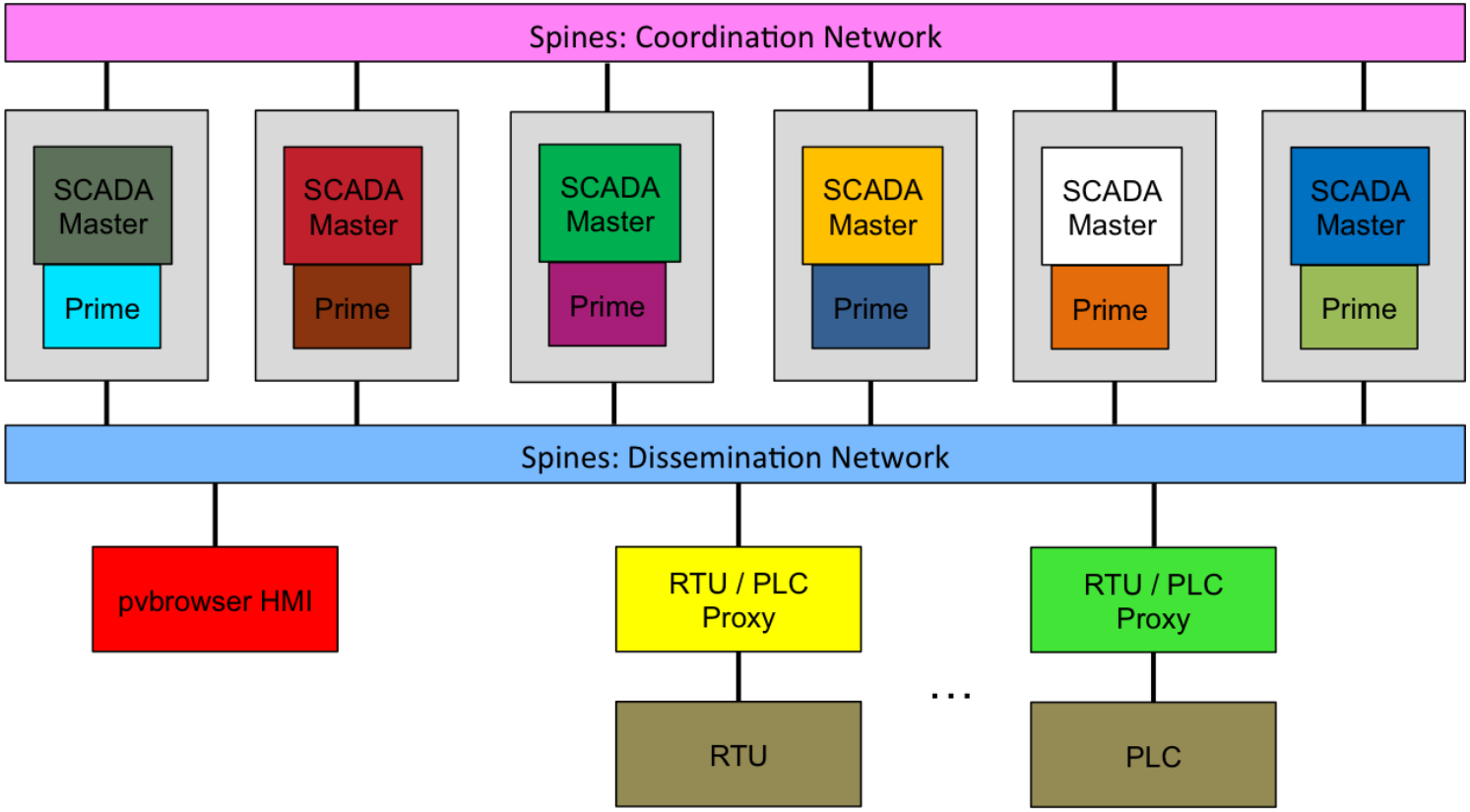
Spire: Addressing System Compromises

- 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?

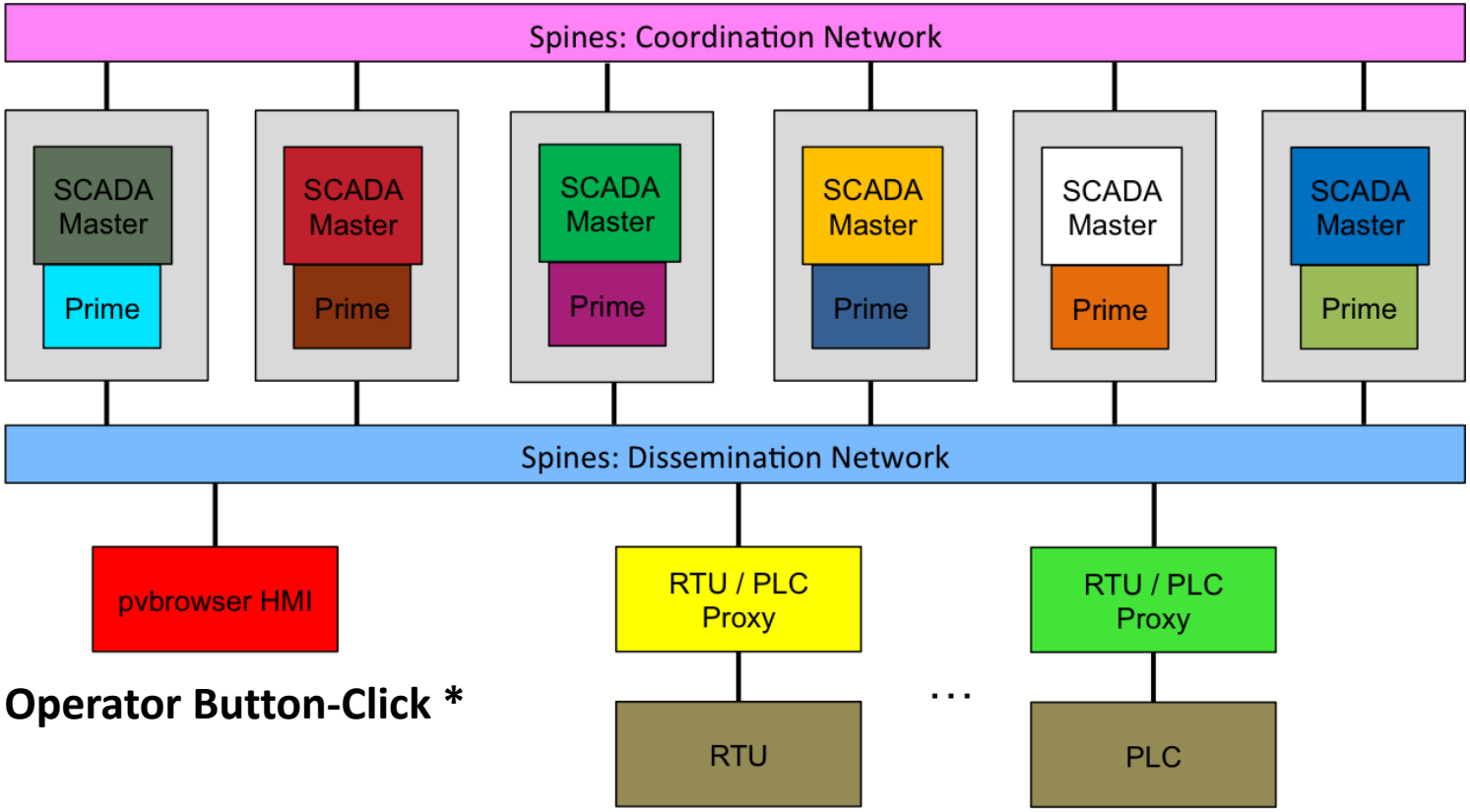
Spire: Addressing System Compromises

- 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

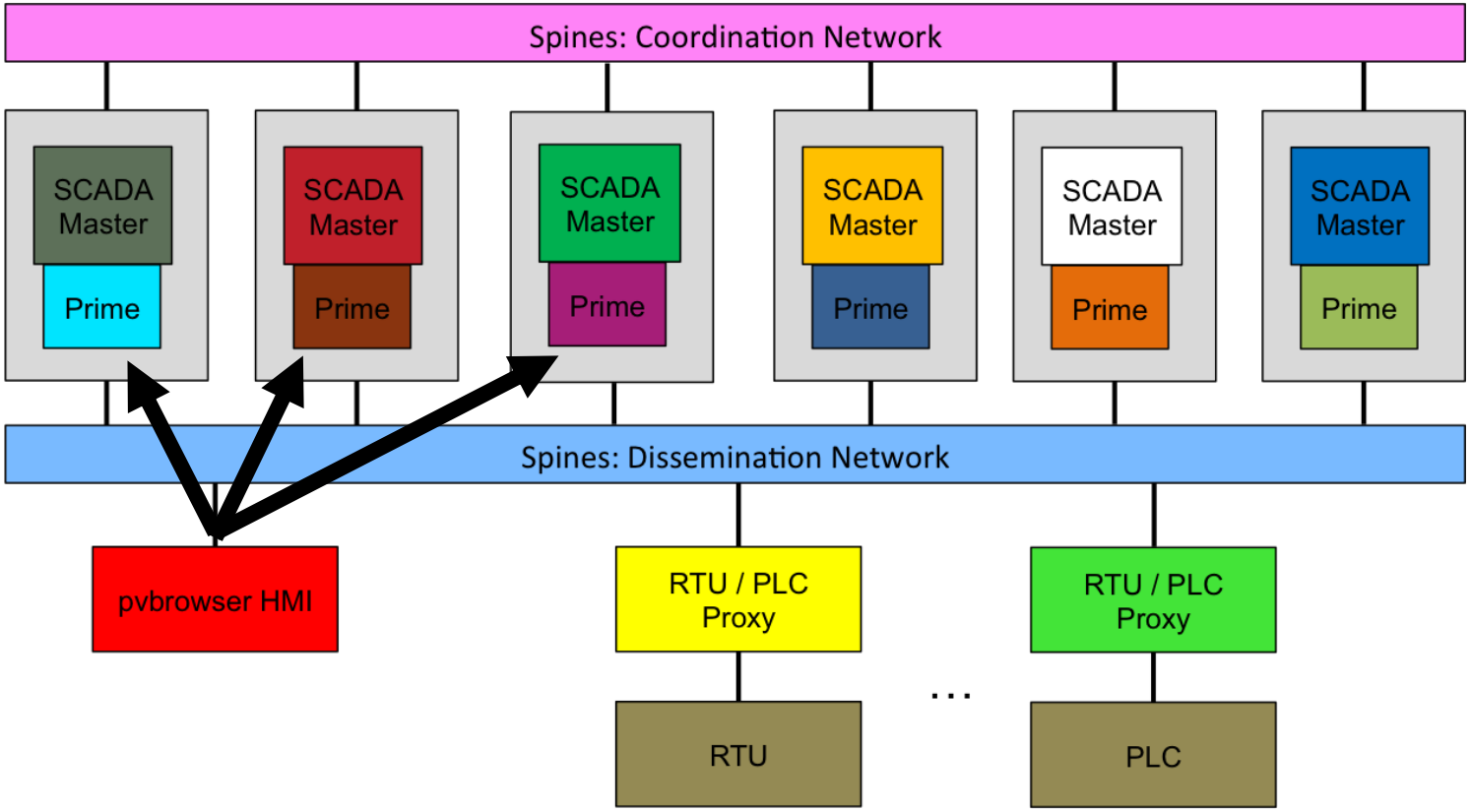


Spire Operation



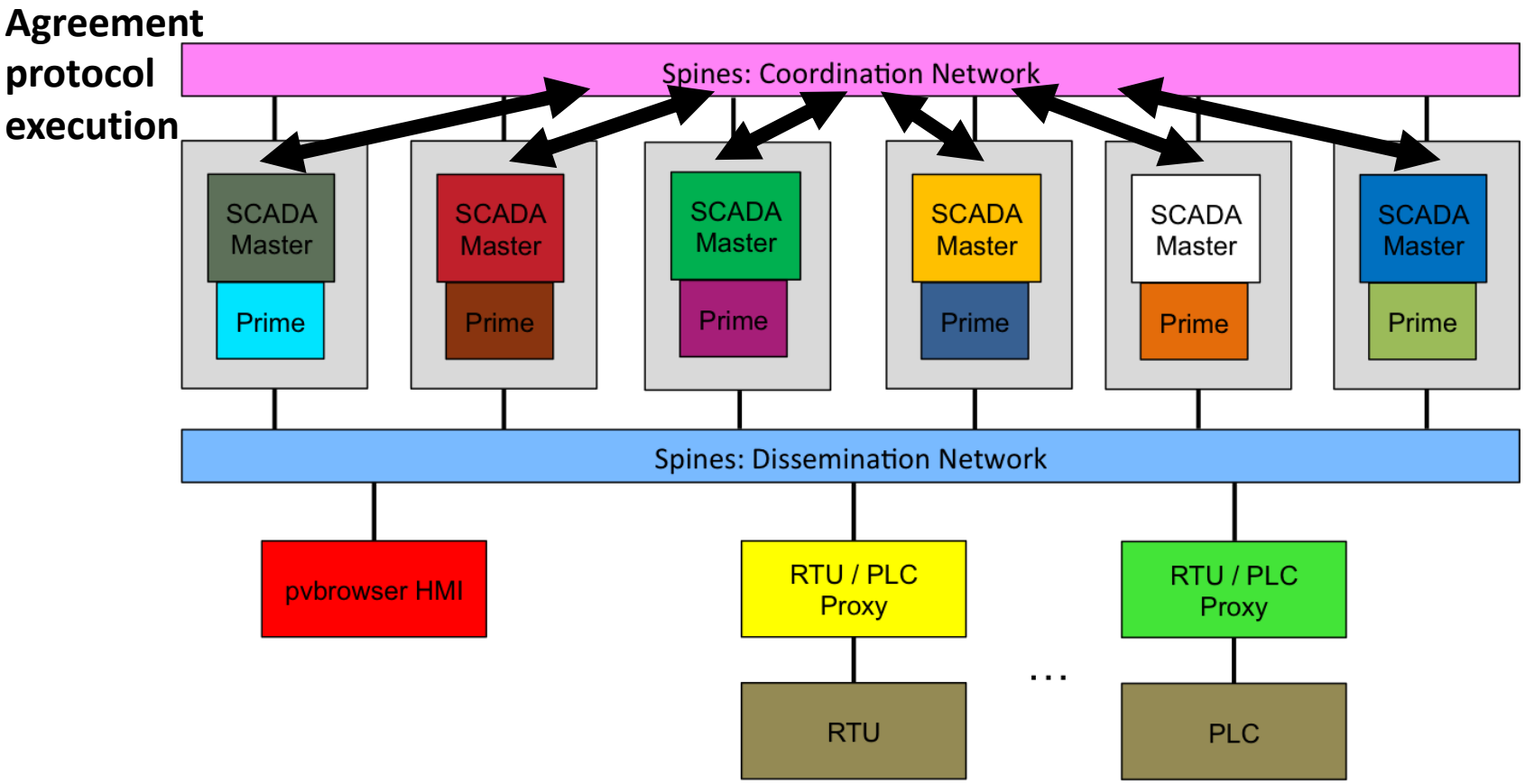
*** Operator Button-Click ***

Spire Operation



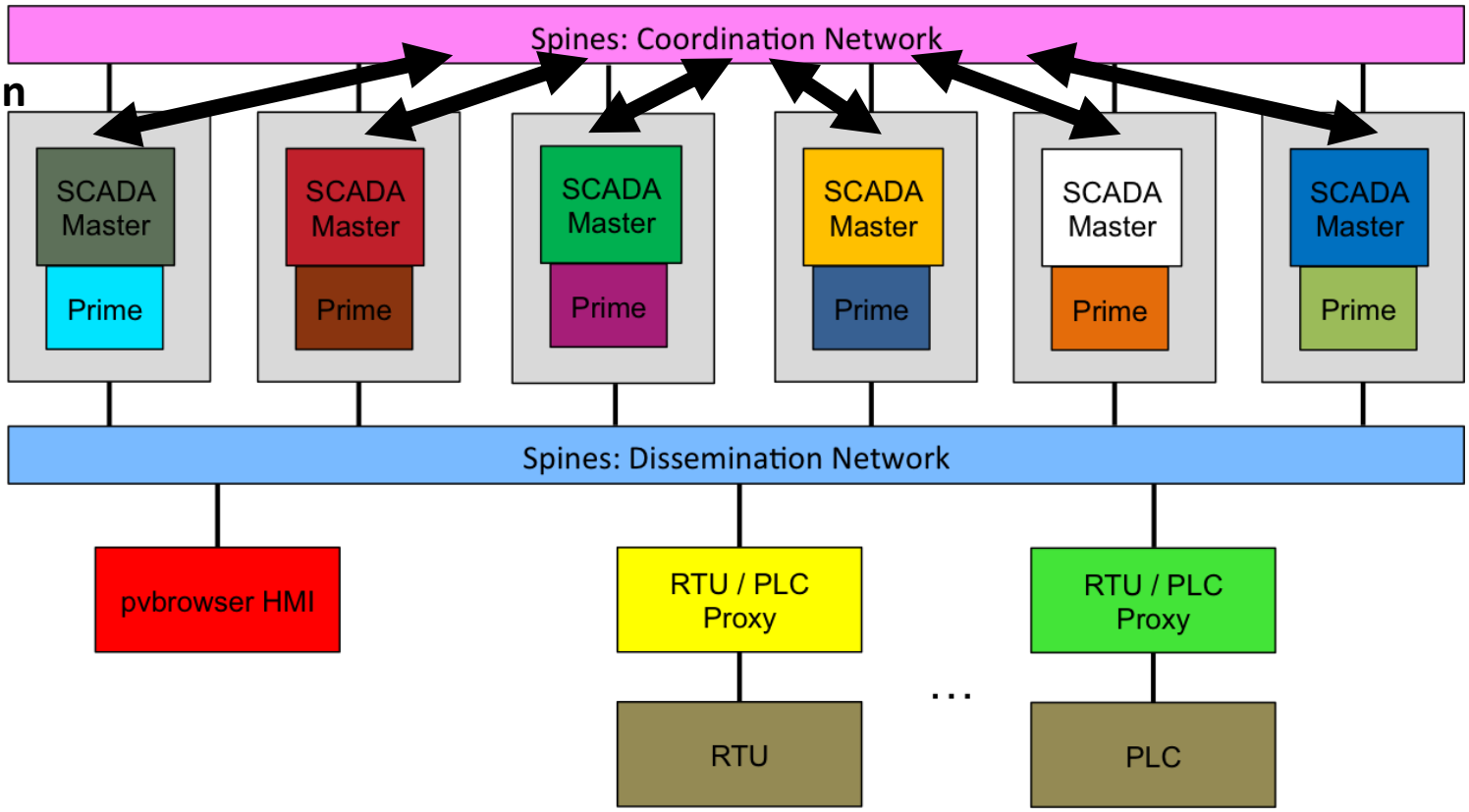
Send to f+k+1 replicas

Spire Operation

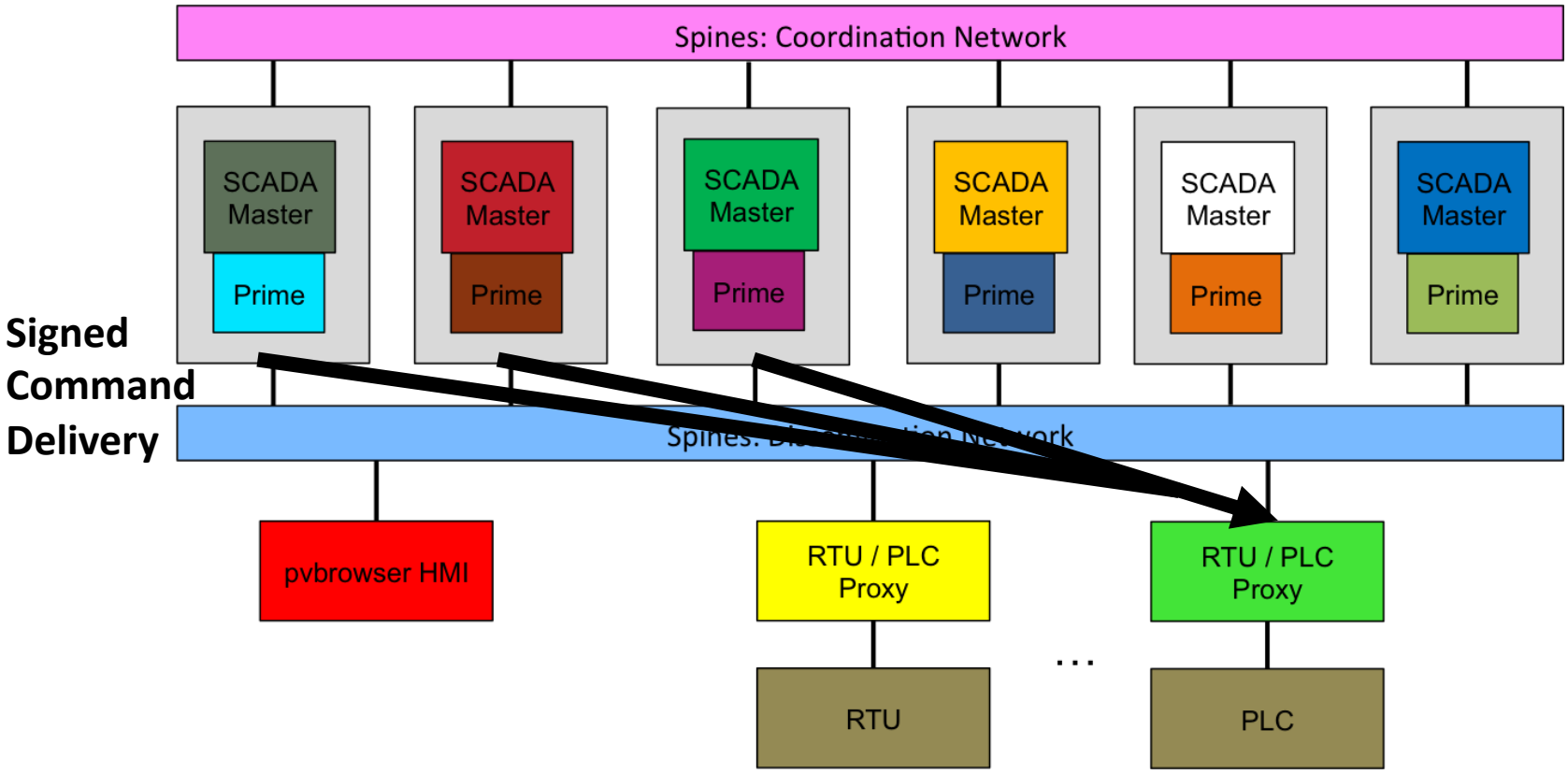


Spire Operation

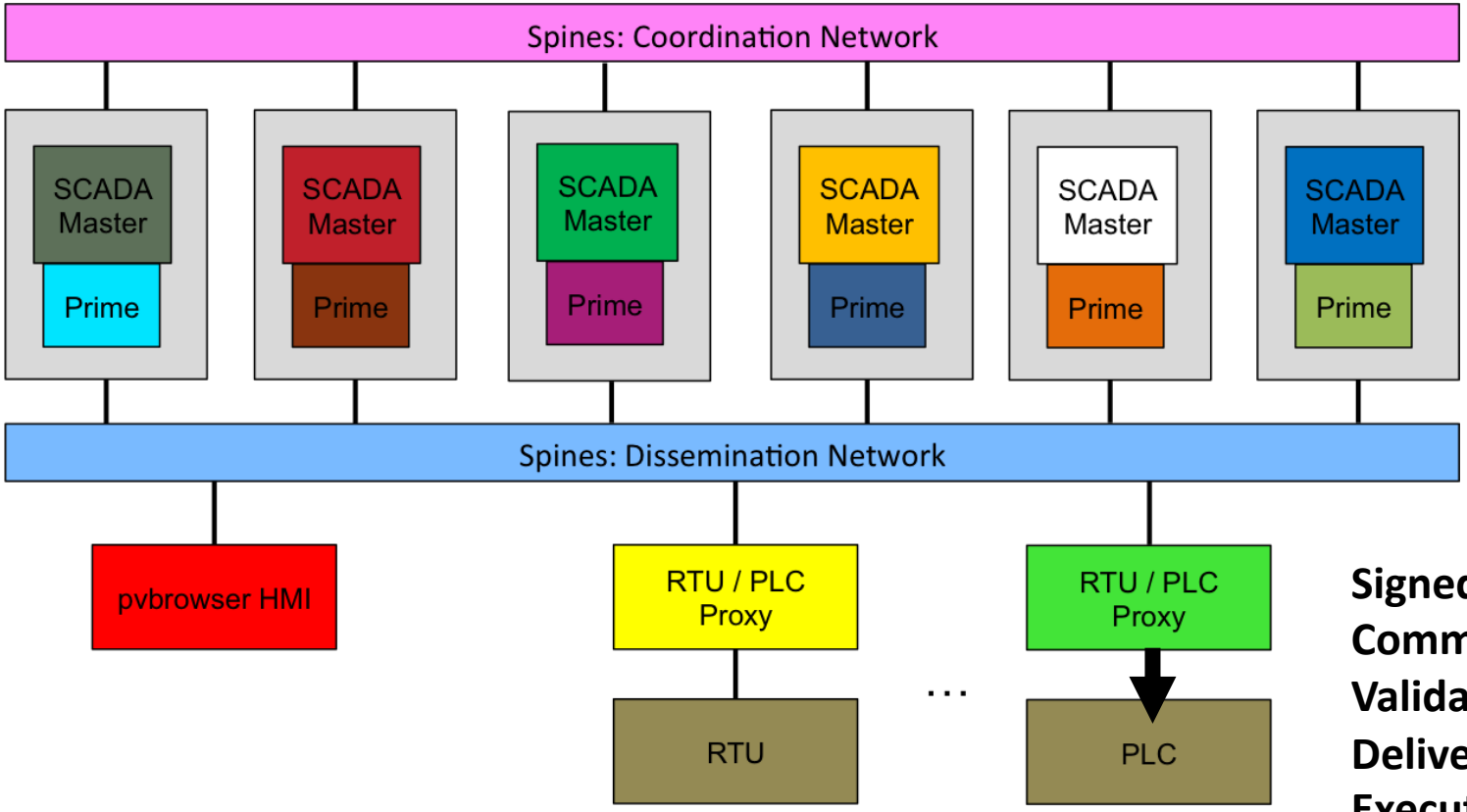
Threshold signature generation



Spire Operation

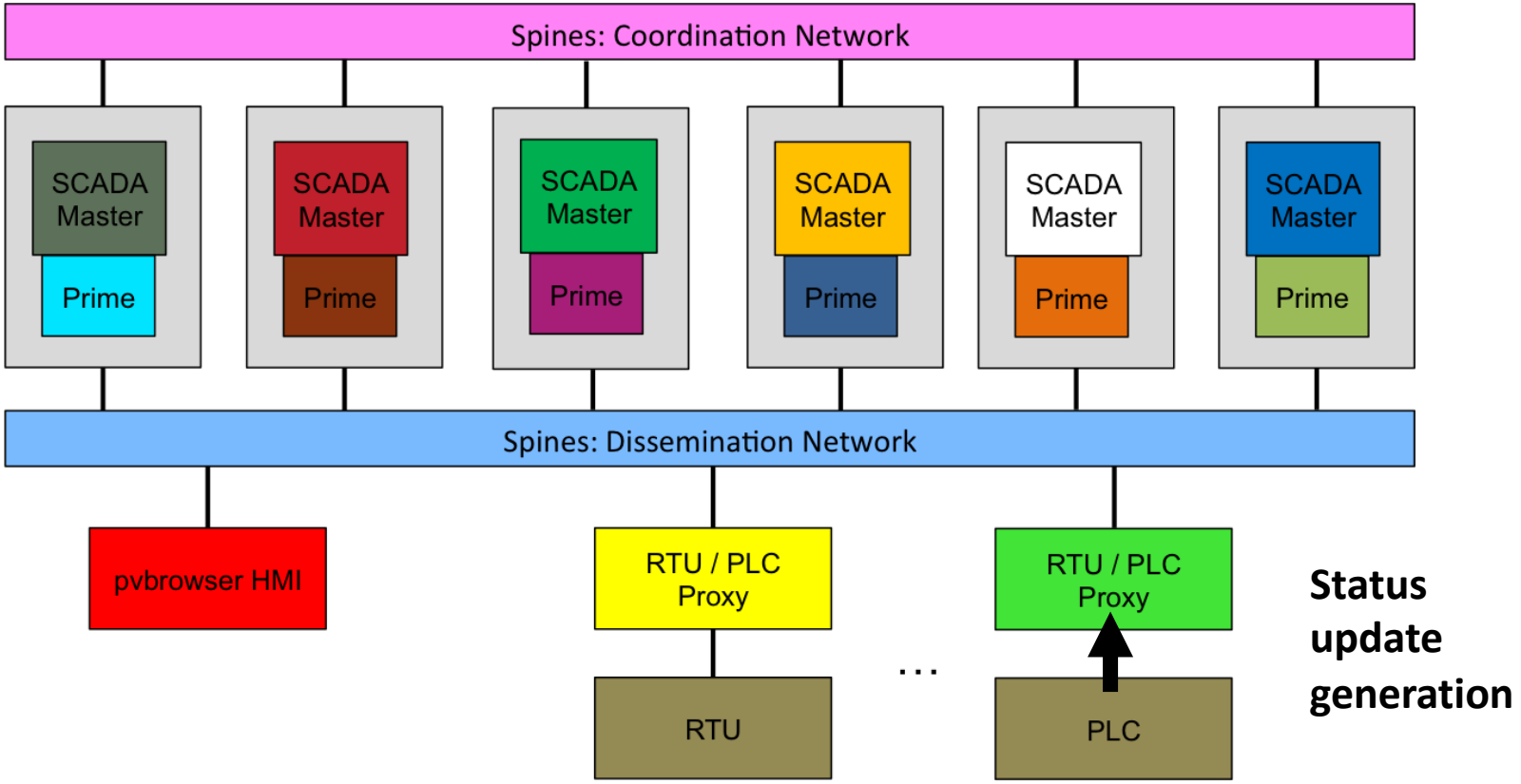


Spire Operation

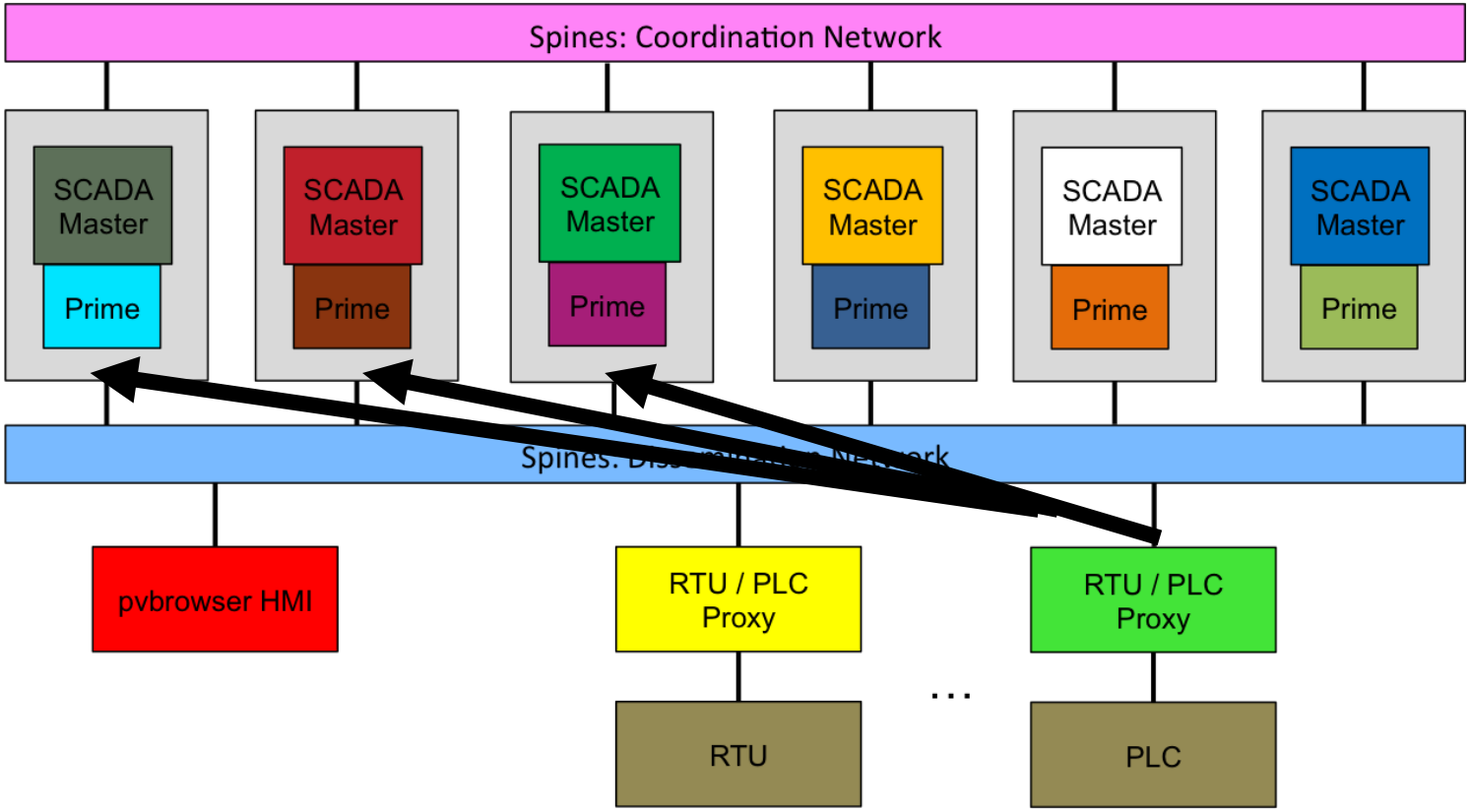


Signed Command Validation, Delivery and Execution

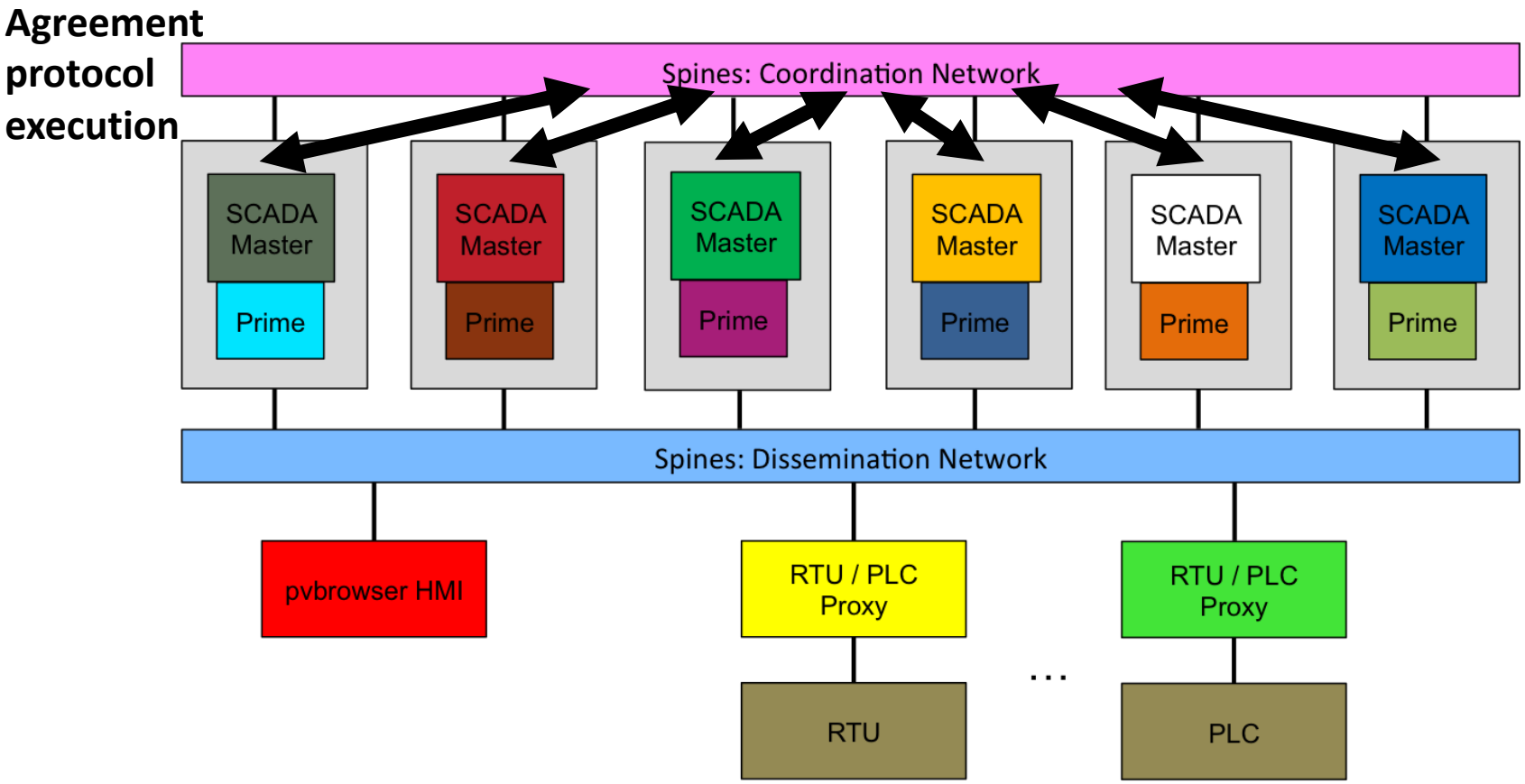
Spire Operation



Spire Operation

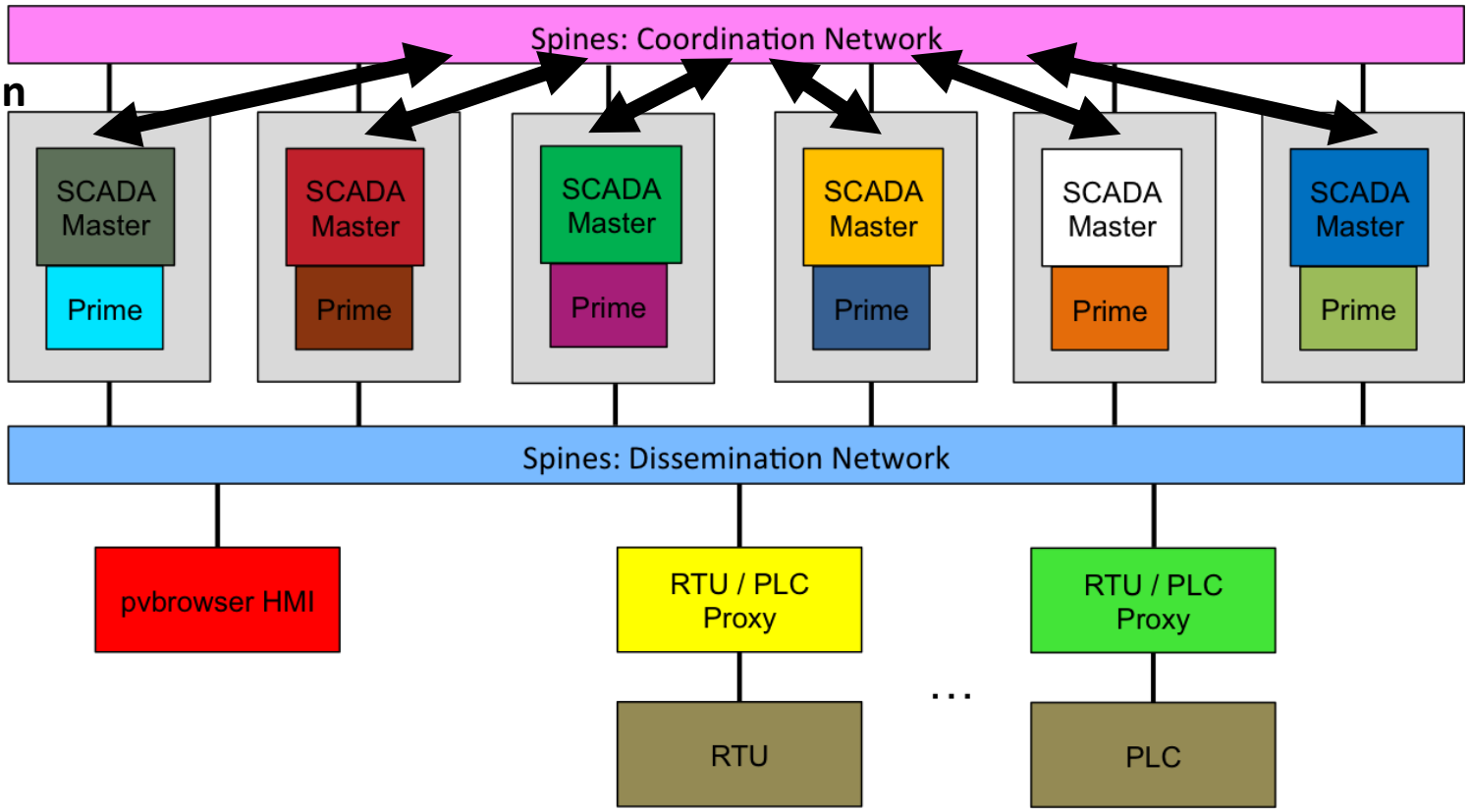


Spire Operation

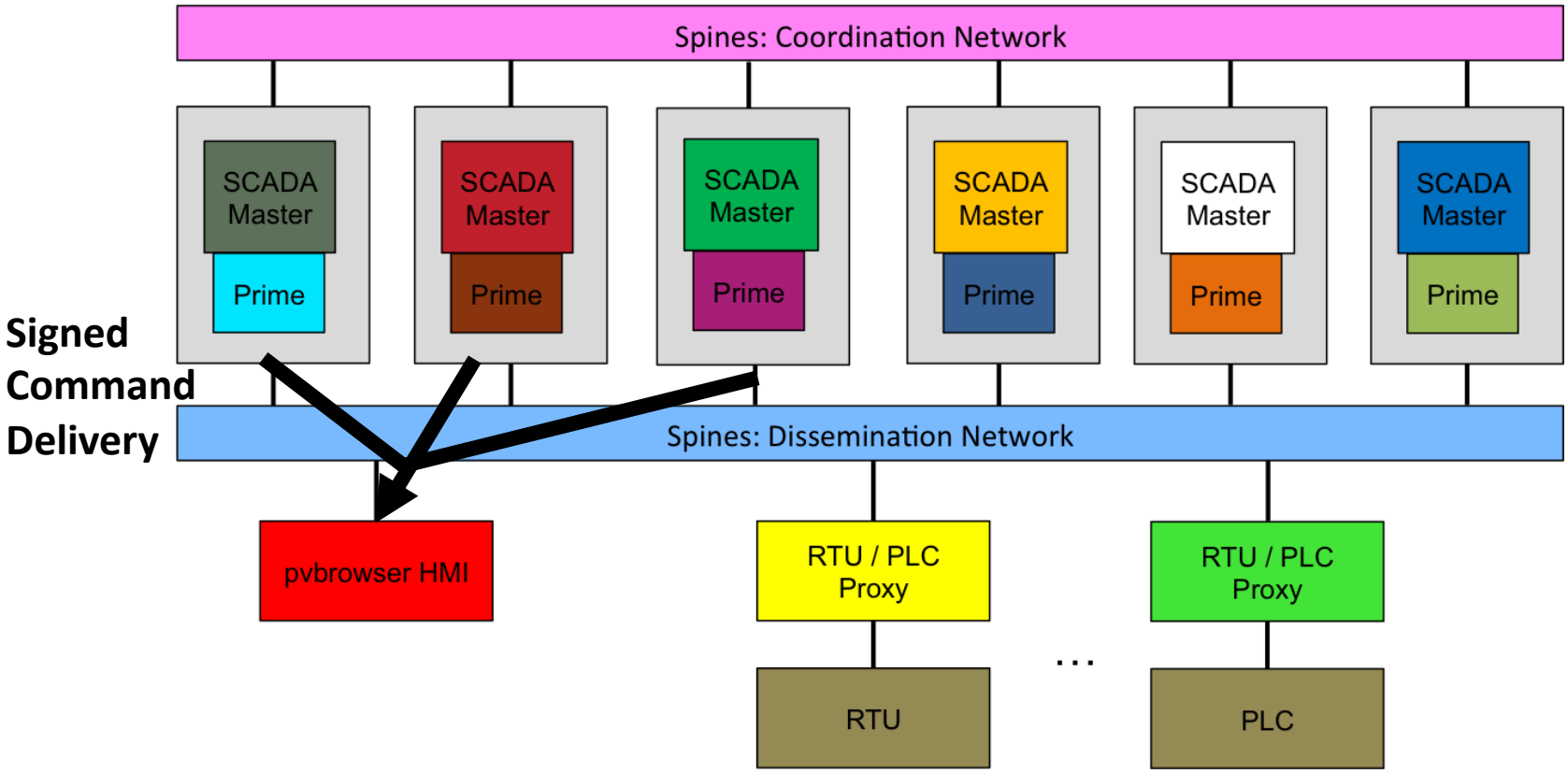


Spire Operation

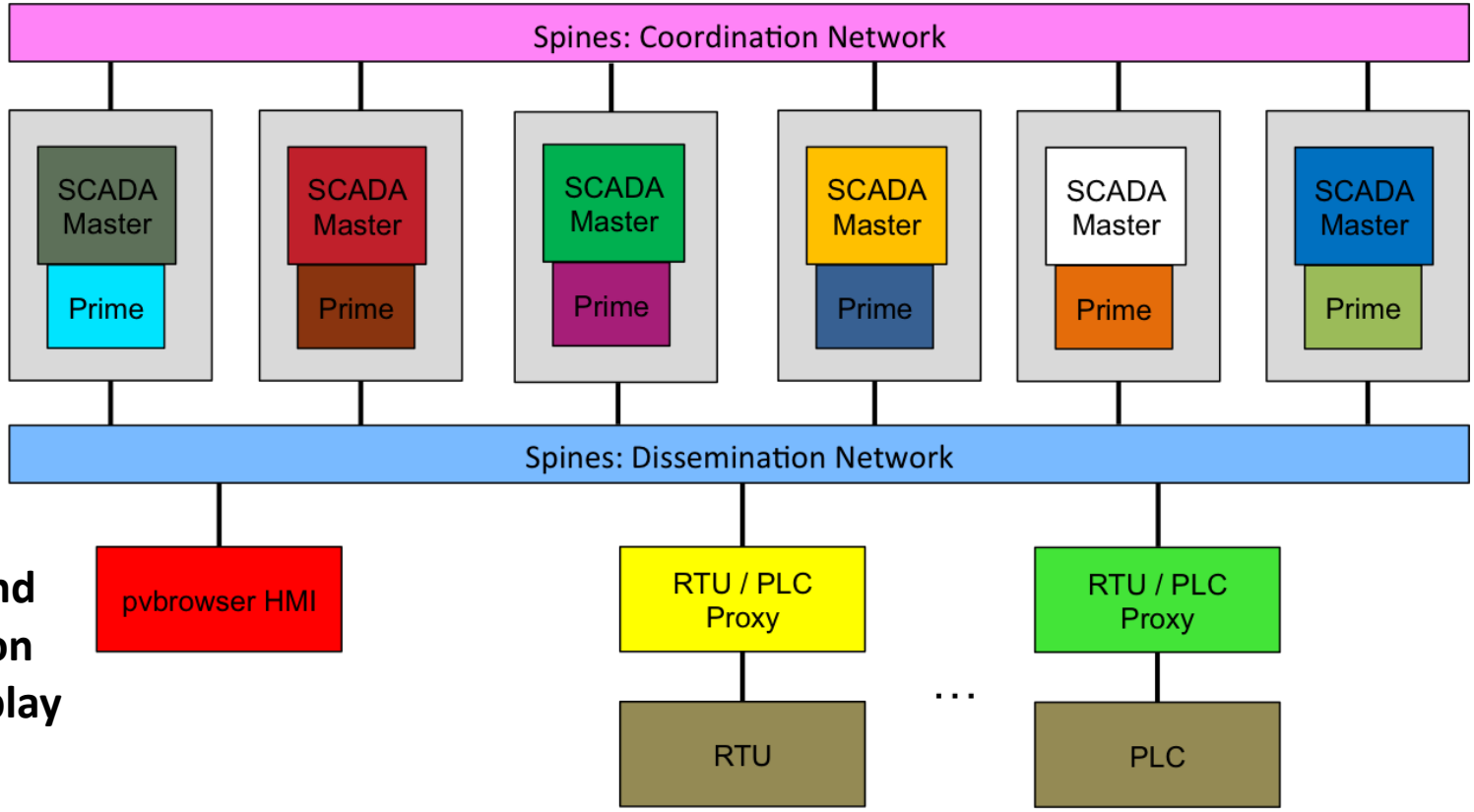
Threshold signature generation



Spire Operation

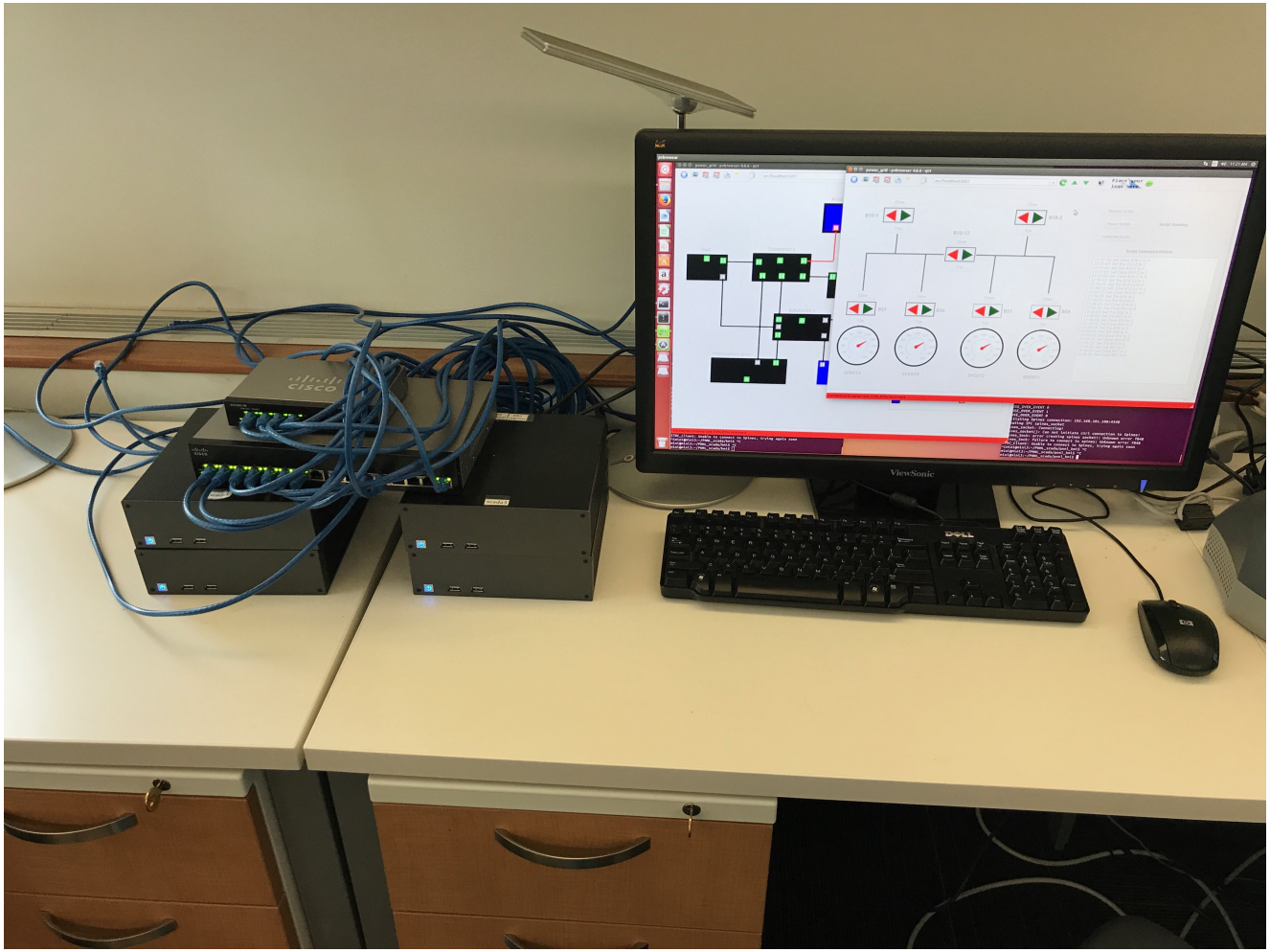


Spire Operation



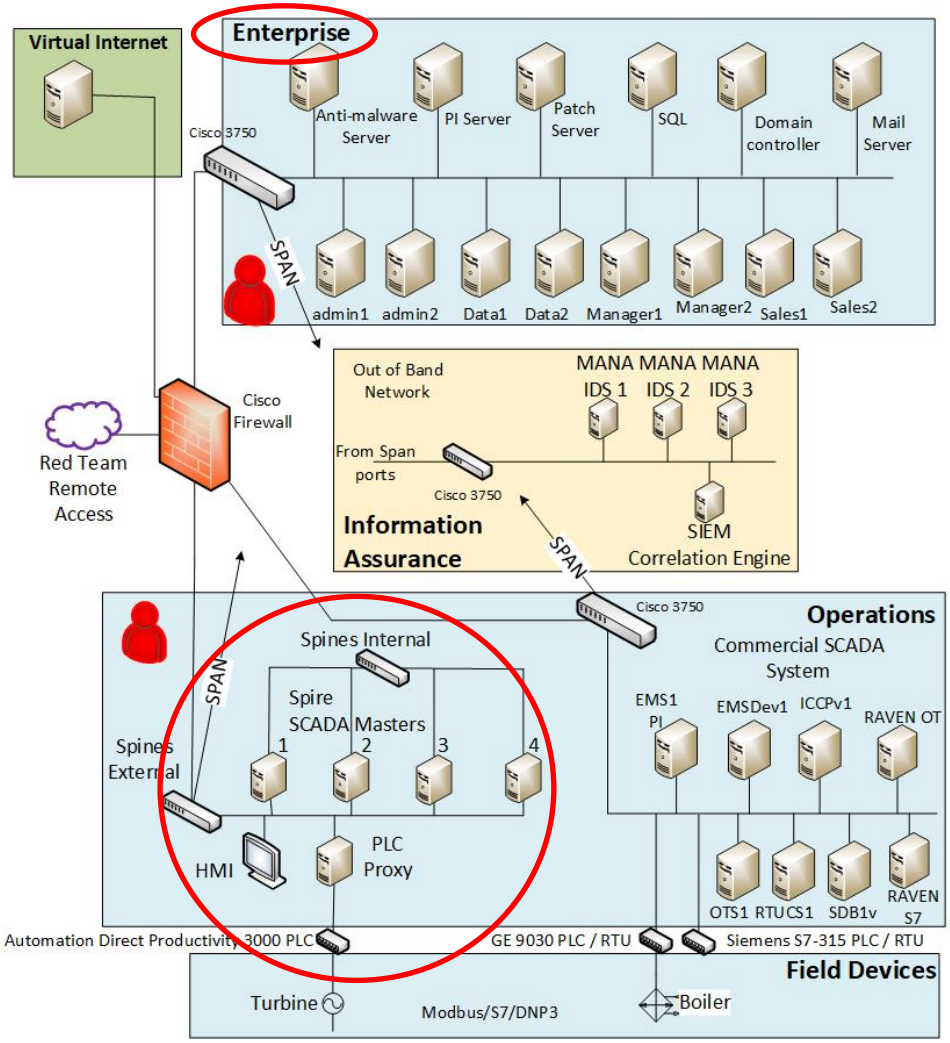
Signed Command Validation and Display Update

Spire as Deployed @ PNNL



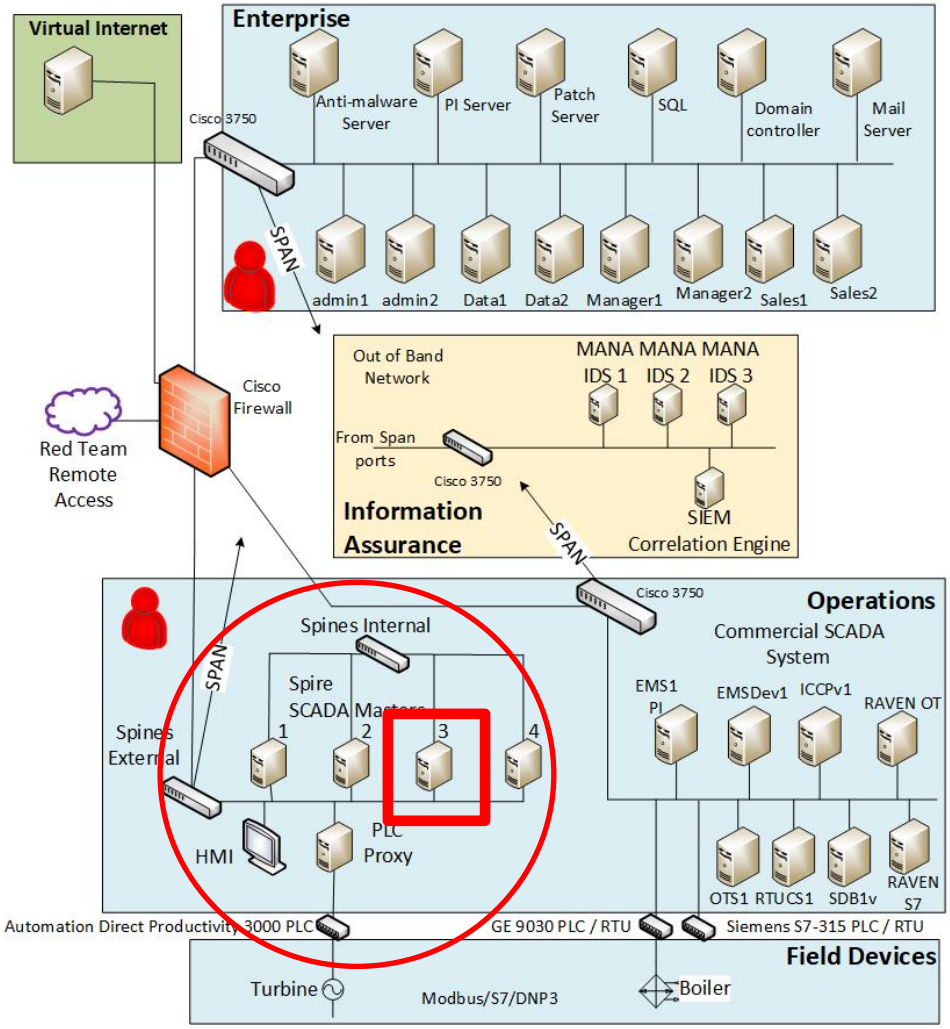
Spire System Attacks

- Started from enterprise network
  - No visibility; gave up after a couple hours
- Given direct access to operations network
  - 2 full days of network attacks (port scanning, ARP poisoning, IP address spoofing, DoS via traffic bursts, …)
- No effect on the system



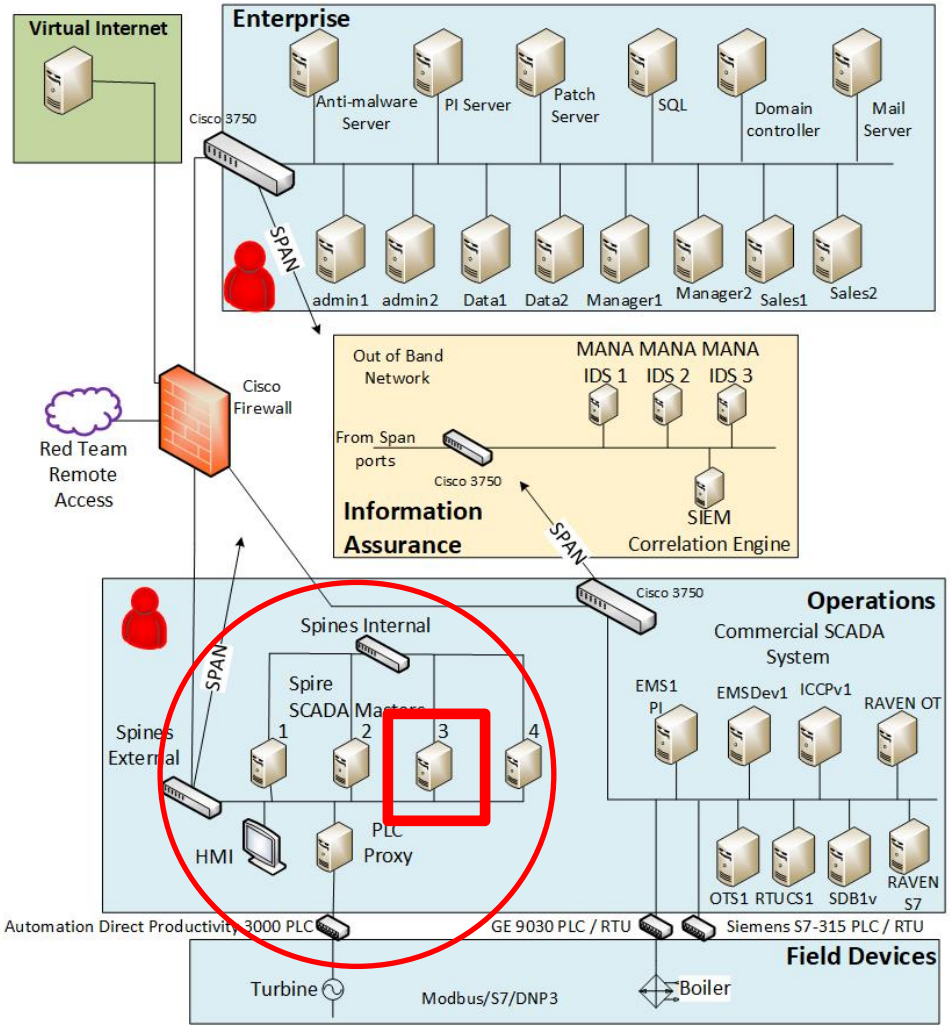
Spire System Excursion (1)

- Excursion: Red team given access to a SCADA Master replica
- User-level access
- Root access + source code
- No effect on the system



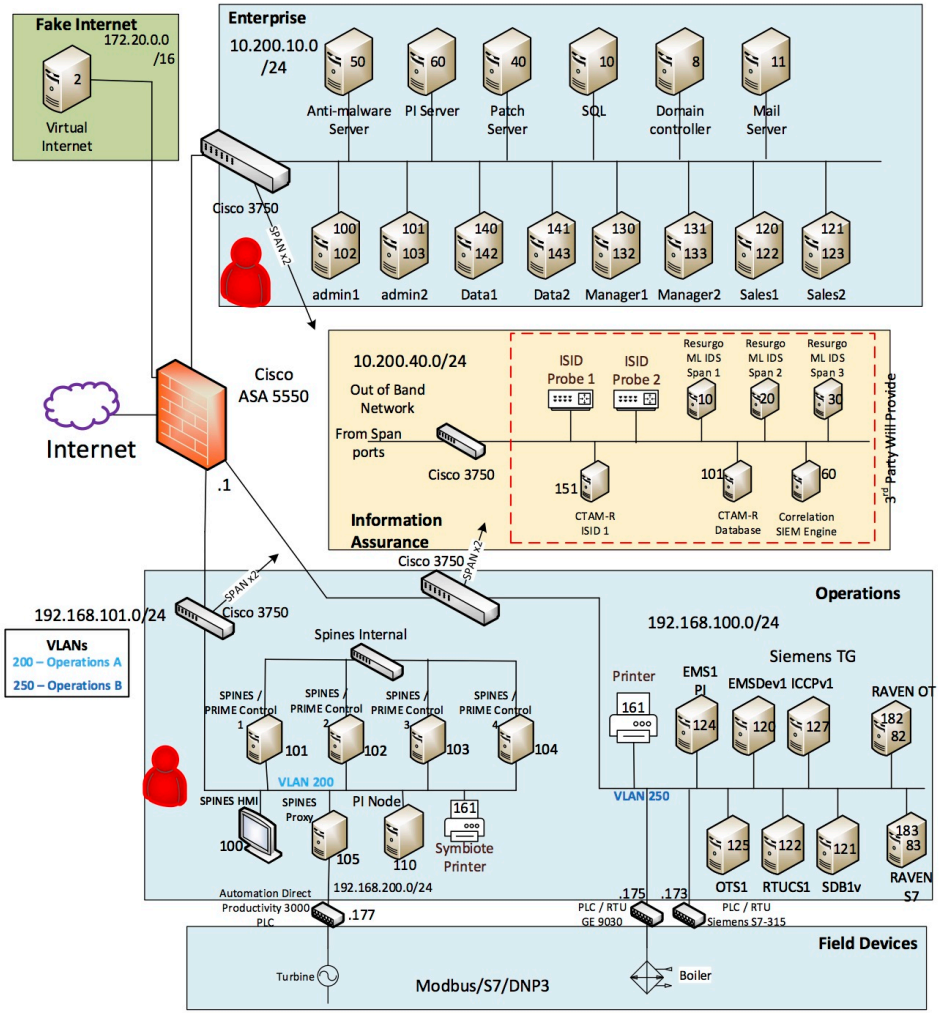
Spire System Excursion (2)

- Excursion: Red team given access to a SCADA Master replica
- User-level access
  - Stopped Spines daemon, launched modified version
  - Tried to escalate privilege
  - Patched running Spines daemon to attempt exploit
- Root access + source code
  - Primarily focused on Spines and fairness
  - Ran modified versions
- No effect on the system



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 Test-Deployment

January 22 – February 2, 2018

DoD ESTCP Power Plant Test Deployment

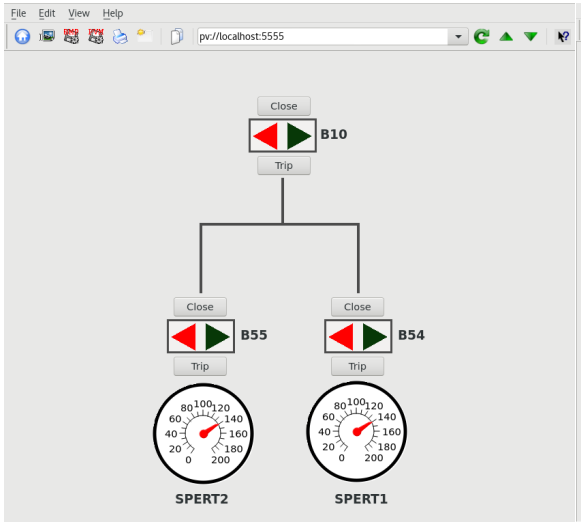
- Spire test deployment at Hawaiian Electric Company (HECO)
  - "Mothballed" Honolulu plant
- Spire installed in Distributed Control System (DCS) room
  - Managed small power topology, controlling 3 physical breakers via Modbus PLC
- Deployment goals
  - Operate correctly in real environment without adverse effects
  - Meet performance requirements

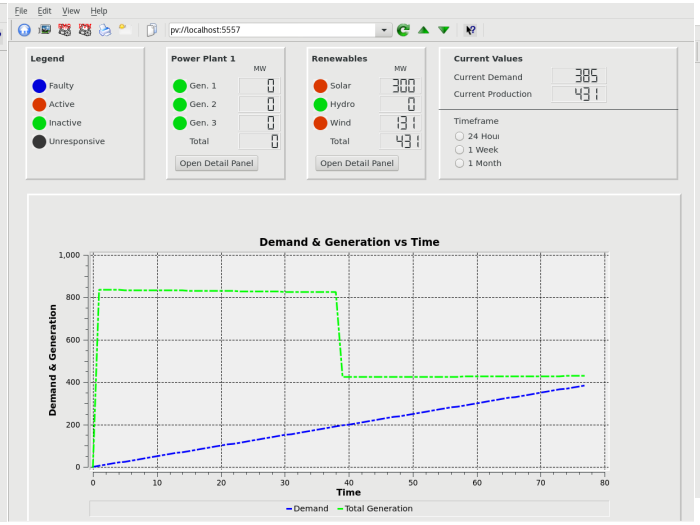
DoD ESTCP Power Plant Test Deployment

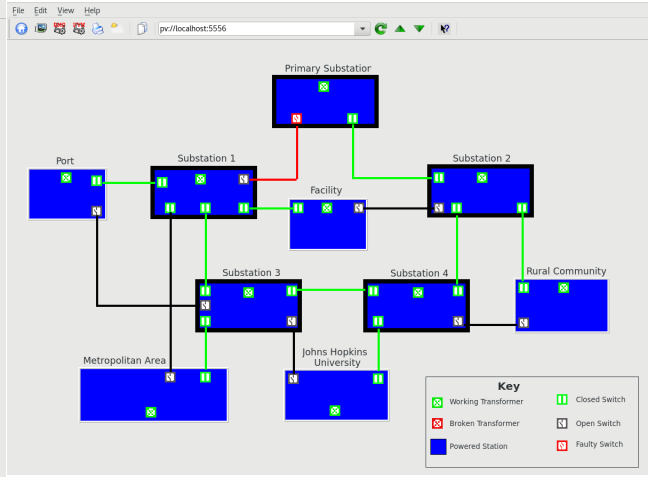
- Spire test deployment at Hawaiian Electric Company (HECO)
  - "Mothballed" Honolulu plant
- Spire installed in Distributed Control System (DCS) room
  - Managed small power topology, controlling 3 physical breakers via Modbus PLC
- Deployment goals
  - Operate correctly in real environment without adverse effects
  - Meet performance requirements

Spire Setup

- Spire HMIs placed in 3 locations throughout the plant: DCS room, control room, demonstration room
- 3 SCADA Scenarios: 1 with real PLC and physical breakers, 2 emulated with a total of 16 emulated PLCs

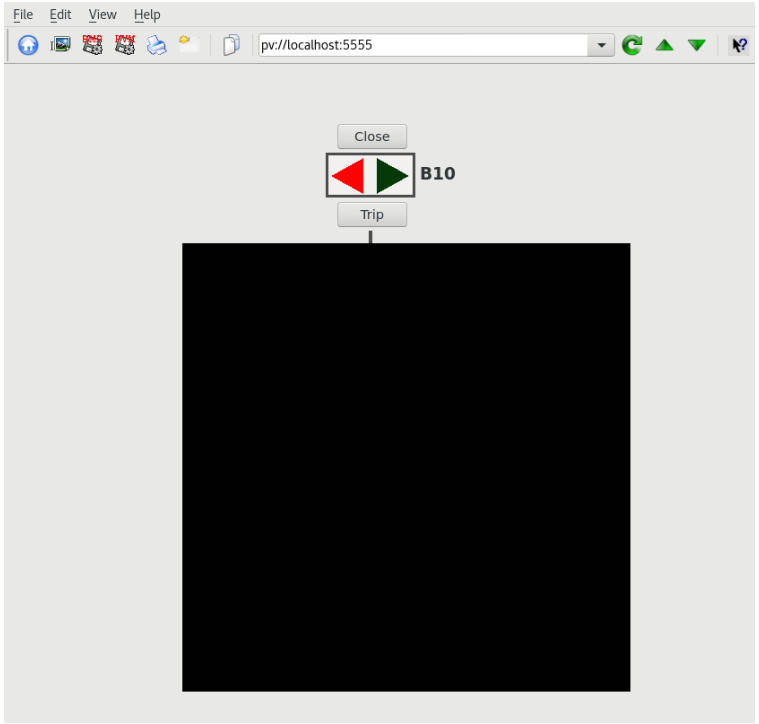




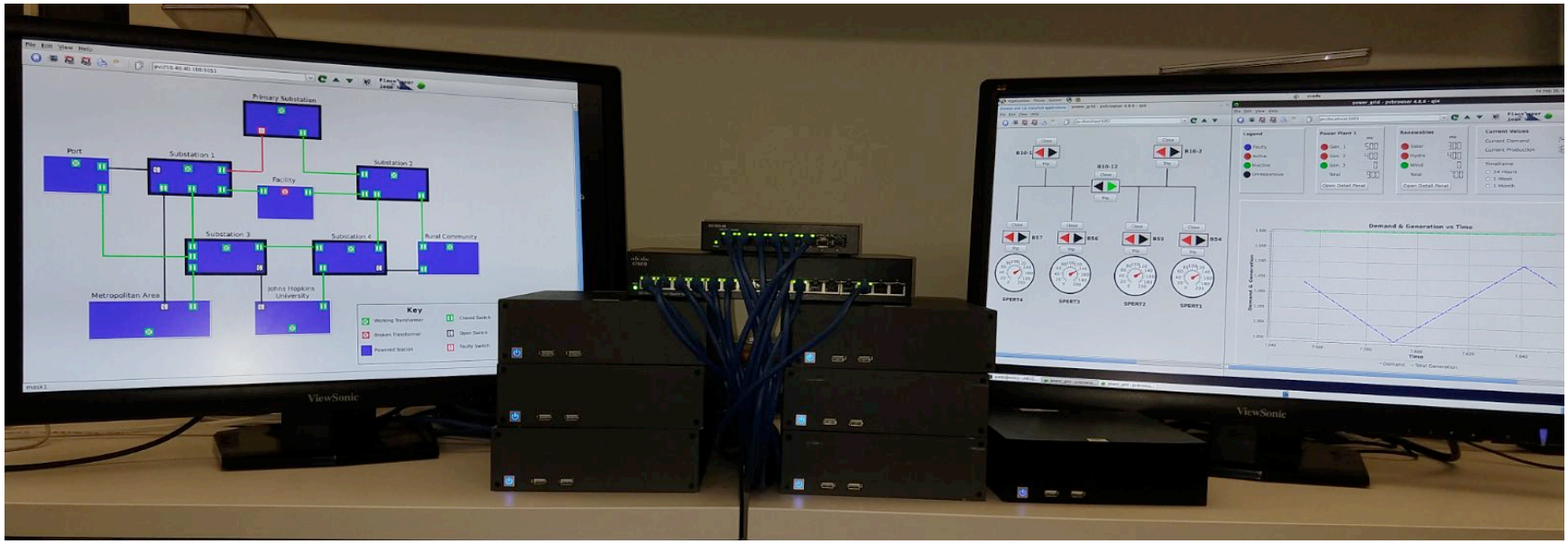


Deployment Results

- 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



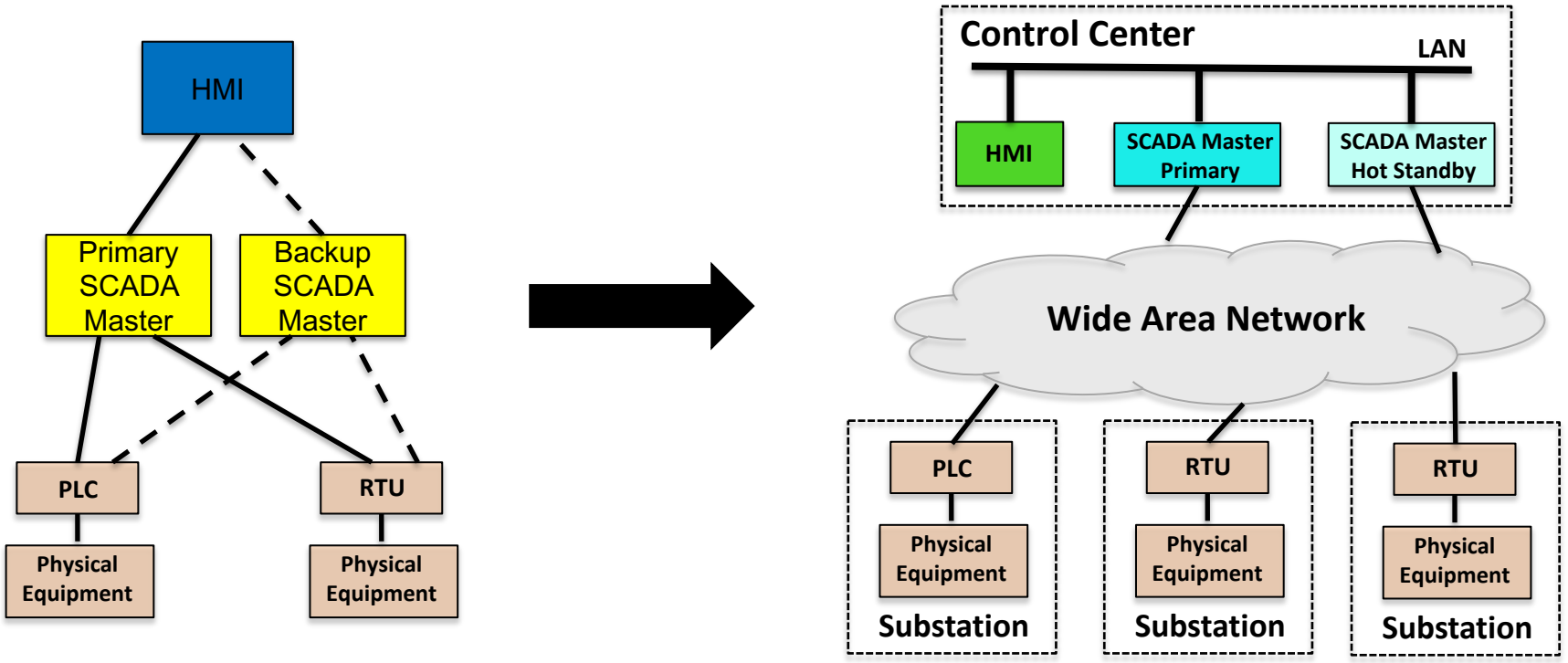
The Spire System: Single Control Center



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

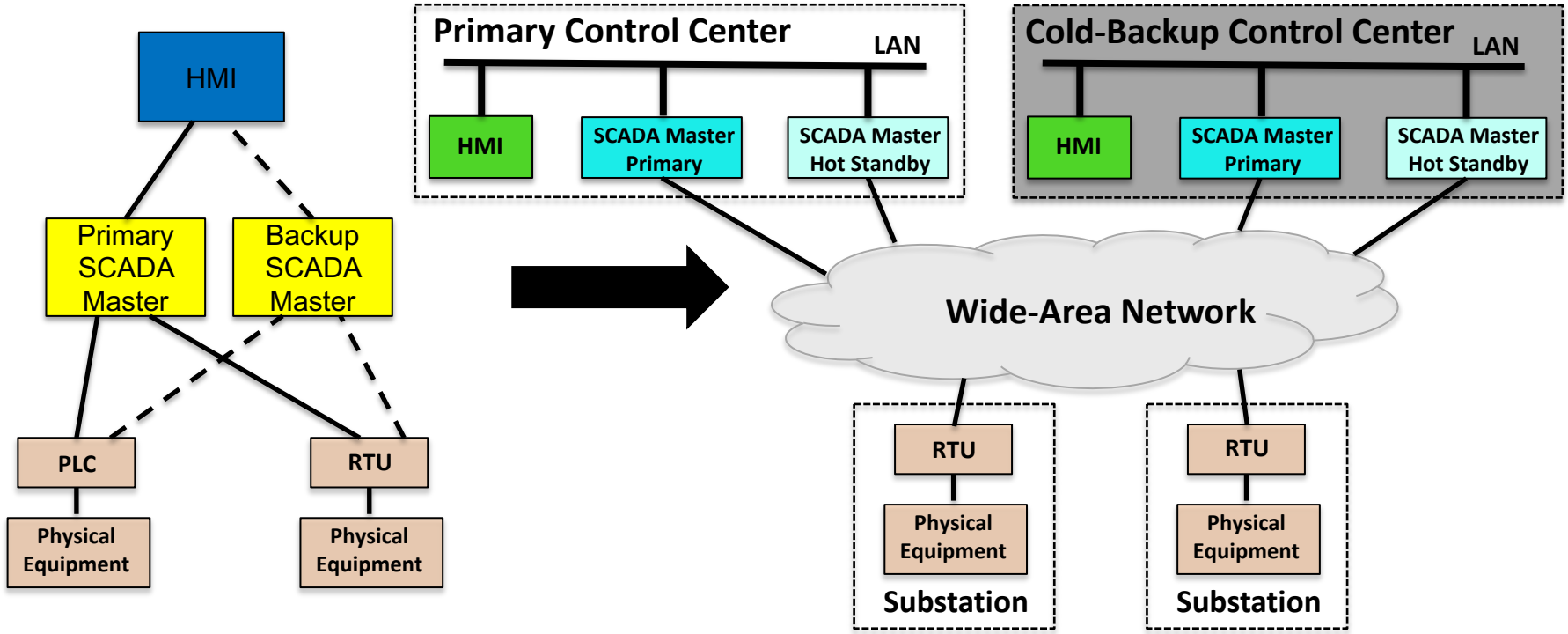
Wide-Area Transmission Architecture

Wide-Area Transmission Systems



- SCADA systems support large power grids with PLCs in many substations spanning hundreds of miles
- What happens if the control center is disconnected?

Wide-Area Transmission Systems



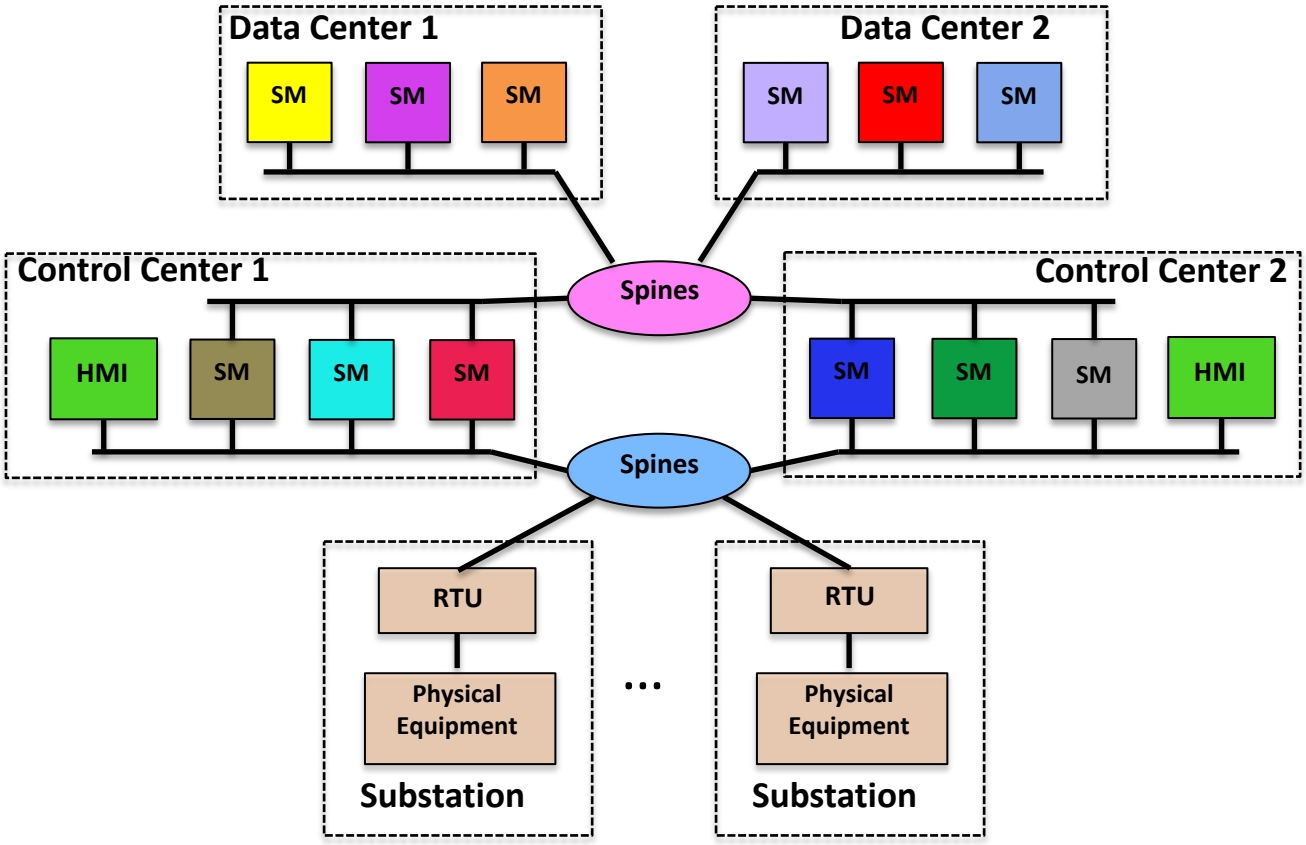
- Primary-Backup architecture is not sufficient to address malicious attacks -- disconnection leads to split-brain problem

Resilient Wide-Area Architecture

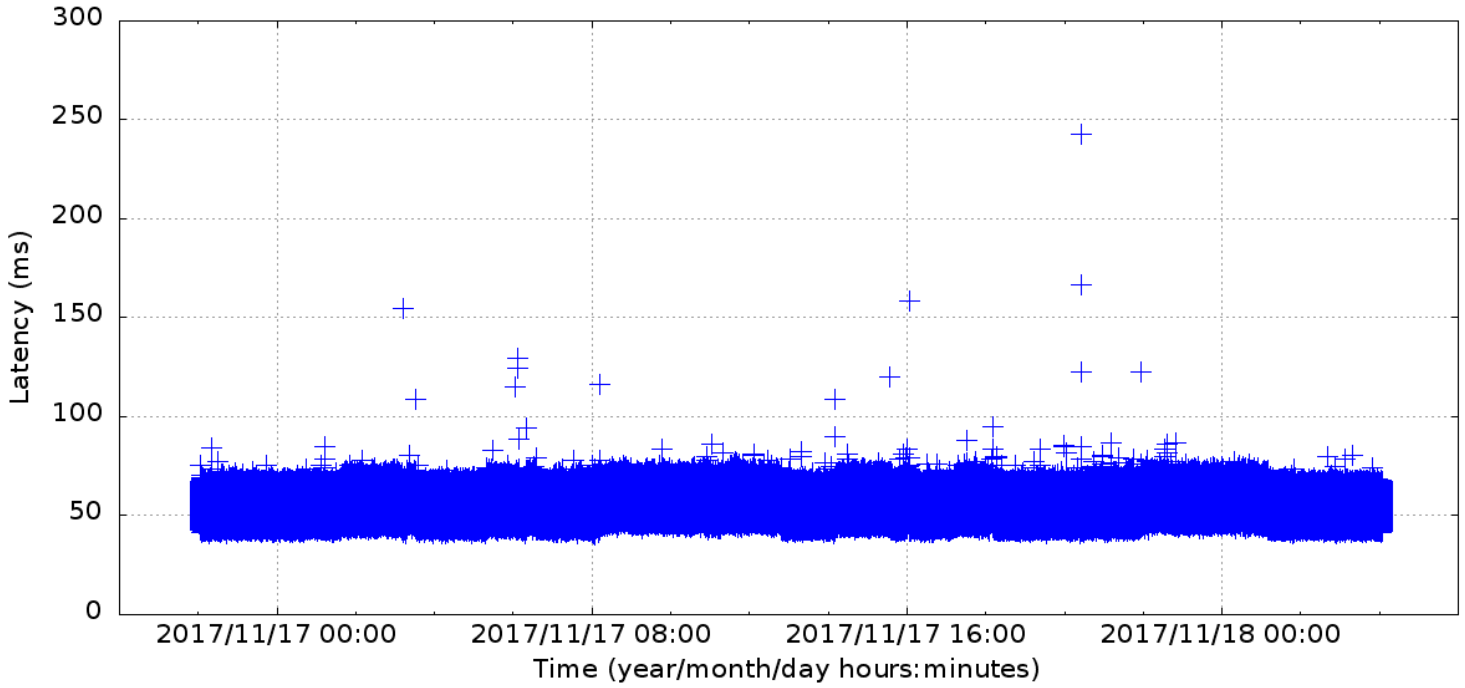
- To protect against sophisticated network attacks, Spire supports multiple control sites
- Since it is expensive to construct control sites, Spire is able to operate with two control sites plus additional sites that can be served by commodity data centers (that lack the ability to communicate with RTUs and PLCs in the field)

Resilient Wide-Area Architecture

- Successfully withstands: 1 intrusion, 1 disconnected site, 1 replica undergoing proactive recovery

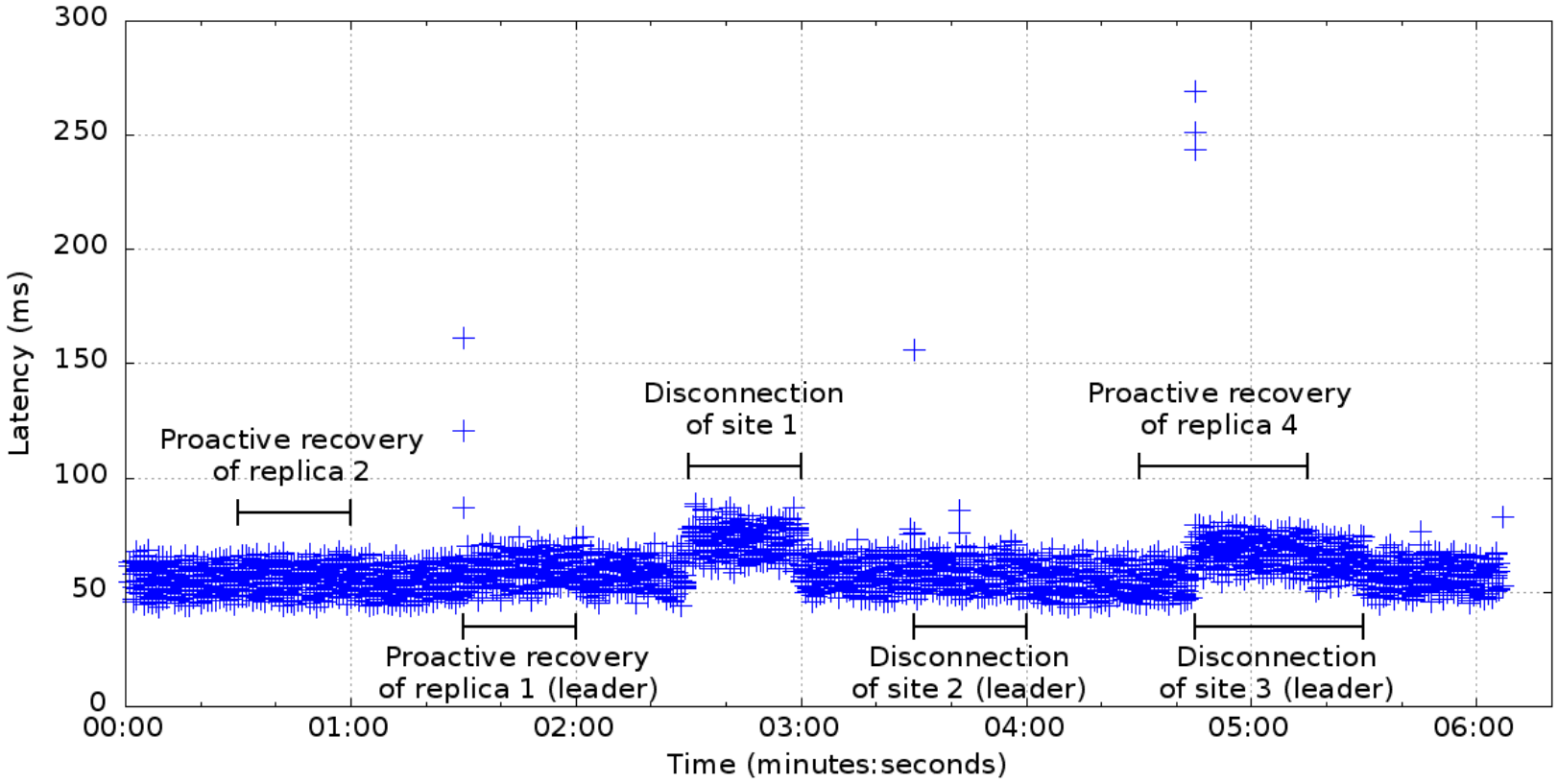


Wide Area Update Latency Plot



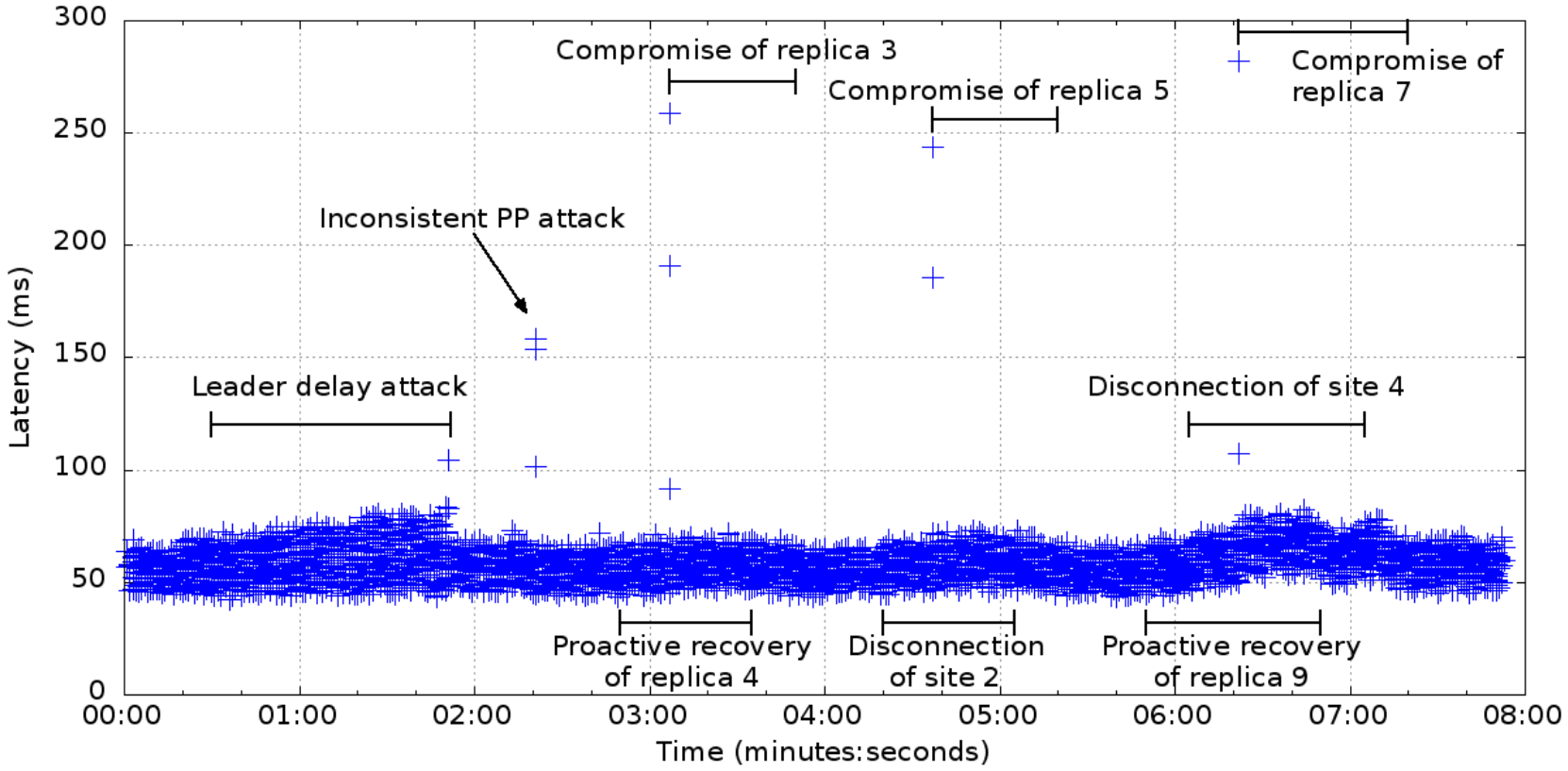
- 30-hour wide-area deployment of configuration 3+3+3+3
  - Control centers at JHU and SVG, data centers at WAS and NYC
  - 10 emulated substations sending periodic updates
  - 1.08 million updates (108K from each substation)
  - Nearly 99.999% of updates delivered within 100ms (56.5ms average)

Wide Area: Latency Under Attack



- Targeted attacks designed to disrupt the system
  - All combinations of site disconnection (due to network attack) + proactive recovery

Wide Area: Latency Under Attack

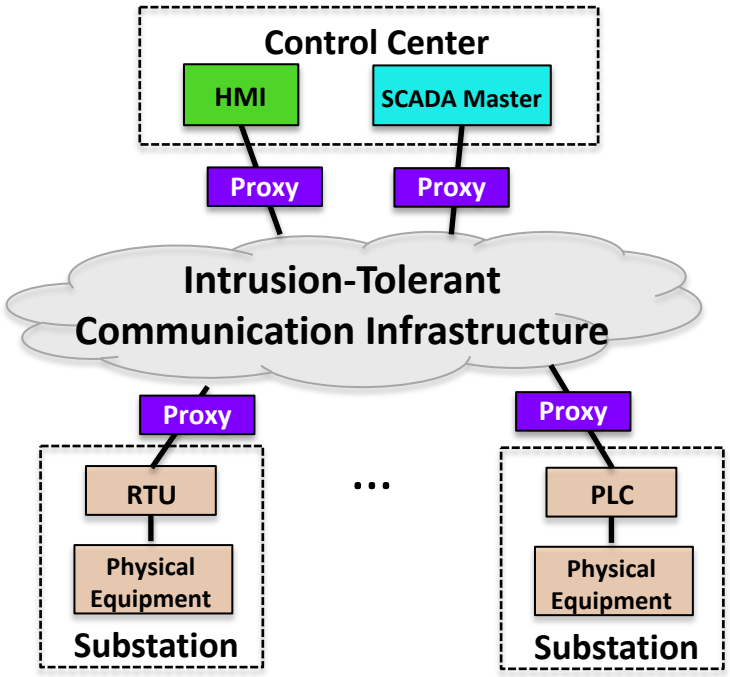


- Targeted attacks designed to disrupt the system
  - All combinations of intrusion + site disconnection (due to network attack) + proactive recovery

Path to Transition

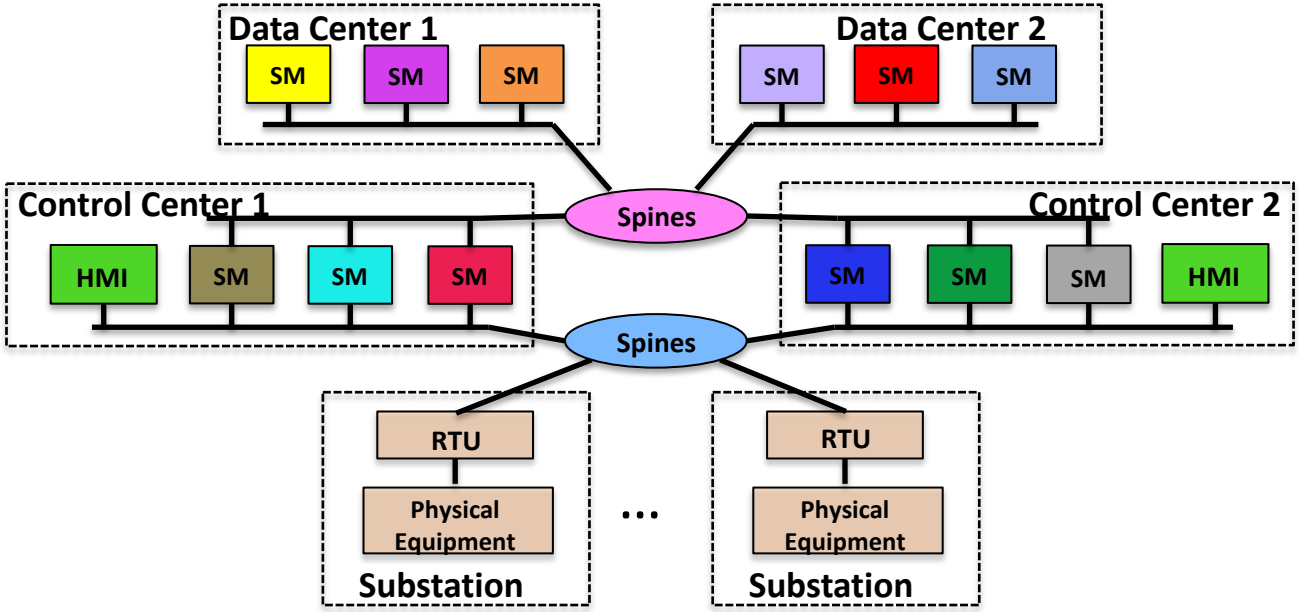
First Step: Network-Level Resilience

- Protects communication infrastructure
  - Standard, insecure protocols (e.g. Modbus, DNP3) limited to direct (cable) connection between proxy and device
- Accommodates existing system architecture and components



Second Step: Full Intrusion-Tolerance

- Employs full power of Spire system, protecting against system intrusions/compromises as well as network attacks
  - Protects communication infrastructure (intrusion-tolerant network)
  - Protects SCADA Master (intrusion-tolerant system state)
- Requires substantial architectural changes



Path to Transition

- Discussions with a SCADA manufacturer
- Discussions with several U.S.-based power companies
- Discussions with several relevant U.S. government entities
- Looking for partners

Resources

- JHU DSN Lab www.dsn.jhu.edu
- Spread Concepts LLC www.spreadconcepts.com

- Yair Amir www.cs.jhu.edu/~yairamir/
- Amy Babay www.cs.pitt.edu/~babay/

- Spire www.dsn.jhu.edu/spire/
- Multicompiler www.github.com/securesystemslab/multicompiler

- Papers:
  - Deploying Intrusion-Tolerant SCADA for the Power Grid www.dsn.jhu.edu/papers/DSN_2019_SCADA_Experience.pdf
  - Toward an Intrusion-Tolerant Power Grid: Challenges and Opportunities www.dsn.jhu.edu/papers/scada_ICDCS_2018.pdf
  - Network-Attack-Resilient Intrusion-Tolerant SCADA for the Power Grid www.dsn.jhu.edu/papers/scada_DSN_2018.pdf