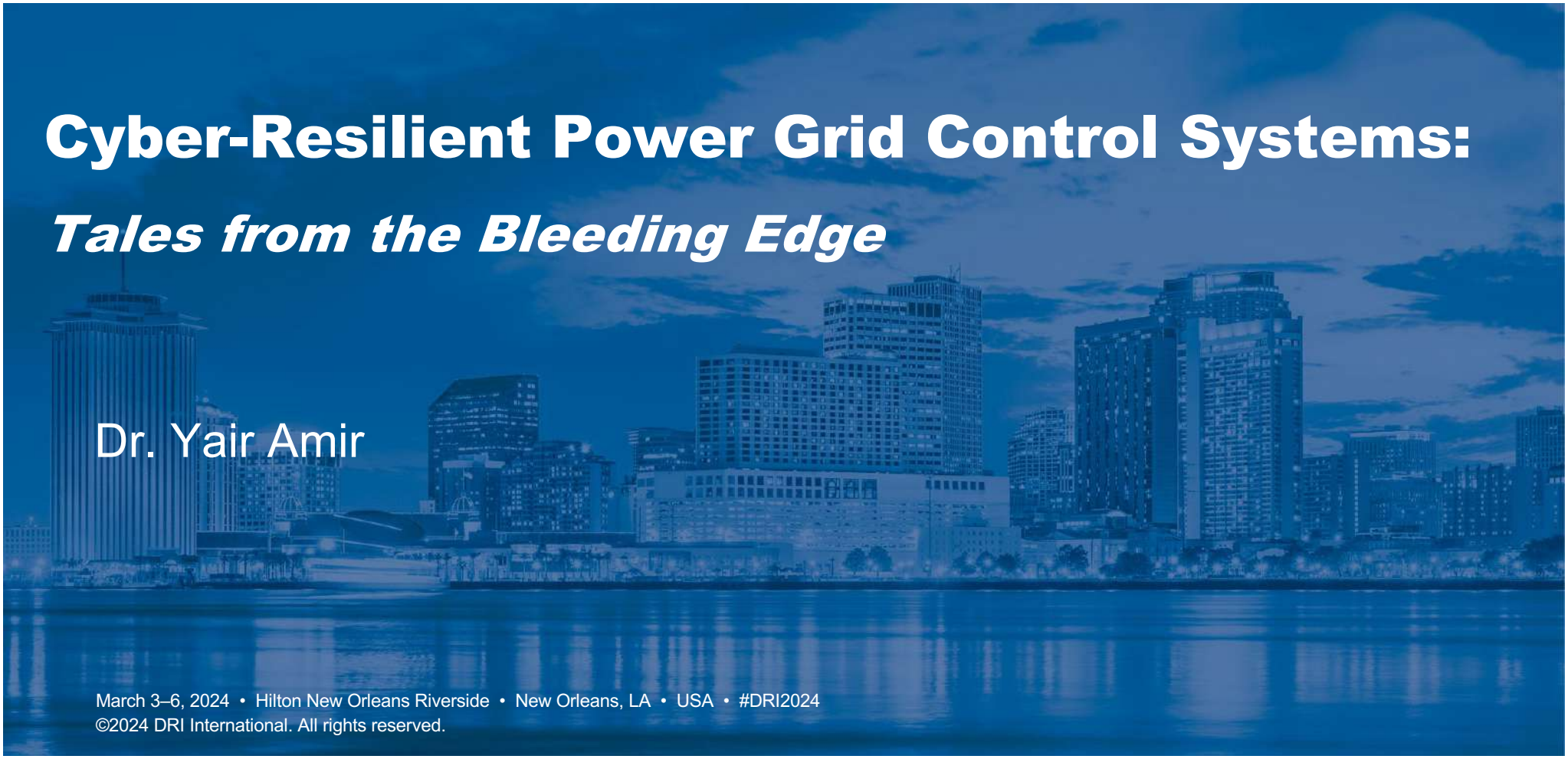


Cyber-Resilient Power Grid Control Systems:

Tales from the Bleeding Edge

Dr. Yair Amir

March 3–6, 2024 • Hilton New Orleans Riverside • New Orleans, LA • USA • #DRI2024

DRI2024
The Business Continuity Conference

Speaker Card

- Resilient networked systems engineer for nearly 4 decades
  - » Open-source infrastructure tools
  - » Deployed systems in the commercial and government spaces
- Professor of Computer Science @ Johns Hopkins University (1995)
  - » Distributed Systems and Network lab (https://jhu-dsn.github.io/)
  - » Converted to Professor Emeritus last year ☺
- Co-founder of Spread Concepts LLC (2000)
  - » A boutique consulting firm (www.spreadconcepts.com)
- Co-founder of LTN Global Communications (2008)
  - » A specialized global cloud provider serving the media industry (www.ltnglobal.com)
- Passionate about making the power grid resilient to cyberattacks
  - » System compromises and network attacks (https://jhu-dsn.github.io/spire/)

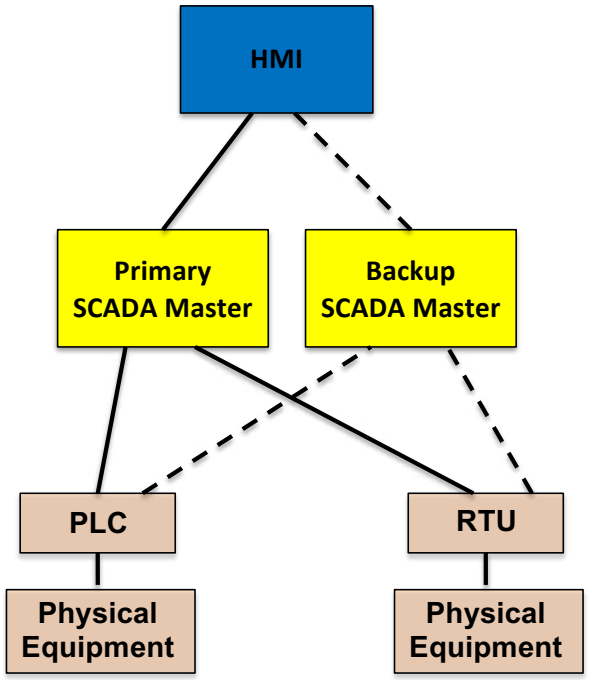
SCADA: Control Systems for the Power Grid

(and other critical infrastructure)

- Supervisory Control And Data Acquisition (SCADA): monitoring and control of critical infrastructure
  - » Power grid, water supply, waste management
- Must be continuously available and operating at expected level of performance
  - » 100-200 milliseconds – control-center to field-device cycle
  - » ~4 milliseconds – certain safety operations in the substation
- Failures and downtime can cause catastrophic consequences
  - » Power outages, blackouts
  - » Equipment damage
  - » Human casualties
- Becoming a target for nation-state attackers

SCADA for the Power Grid: a Primer

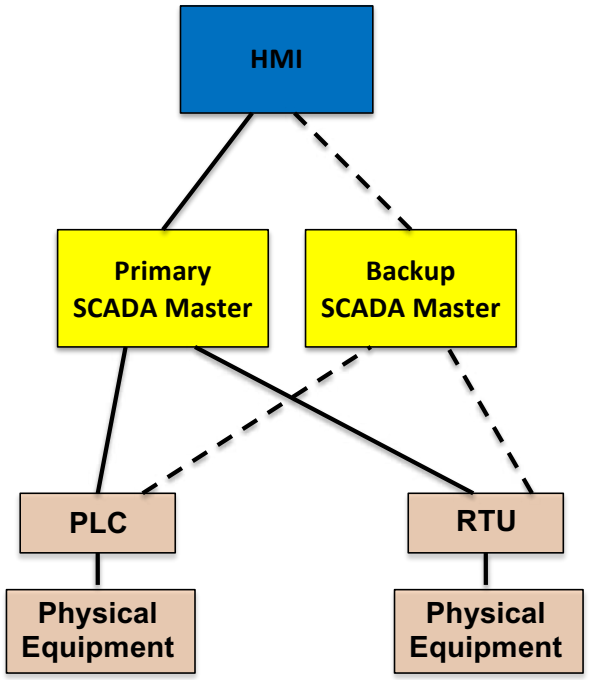
- Human Machine Interface (HMI) provides graphical displays for the operator
- SCADA Master provides central management and control
  - » Primary and backup architecture for redundancy
    - Backup takes over if primary fails
- Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) control power equipment
  - » Essentially, specialized computers



Emerging Power Grid Threats

SCADA systems are vulnerable on several fronts:

- System-level compromises
  - » SCADA Master – system-wide damage
  - » RTUs and PLCs – more limited effects
  - » HMIs
- Network-level attacks
  - » Routing attacks that disrupt or delay communication
  - » Resource-consumption denial of service attacks that disrupt communication
  - » Sophisticated denial of service attacks that isolate critical components from the rest of the network



Notable Nation-State Attacks on SCADA

- Stuxnet (2010)
  - » Targeted certain Siemens PLCs, re-programming them to cause physical damage to controlled equipment (centrifuges used to separate nuclear material in Iran)
- Ukraine power grid attack – *BlackEnergy-3* (2015)
  - » Power outage affecting about 230,000 customers for several hours
  - » Switched off 30 substations
  - » First publicly-acknowledged cyberattack leading to grid outage
- Ukraine power grid attack – *CRASHOVERRIDE* (2016)
  - » Part of Kyiv lost power for an hour
  - » Aimed to compromise protective relays, allowing a power surge to destroy the transformers they protect. Damage could have been much worse if successful in that goal
- Colonial Pipeline attack – (2021)
  - » Ransomware attack on the billing infrastructure (essentially an IT system)
  - » Shutdown of the pipeline (OT system) as a precaution, leading to several days of fuel shortages

Current State of Response

- ”Best Practices Stop Nation-State Attackers”
  - Joseph H. McClelland, Director, Federal Energy Regulatory Commission (FERC), November 2019 @ the National Academies
- Is this a good assumption?
  - A strong assumption about perimeter defense
  - Probably **yes** for common threats
  - It still requires a process
    - Compilation of best practices; dissemination; implementation; continuous update
    - As you all know ☺
- Is it implemented in practice?
  - In my limited experience with big utilities – **yes** – (Hawaiian Electric, PJM, Florida Power & Light)
- What about sophisticated Nation-State attackers?

DoD Environmental Security Technology Certification Program (ESTCP) Project (2016-2018)

Resurgo LLC, Johns Hopkins University, Spread Concepts LLC

Pacific Northwest National Lab (PNNL), SANDIA National Labs

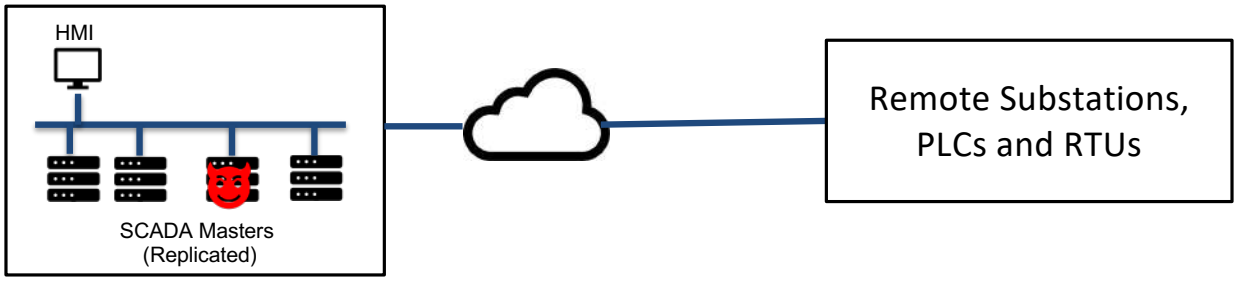
Hawaiian Electric (HECO)

Address two questions:

- Are Best Practices effective against Nation-State attackers ?
  - Red Team Experiment
  - Test Deployment in a utility
- Is there a benefit to cyber-resilient SCADA research coming out of DoD/DARPA ?
  - Spire: Intrusion-tolerant SCADA for the power grid

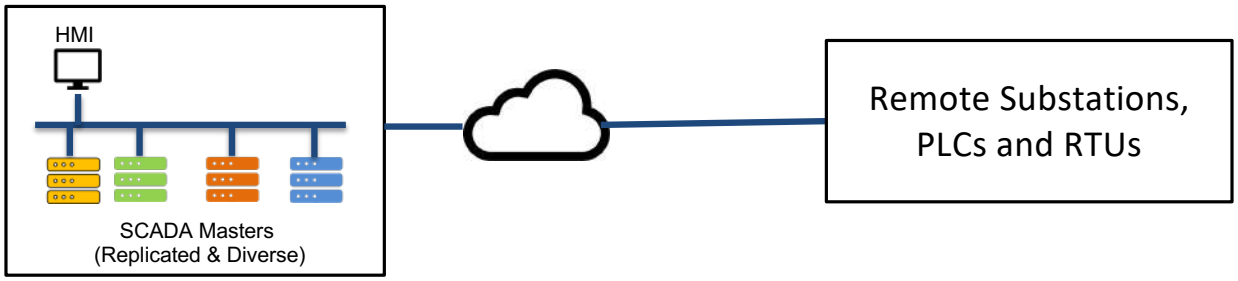
Spire: Intrusion-Tolerant SCADA for the Power Grid

- Spire continues to work correctly even under system-level compromises and network-level attacks
- Intrusion-tolerance as the core design principle
  - » Intrusion-tolerant network addressing network-level attacks
  - » Intrusion-tolerant system architecture addressing system-level compromises
    - Replication + voting
    - What prevents an attacker from reusing the same exploit to compromise all replicas?



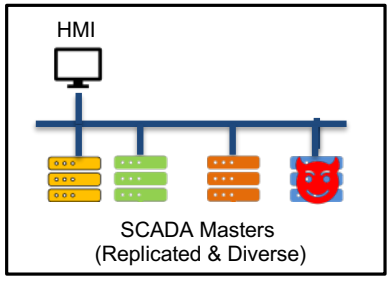
Spire: Intrusion-Tolerant SCADA for the Power Grid

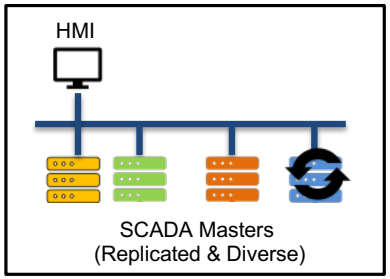
- Spire continues to work correctly even under system-level compromises and network-level attacks
- Intrusion-tolerance as the core design principle
  - » Intrusion-tolerant network addressing network-level attacks
  - » Intrusion-tolerant system architecture addressing system-level compromises
    - Replication + voting
    - Diversity
    - What prevents an attacker from compromising more and more components over time?

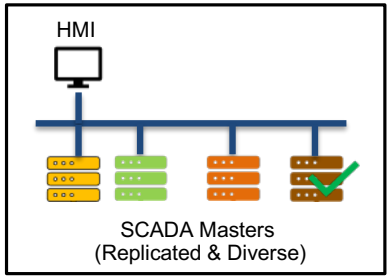


Spire: Intrusion-Tolerant SCADA for the Power Grid

- Spire continues to work correctly even under system-level compromises and network-level attacks
- Intrusion-tolerance as the core design principle
  - » Intrusion-tolerant network addressing network-level attacks
  - » Intrusion-tolerant system architecture addressing system-level compromises
    - Replication + voting
    - Diversity
    - Proactive Recovery

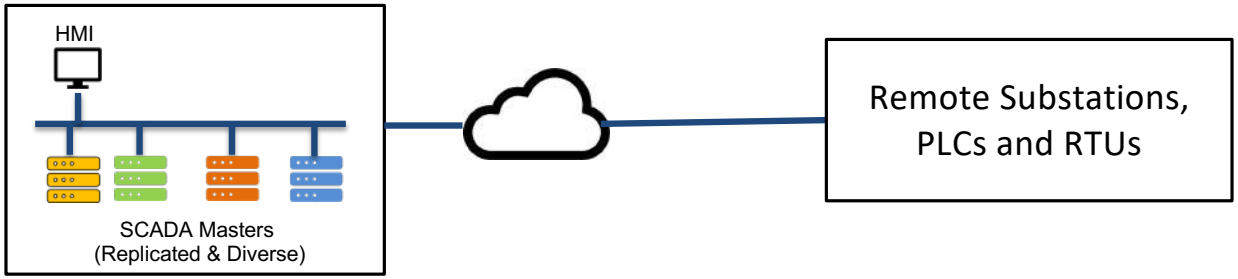






Spire: Intrusion-Tolerant SCADA for the Power Grid

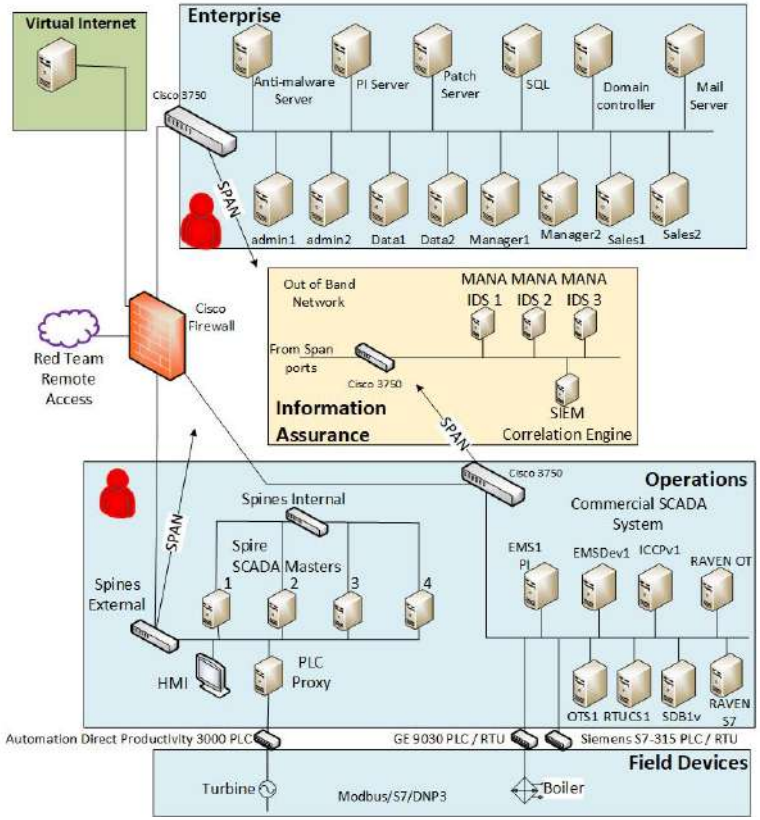
- Spire continues to work correctly even under system-level compromises and network-level attacks
- Intrusion-tolerance as the core design principle
  - » Intrusion-tolerant network addressing network-level attacks
  - » Intrusion-tolerant system architecture addressing system-level compromises
    - Replication + voting
    - Diversity
    - Proactive Recovery



- Open source - https://jhu-dsn.github.io/spire/

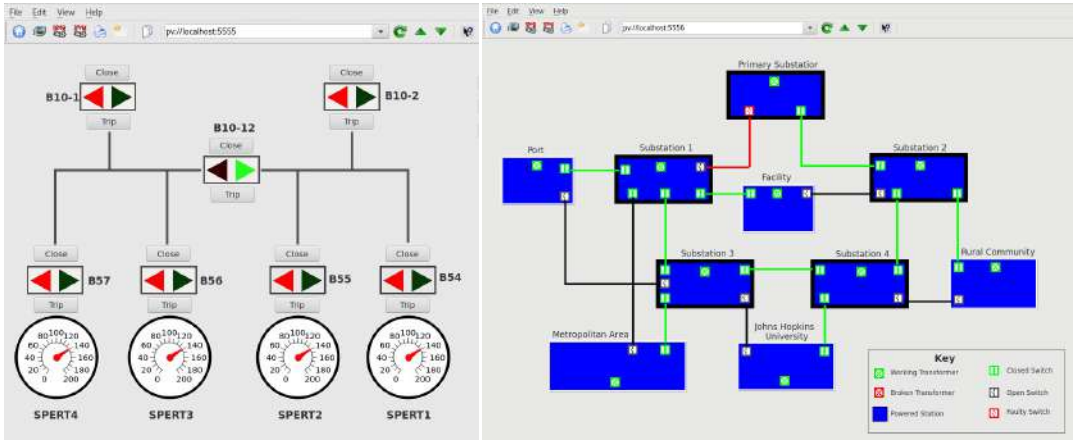
DoD ESTCP Red Team Experiment

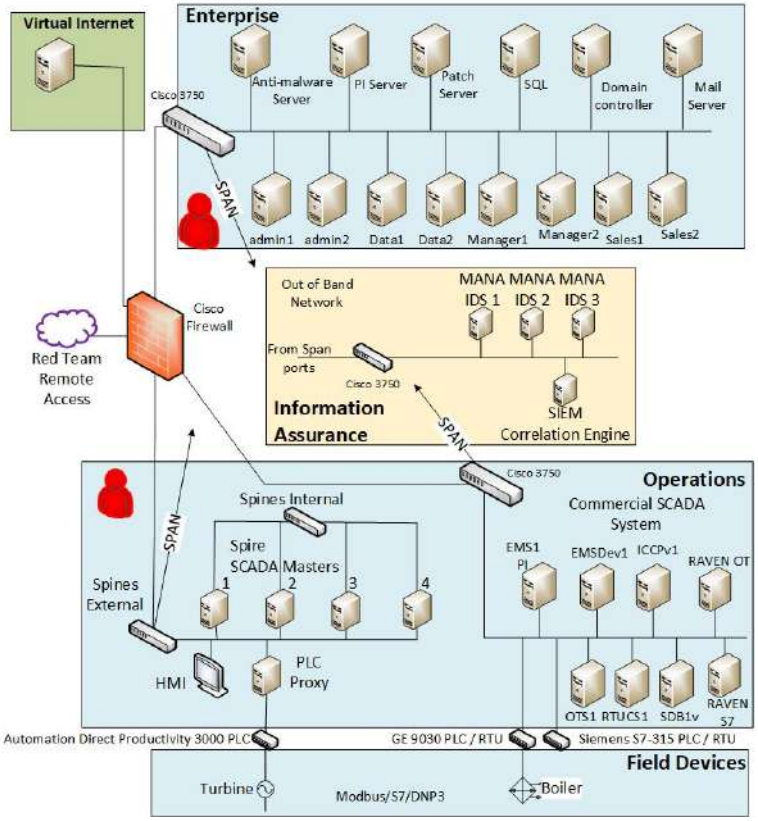
- Conducted at Pacific Northwest National Lab (PNNL)
- Power plant network set up with input from Hawaiian Electric Company
- Parallel operations networks
  - » NIST-compliant commercial SCADA system
  - » The Spire system
- Machine-learning-based intrusion detection system for situational awareness
  - » Unsupervised learning with packet analysis and traffic pattern analysis-based models
  - » Monitoring both enterprise and operations networks
- Commercial system and Spire each attacked by Sandia National Labs red team



SCADA System Setup for the Experiment

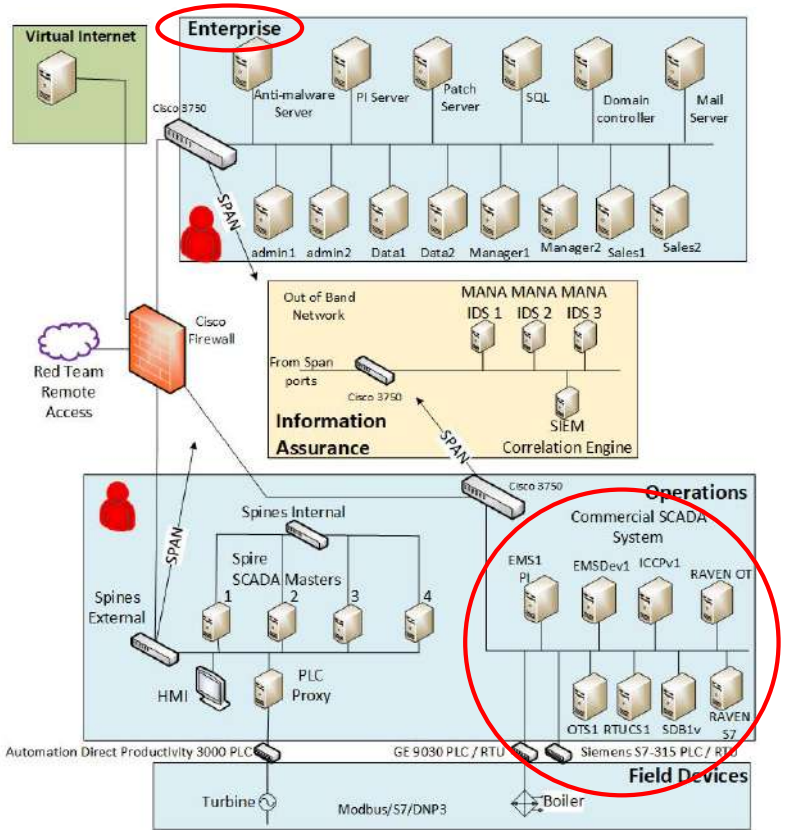
- Conducted at Pacific Northwest National Lab (PNNL)
- Power plant network set up with input from Hawaiian Electric Company





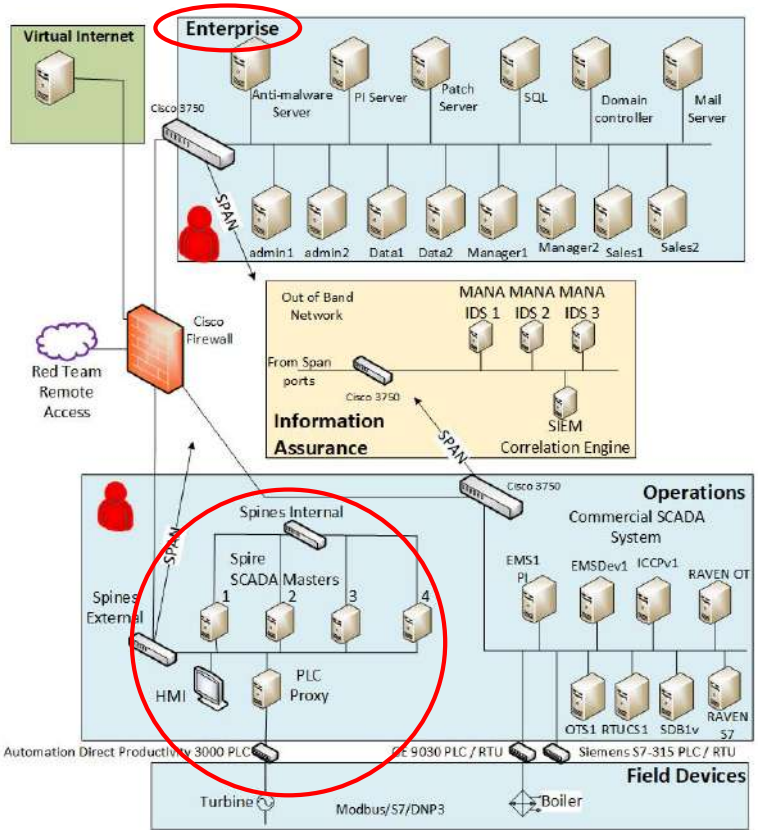
Commercial Systems Attacks

- Red team started from Enterprise network
  - » Goal: Establish baseline
  - » Surprising result:
    - Got access to operations network
    - Established direct control over PLC
    - Damage to PLC requiring firmware reinstall
- Red team given access to Operations network
  - » In addition to what they could do before …
    - Disrupted and modified SCADA Master to HMI communication
    - In effect, got full control over the system while at the same time controlled the view of the operator



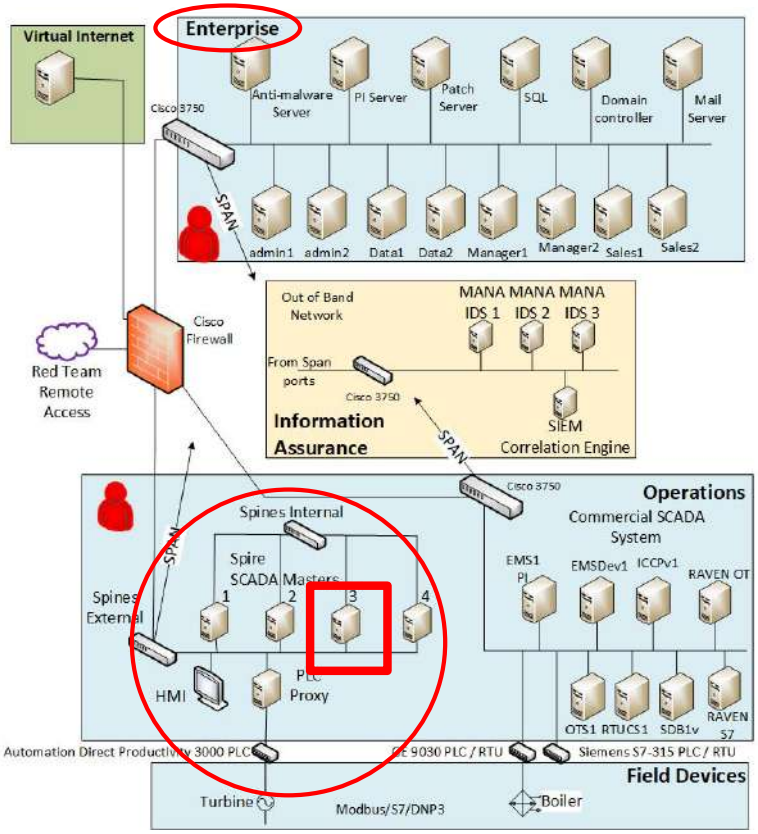
Spire System Attacks

- Red team started from Enterprise network
  - » Goal: Establish baseline
  - » As expected, no visibility from Enterprise network
    - Red team gave up after a couple of hours
- Red team given access to Operations network
  - » Two full days of attacks
    - No effect on system operation
    - No ability to penetrate in the allotted time
- All attacks were detected by the machine-learning-based intrusion detection system
  - » However, there were too many false positives to be useful
  - » This was later fixed for the test deployment at Hawaiian Electric



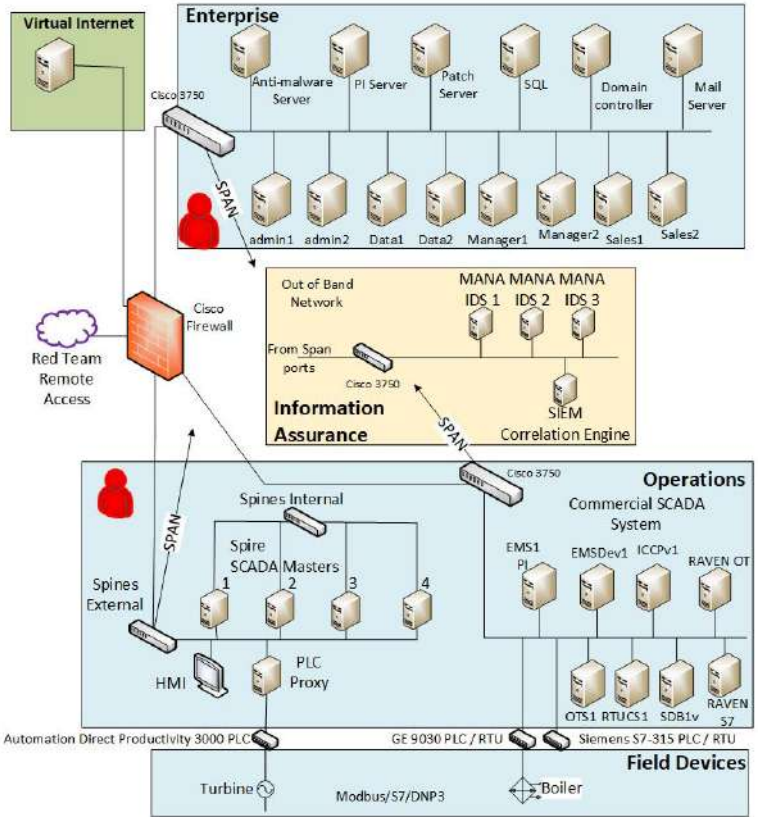
Spire System Excursion

- Testing Spire's ability to work in the face of compromises
- Red team was given access to one replica
- User-level access + cryptographic key
  - » Stopped system components, launched modified version of system components
  - » Tried to escalate privilege
  - » Patched the intrusion-tolerant network on that replica
- Root access + source code
  - » Focused on the intrusion-tolerant network
  - » Ran modified versions trying to attack its fairness
- No effect on system operation



DoD ESTCP Red Team Takeaways

- Today's power grid is vulnerable
  - » A nation-state hacker team from SANDIA National Labs remotely took down a grid setup according to best practices within a couple of hours
  - » Don't ask me how they penetrated the operations network – I have no idea
  - » I do understand how they did what they did once they penetrated that network
- There is a meaningful difference between current best practices and an intrusion-tolerant approach
  - » Spire's intrusion-tolerant network protected the system during the first two days
  - » Spire's intrusion-tolerant system architecture handled the compromise during the excursion

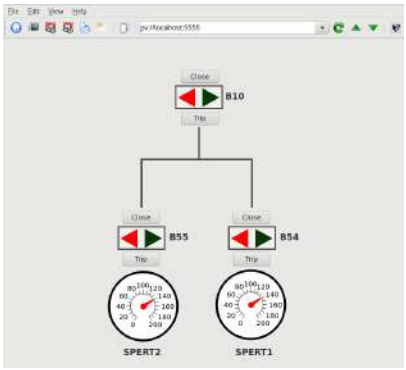


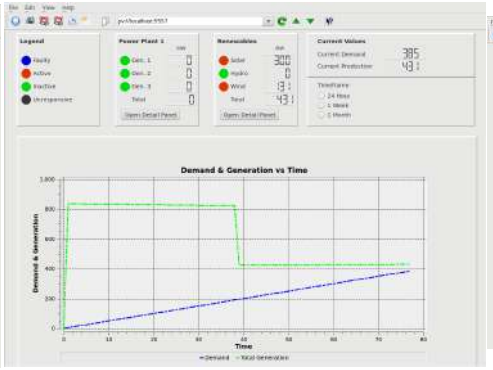
DoD ESTCP Power Plant Test Deployment

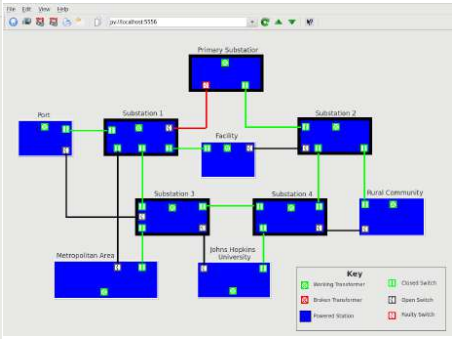
- Conducted at Hawaiian Electric Company (HECO)
  - » “Mothballed” Honolulu plant
- Deployment Goals
  - » Verify that Spire operates correctly in a real environment without adverse effect on other control-center systems
  - » Verify that Spire meets performance requirements
- Spire was installed in the Distributed Control System (DCS) room
  - » Managed a small power topology, controlling 3 physical breakers via a Modbus PLC
  - » Spire HMIs placed in 3 locations throughout the plant: the DCS room, the control room, and a demonstration room

DoD ESTCP Power Plant Test Deployment

- Results:
  - » Spire ran continuously for 6 days without adverse effects on other plant systems
  - » Timing experiment measuring Spire's HMI reaction time showed it met end-to-end latency requirements







DoE Grid Modernization Lab Call (GMLC) Project (2020-2023)

Pacific Northwest National Lab (PNNL), Johns Hopkins University

SANDIA National Labs, GE, Siemens, Hitachi Energy

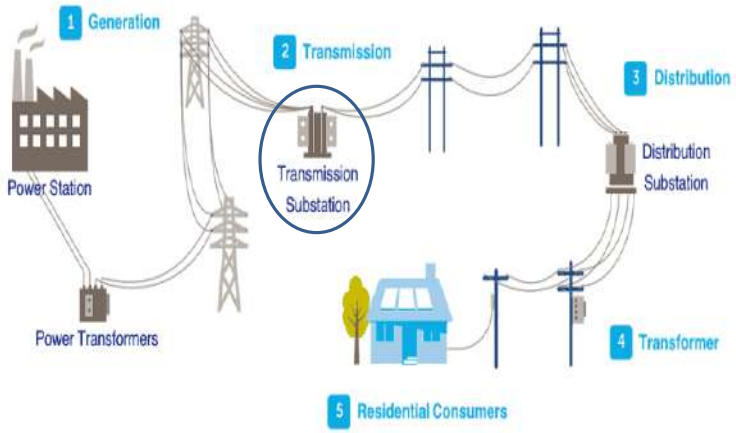
Western Area Power Administration (WAPA)

In light of the DoD ESTCP project results:

- What is the most vulnerable part of the grid we should protect with this approach?
  - High-voltage protective relays protecting high-voltage transformers in substations
- What is the most demanding requirement? Can Spire meet it?
  - In case of detecting a power surge, the high-voltage protective replay has to trip (disconnect) the power within a quarter of a cycle (about 4 milliseconds) to protect the transformer
  - This has to work even in the face of a successful attack and compromise

Intrusion-Tolerance for Power-Grid Substations

- High-voltage transformers
  - » Cost millions of dollars
  - » Have long procurement process (over a year!)
  - » Damaging a few of them can have a large impact on the grid for a long period of time
- High-Voltage protective relays may be vulnerable to cyberattacks
  - » A protective relay that does not trip when it should, can cause irreparable damage to the transformer and its connected customers
  - » A protective relay that does unnecessarily trip, causes a major disruption to a large number of customers



Picture: https://www.electricaltechnology.org/2021/10/electric-power-distribution-network.html

Picture by

Physical Attacks on Substations in Ukraine

Ukrenergo workers at a substation in eastern Ukraine are salvaging pieces of equipment that still can be used for repairs.

source: https://www.newyorker.com/culture/photo-booth/the-impact-of-russian-missile-strikes-on-ukraines-power-grid

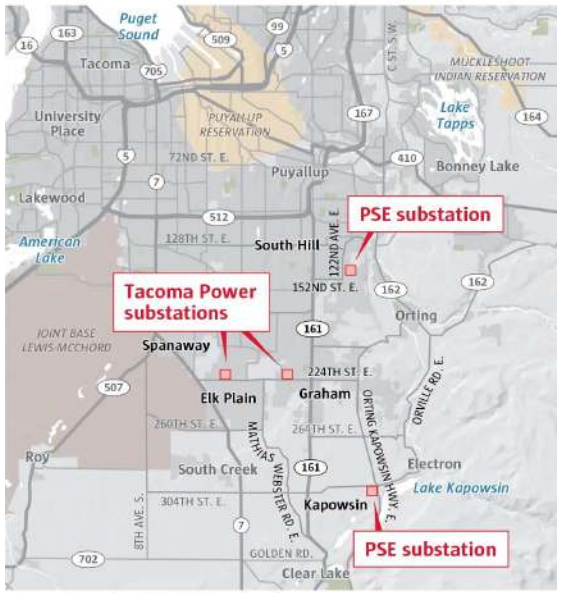
"Russia is systematically shelling electrical substations throughout Ukraine."

source: https://texty.org.ua/articles/108414/whats-up-with-the-power-how-russia-destroys-energy-infrastructure/

Physical Attacks on Substations in the US

Pierce County Christmas Day substation attacks

The first of four attacks was estimated to have happened in the early morning and the last in the evening on Christmas Day.



Source: Pierce County Sheriff's Department FIONA MARTIN / THE SEATTLE TIMES

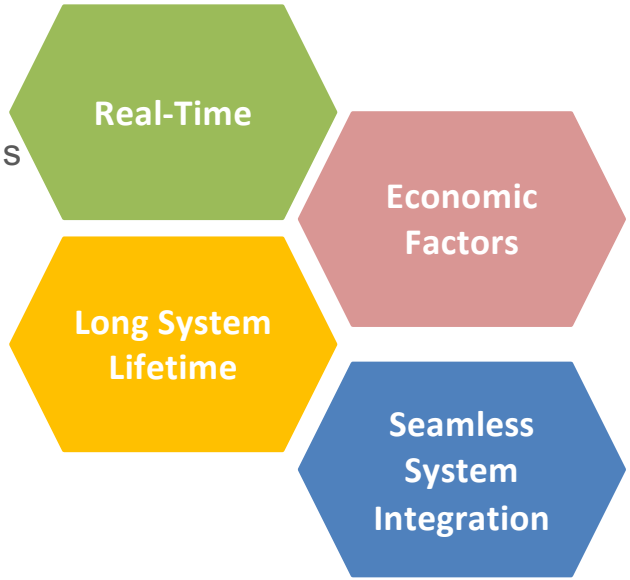
"Attacks on Electrical Substations Raise Alarm."

Sources:
https://www.nytimes.com/2023/02/04/us/electrical-substation-attacks-nc-wa.html
https://www.seattletimes.com/seattle-news/what-motivated-the-pacific-northwest-substation-attacks/
https://myfox8.com/news/investigations/power-grid-attack/2-months-since-moore-county/

Intrusion-tolerant Protective Relay for the Substation

Design Considerations

Very exact real-time latency requirement of quarter-power cycle in all operating conditions



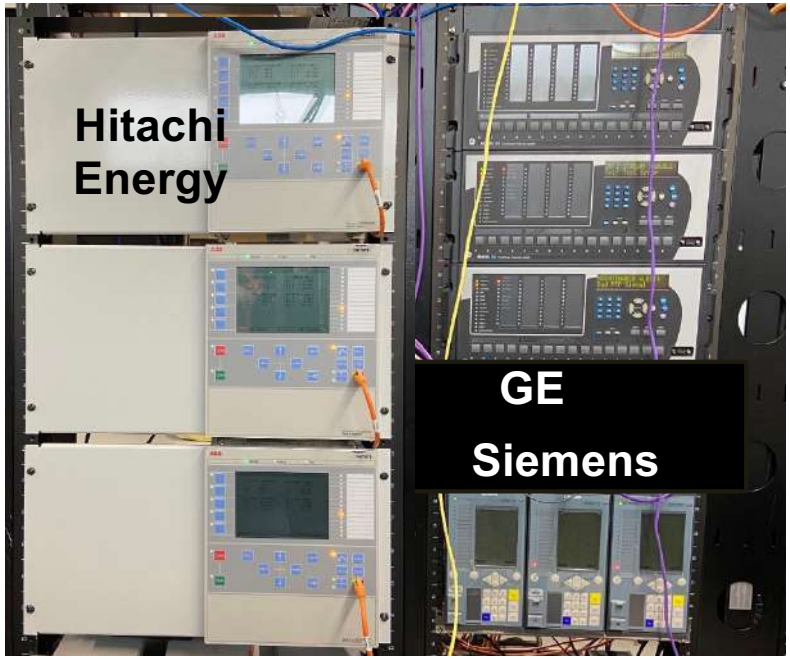
The protective relay is a reasonably expensive device and there are many of them in the system

Resilience with continuous availability and long system lifetime

The solution should be capable of integrating into existing substations without changes to the infrastructure

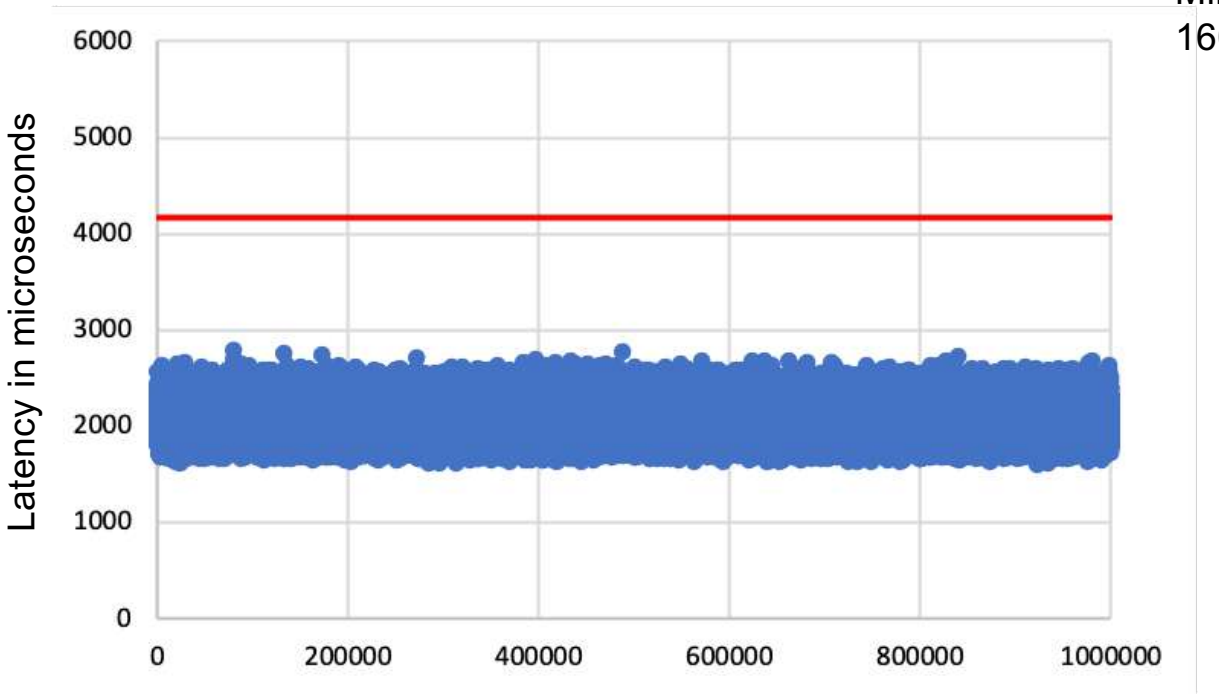
Spire for the Substation

- The first intrusion-tolerant real-time architecture and protocols for the substation
  - » Simultaneously addresses protective relay compromises and network attacks
  - » Meeting the strict latency requirement while under a successful attack (4.167 milliseconds)
- Successful red team experiment in 2022
  - » Sandia National Labs @ Pacific Northwest National Lab
  - » 192 attack scenarios over several months
  - » A single minor issue discovered and fixed
- Industry transitions
  - » GE transition in late 2022
  - » Siemens transition in 2023
- Johns Hopkins open-source release, February 2024



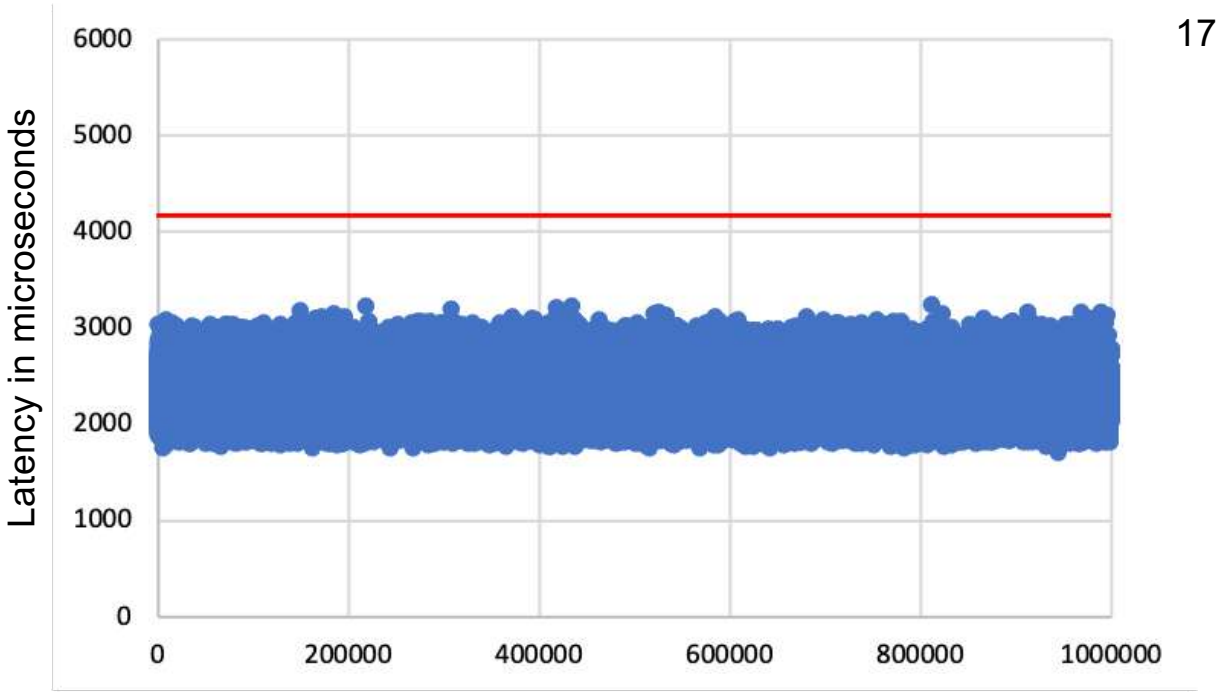
https://jhu-dsn.github.io/spire/

Performance Evaluation: Fault-free Operation



Minimum / Average / Maximum
1604 / 2048 / 2789 microseconds

Performance Evaluation: Operation during a Compromise



Minimum / Average / Maximum
1716 / 2268 / 3253 microseconds

Beyond Current Best Practices?

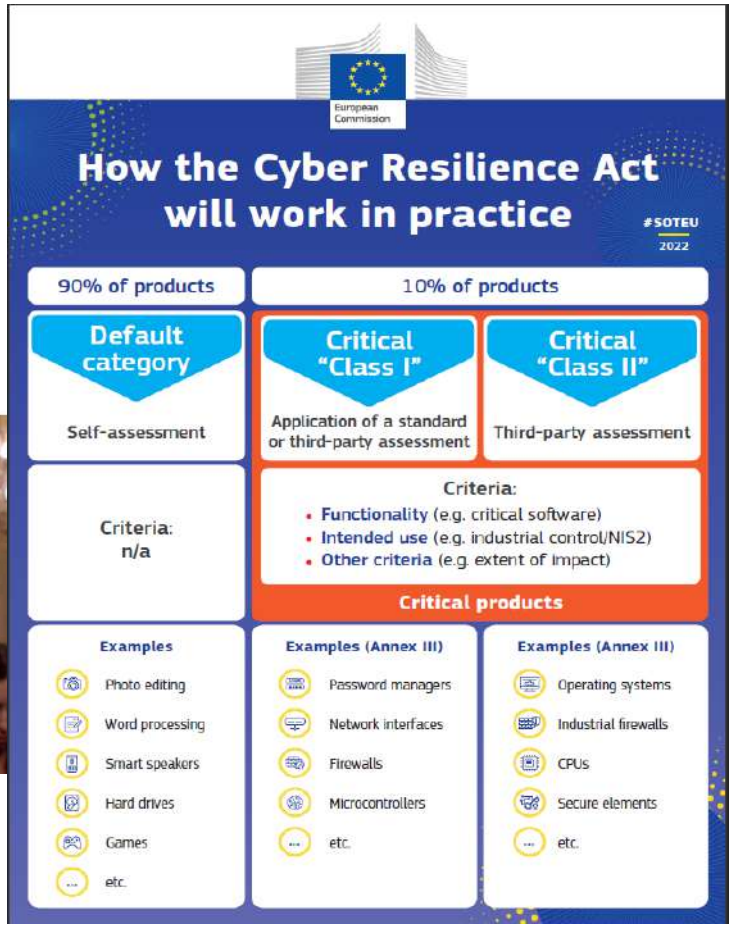
- Two kinds of industry
  - » Regulated – transmission and distribution
    - Is it required?
  - » Highly Competitive – generation
    - Who will pay for it?
- Uncertain benefit
  - » If we do not invest and nothing major happens – we win (status quo)
  - » If we do invest and nothing happens – how do we measure investment effectiveness / return on investment?
  - » If we do invest and are compromised anyway – double whammy ☺
- Who is responsible anyway?
  - » If a nation-state attacker takes down the grid, is it the utility's fault or the government responsibility?
    - Why do we pay taxes?
  - » Companies perceive it as their responsibility (**good**)
    - But not as urgent
- Perhaps a necessity?

Just recently …

FBI director warns that Chinese hackers are preparing to 'wreak havoc' on US critical infrastructure

By Hannah Rabinowitz and Sean Lyngaas, CNN
4 minute read · Updated 4:43 PM EST, Wed January 31, 2024

FBI Director Christopher Wray testified about infrastructure networks before the House China committee



Sources: https://www.cnn.com/2024/01/31/politics/china-hacking-infrascture-fbi-director-christopher-wray/index.html
https://blog.gitguardian.com/are-the-fears-about-the-eu-cyber-resilience-act-justified/
https://www.wsj.com/politics/national-security/u-s-disables-chinese-hacking-operation-that-targeted-critical-infrastructure-184bb407

Beyond Current Best Practices

- We need your help!
- We do what we can
  - » Invent the algorithms, develop the system, red-team it, test-deploy it in a utility, transition it to the manufacturers
- But
  - » The regulator does not ask for such capabilities
    - Do they know there are solutions?
  - » Siemens and GE report that their customers are not asking for such capabilities
    - Without that they will not invest in taking a solution to market
- A step-by-step approach is possible
  - » First step: incorporate the intrusion-tolerant network to secure communication and protect against network-level attacks
    - Without changing existing systems - think of this as deploying a sophisticated VPN
  - » Second step: incorporate the full solution to protect against system-level compromises
- We can use all the help we can get – if you have any idea or comment, or would like to help, please reach out!

Credit

- Johns Hopkins University
  - Sahiti Bommareddy, Dr. Amy Babay, Dr. Thomas Tantillo, Trevor Aron, Samuel Beckley, Dr. Jonathan Kirsch
- Spread Concepts LLC
  - John Schultz, Dr. Jonathan Stanton
- Resurgo LLC
  - Kevin Jordan, Eamon Jordan, Kevin Ruddell
- Pacific Northwest National Lab
  - Paul Skare, Christopher Bonebrake, David J Sebastian Cardenas, Carl Miller
- Sandia National Labs
  - Adrian Chaves, Candy Phan
- Hawaiian Electric Company
  - Keith Webster, Bryan Tepper
- Siemens
  - Dr. Stuart Goose, Muhammad Ashif, Dr. Jagannadh Vempati
- GE
  - Paul Caffrey, John Garrity, John Carbone