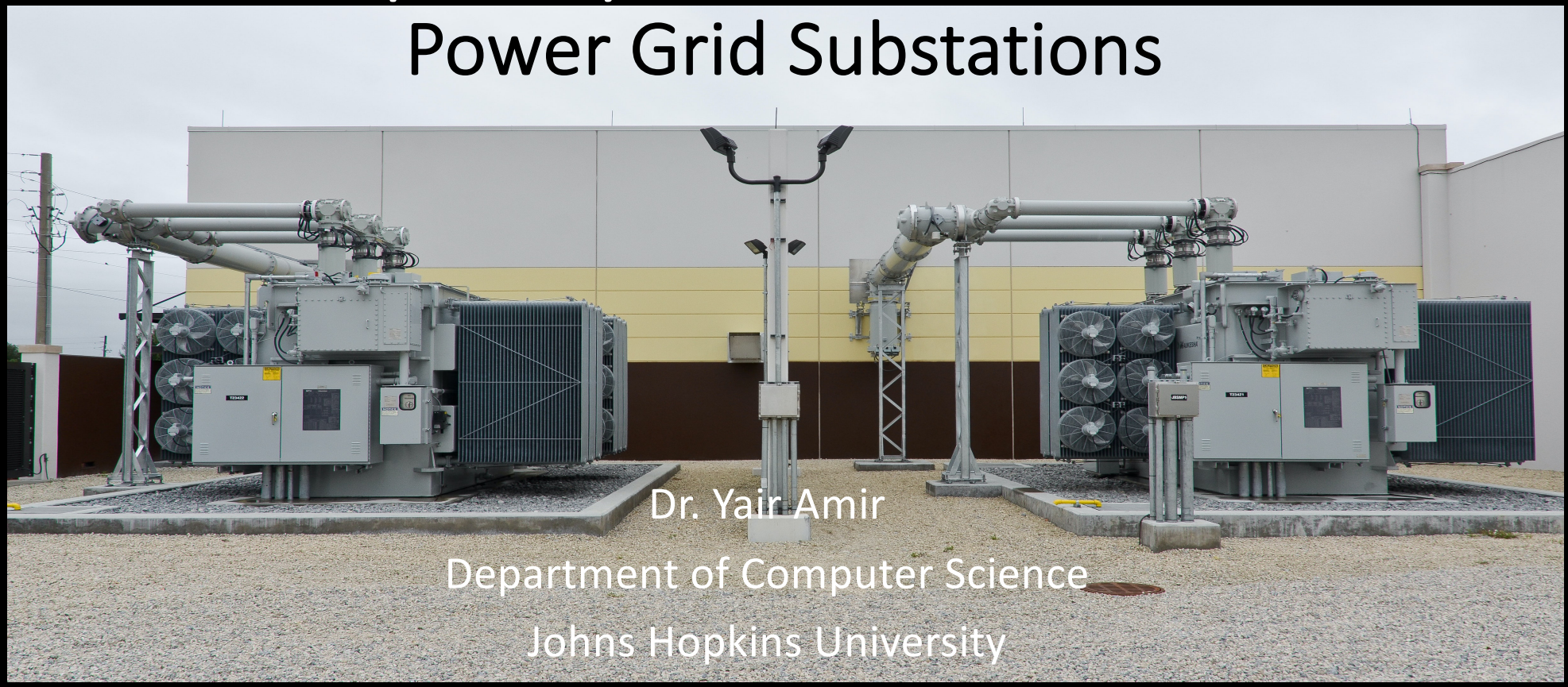
Spire: Cyberattack-resilient Power Grid Substations



Dr. Yair Amir

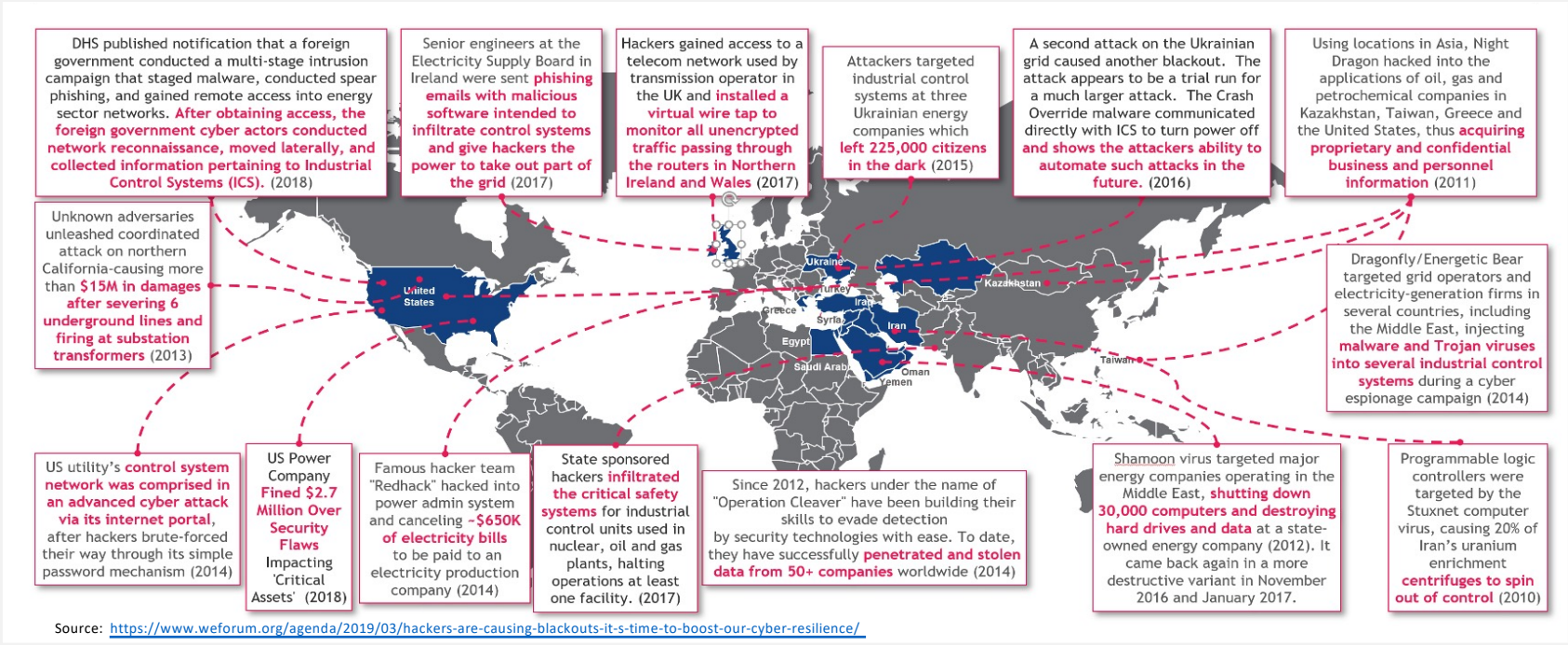
Department of Computer Science

Johns Hopkins University

yairamir@jhu.edu

Picture by

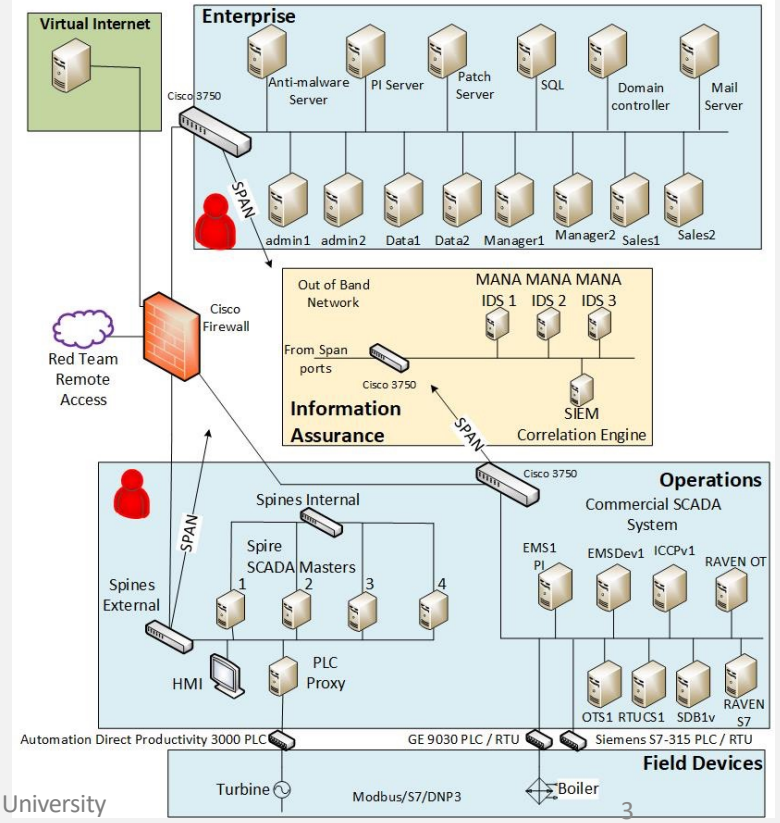
Increasing Cyber Attacks on Grid Control Systems Reinforce the Need for Intrusion-tolerant Systems…



Source: https://www.weforum.org/agenda/2019/03/hackers-are-causing-blackouts-it-s-time-to-boost-our-cyber-resilience/

DoD Red Team Experiment (March – April 2017)

- Hosted at Pacific Northwest National Lab
- Sandia National Labs red team attacked NIST-compliant commercial SCADA architecture and Spire
- Commercial system completely taken over
  - MITM from enterprise network, direct PLC access within hours
- Spire completely unaffected
  - Even after providing access to replica + source code



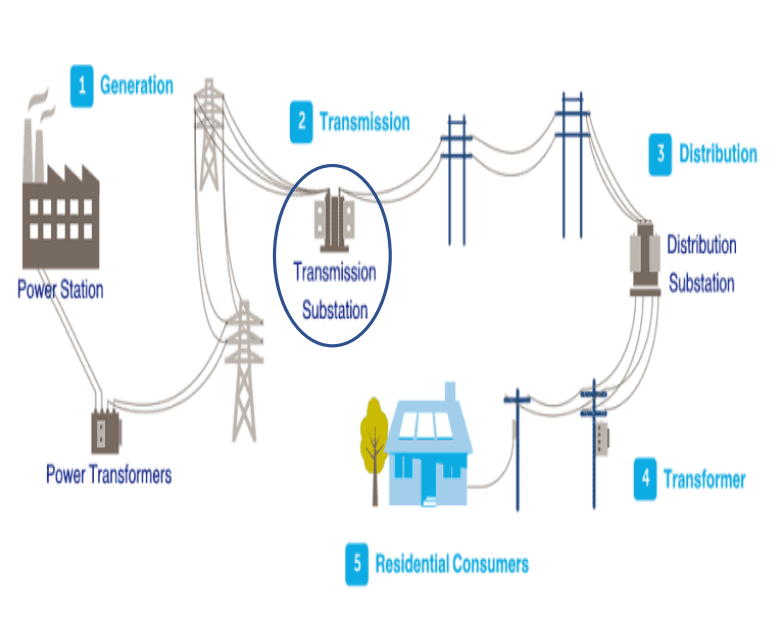
Hawaiian Electric Test Deployment (January – February 2018)

- Spire test deployment at Hawaiian Electric
  - "Mothballed" Honolulu plant
  - Managed small power topology, controlling 3 physical breakers via a Modbus PLC
- Outcome
  - Operated continuously in a real environment for 6 days without interfering with plant systems
  - Successfully met performance (latency) requirements

Babay, Amy, John Schultz, Thomas Tantillo, Samuel Beckley, Eamon Jordan, Kevin Ruddell, Kevin Jordan, and Yair Amir. "Deploying intrusion-tolerant SCADA for the power grid." In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 328-335, 2019.

Byzantine-resilient High-Voltage Relays in the Substation (2020 — 2023)

- Department of Energy identified high-voltage transformers as the most vulnerable component of the grid
  - Cost millions of dollars
  - Long procurement process
  - Compromising a few can impact the grid
- High Voltage Protective Relays protect the transformers; Protective Relays may be vulnerable to cyberattacks
- Byzantine-resilience: resilient all the way to intrusion-tolerance -- working correctly even after a successful intrusion by a sophisticated adversary

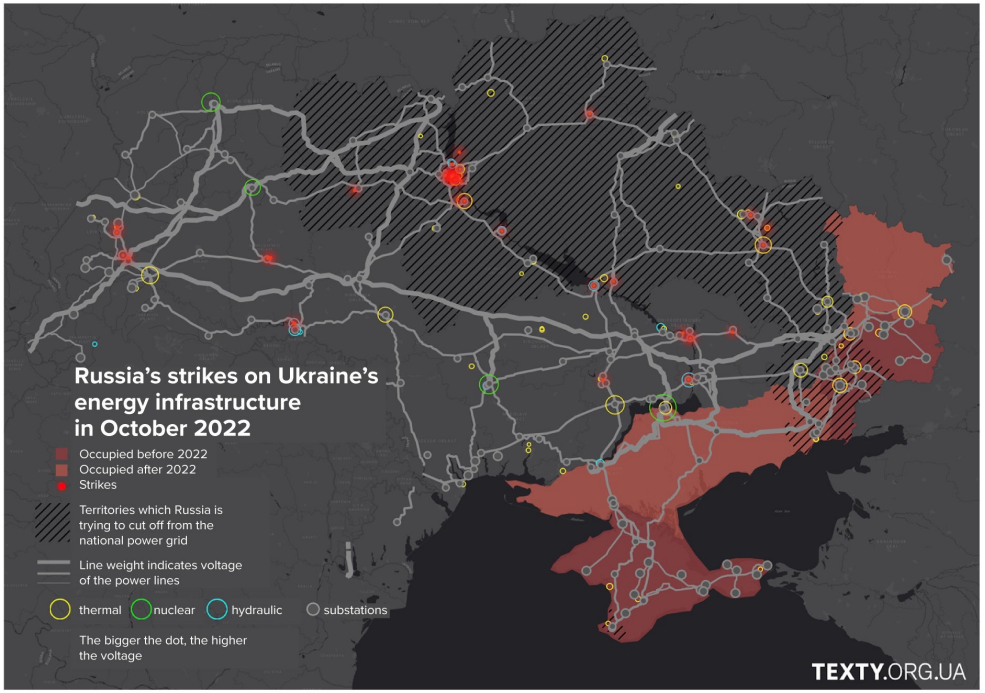


Source: https://www.electricaltechnology.org/2021/10/electric-power-distribution-network.html

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.

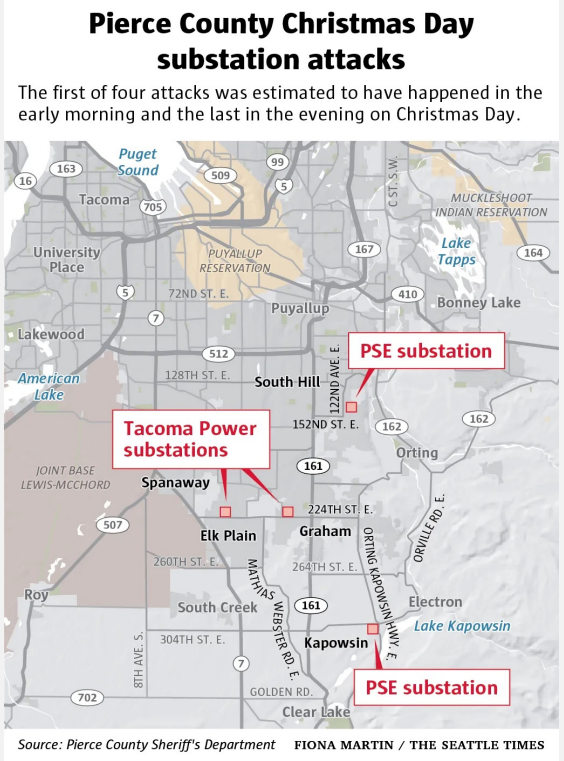
source: https://www.newyorker.com/culture/photo-booth/the-impact-of-russian-missile-strikes-on-ukraines-power-grid



"Russia is systematically shelling electrical substations throughout Ukraine."

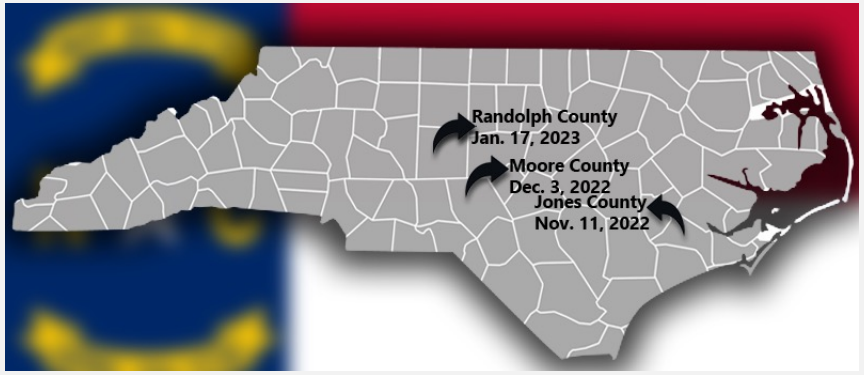
source: https://texty.org.ua/articles/108414/whats-up-with-the-power-how-russia-destroys-energy-infrastructure/

Physical Attacks on Substations in the US



"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/



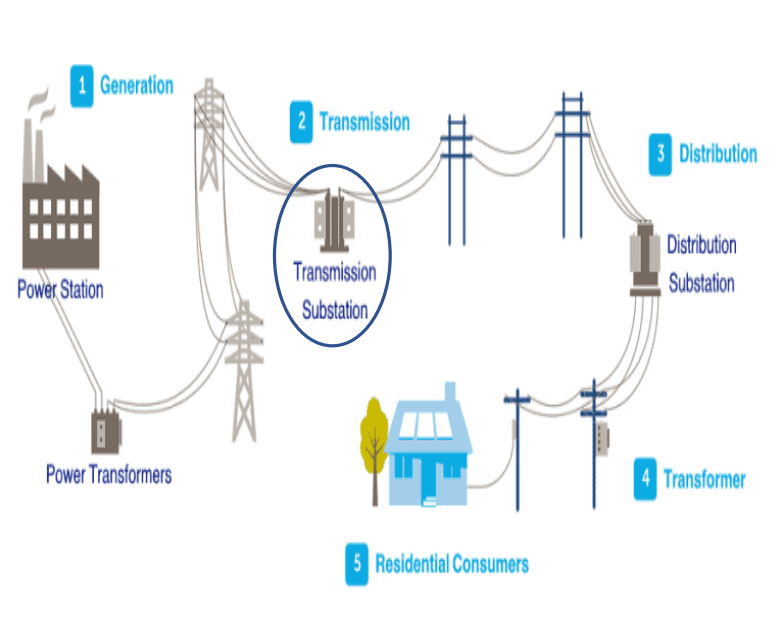
Byzantine-resilient High-Voltage Relays in the Substation (2020 — 2023)

The Cyberattack angle

- 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

DoE project addressing that angle

- Collaboration between Pacific Northwest National Laboratory (PNNL), Sandia National Laboratories (SNL), and Johns Hopkins
- Industry partners: GE, Siemens, and Hitachi Energy

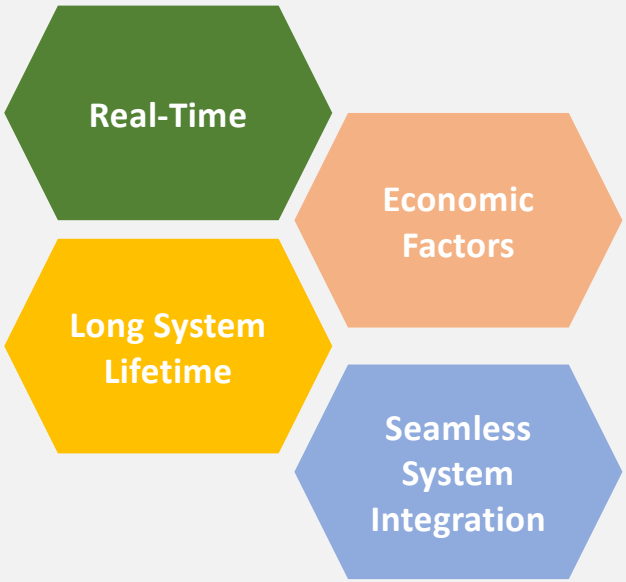


Source: https://www.electricaltechnology.org/2021/10/electric-power-distribution-network.html

Designing Byzantine-resilient Protection

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

Resiliency with long system lifetime with continuous availability

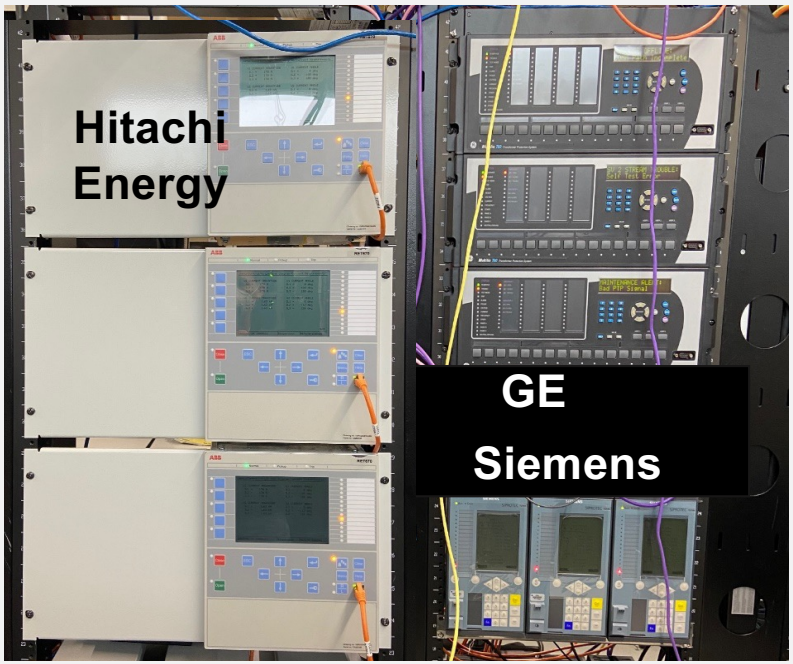


The protective relay is a reasonably expensive device and there are many of them in the system

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

Spire for the Substation

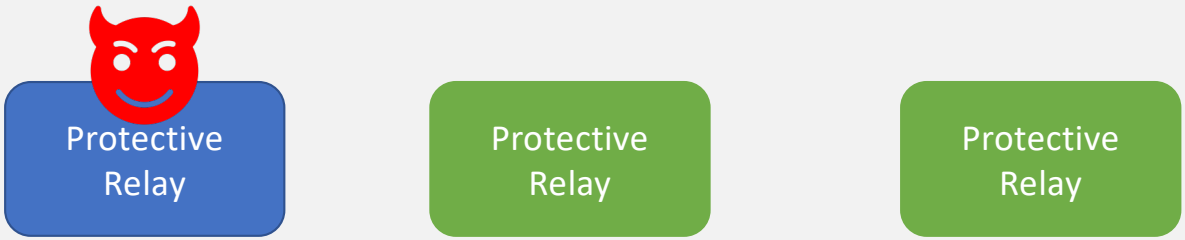
The **first real-time Byzantine-resilient architecture and protocols for the substation** that simultaneously address system compromises and network attacks while meeting the strict timeliness requirement (4.167ms)



Bommareddy, Sahiti, Daniel Qian, Christopher Bonebrake, Paul Skare, and Yair Amir. "Real-time byzantine resilience for power grid substations." In *2022 41st International Symposium on Reliable Distributed Systems (SRDS)*, pp. 213-224. IEEE, 2022.

Sahiti Bommareddy, Maher Khan, David J Sebastian Cardenas, Carl Miller, Christopher Bonebrake, Yair Amir and Amy Babay. "Real-Time Byzantine Resilient Power Grid Infrastructure: Evaluation and Trade-offs". In International Workshop on Explainability of Real-time Systems and their Analysis at the IEEE Real-Time Systems Symposium (RTSS 2022).

Toward a Byzantine-resilient Architecture



Malicious Relay
f=1

f+1 relays need to agree on an action
$f+1=2$

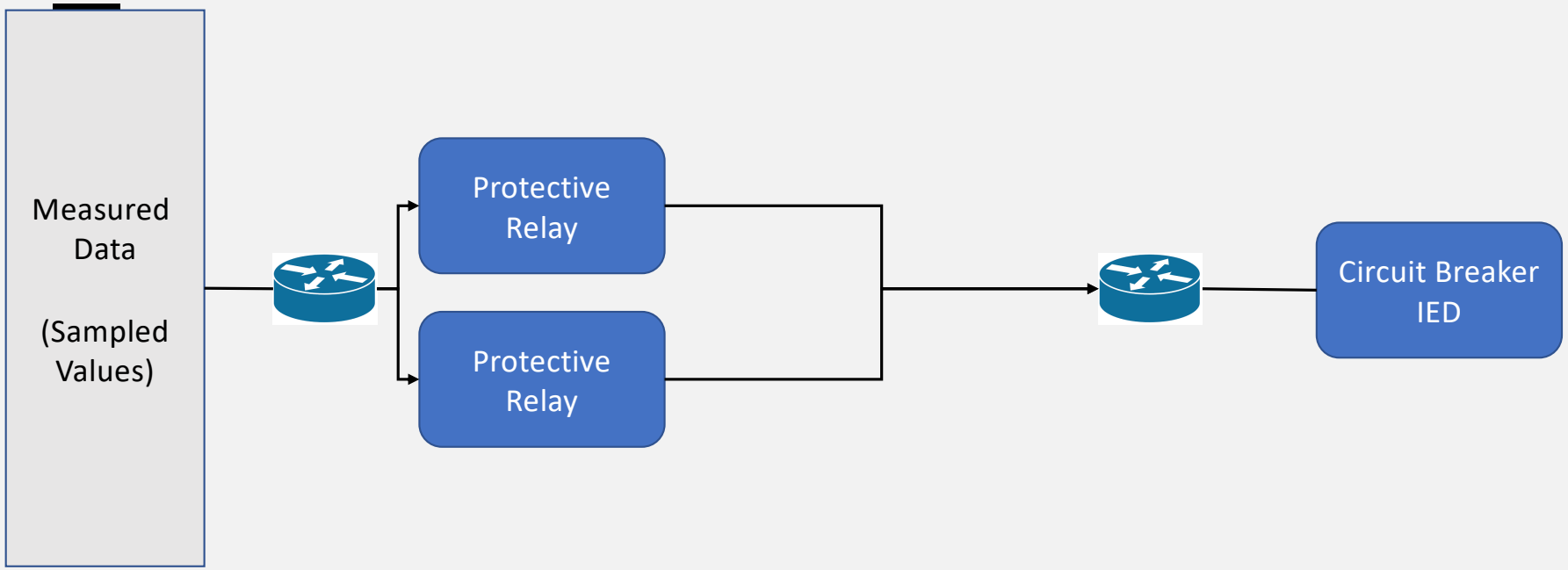
Toward a Byzantine-resilient Architecture

Malicious Relay
f=1

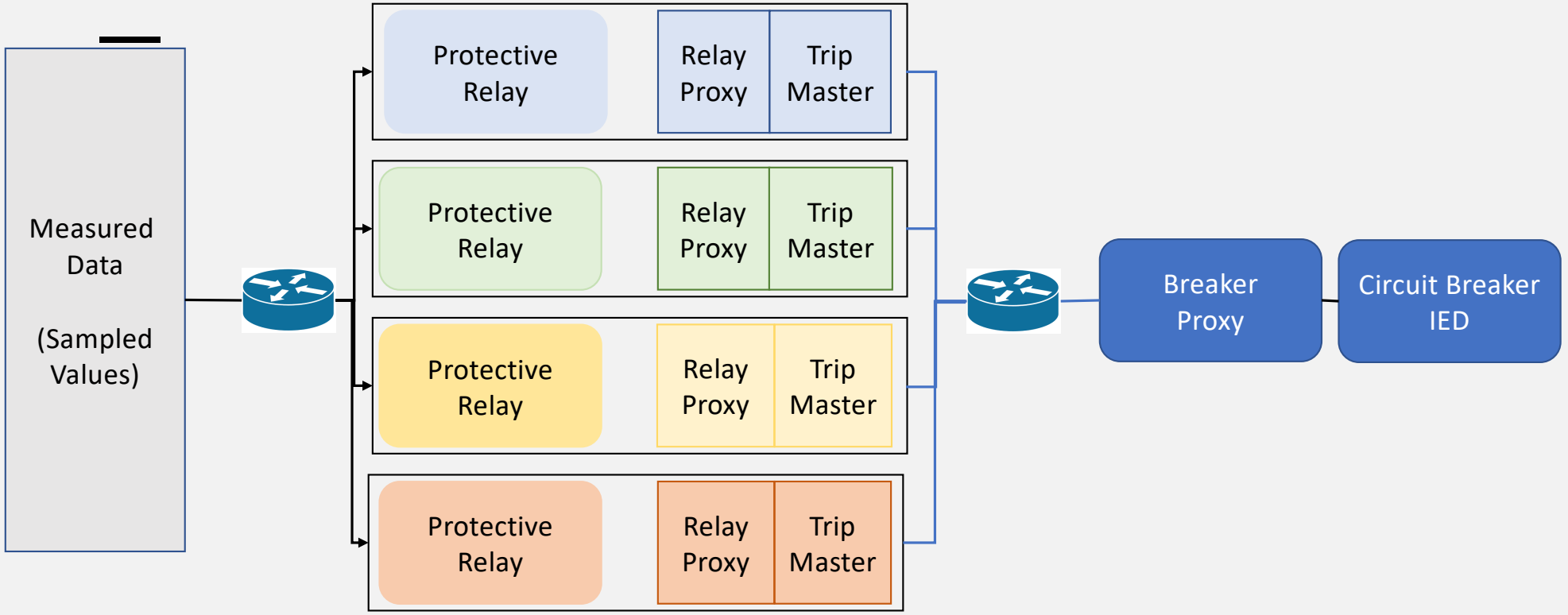
f+1 relays need to agree on an action
$f+1=2$

Relay for proactive recovery
k=1

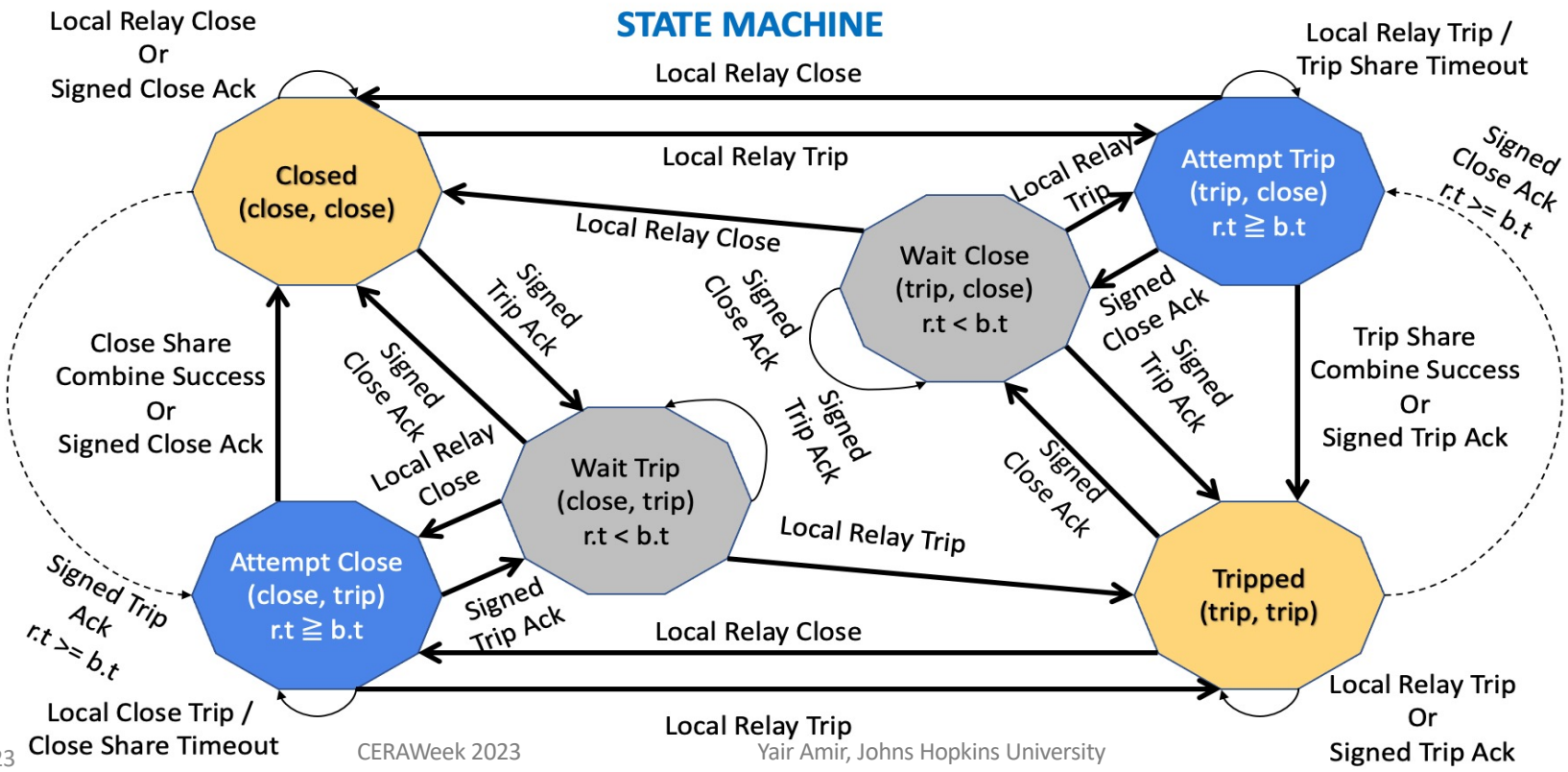
Typical IEC61850 Substation Architecture



Byzantine-resilient Substation Architecture



Protocol: State Machine

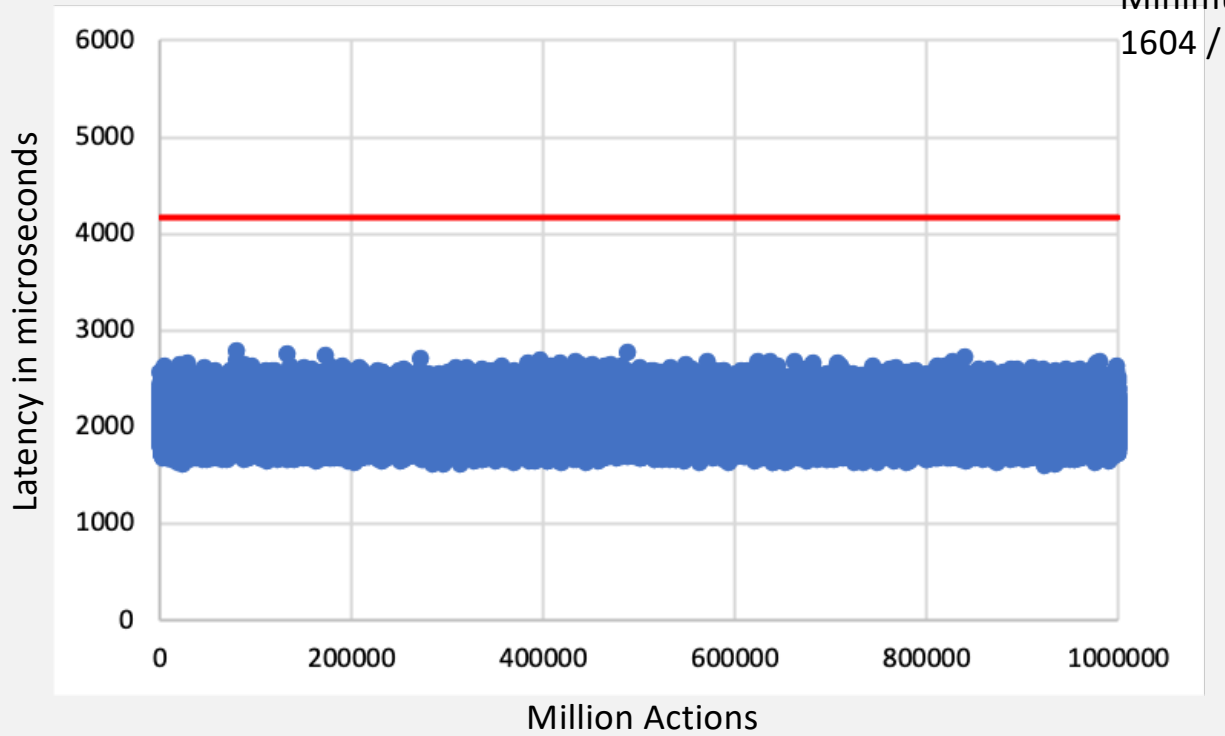


Evaluation Operating Conditions

Operation Condition	Explanation
Fault-Free (Normal)	All four relay nodes are working correctly
Fail-Stop Fault or Proactive Recovery	One of the relay nodes is unavailable due to a fail-stop fault or proactive recovery
Fail-Stop Fault and Proactive Recovery	One of the relay nodes is unavailable due to a fail-stop fault while simultaneously, an additional relay node is undergoing proactive recovery
Byzantine Fault	One of the relay nodes is under the control of a sophisticated attacker. Such compromised node performs two simultaneous attacks for each action : send corrupt share and short intermittent denial of service attacks
Byzantine Fault and Proactive Recovery	One of the relay nodes exhibits the Byzantine Fault condition described above, and simultaneously, an additional relay node is undergoing proactive recovery

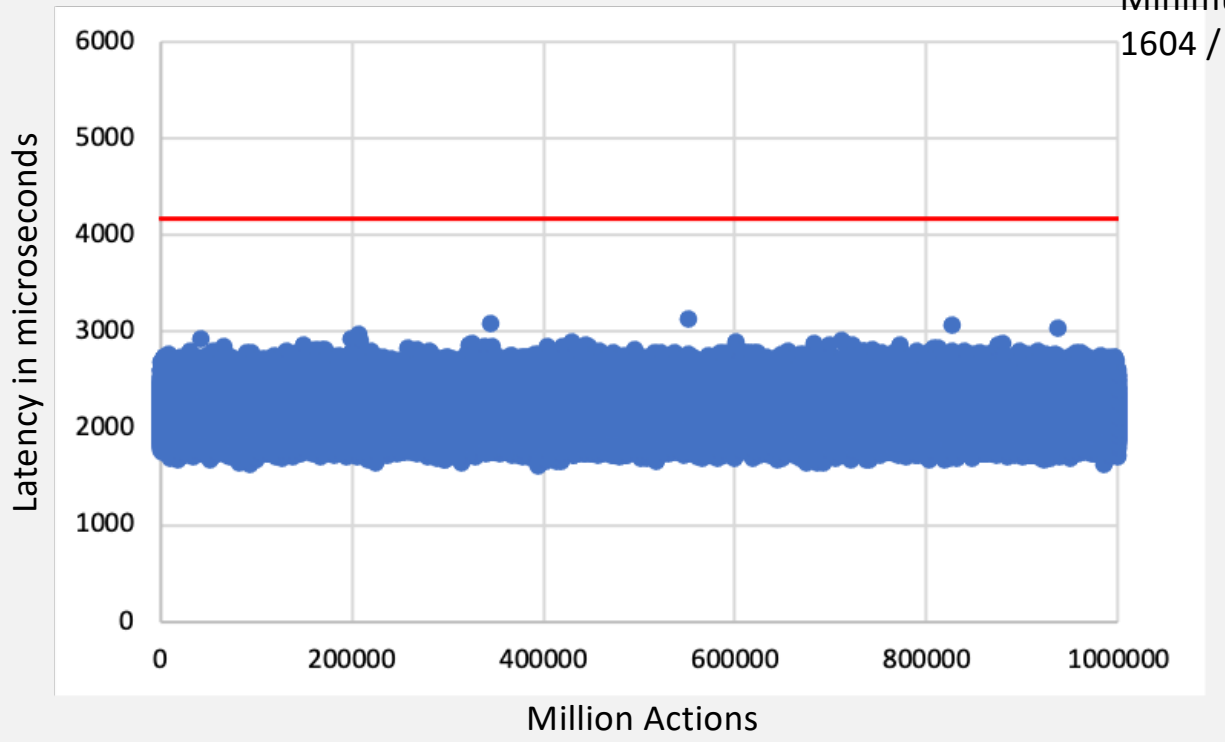
Performance Evaluation : Fault-free Operating Condition

Minimum / Average / Maximum
1604 / 2048 / 2789 microseconds



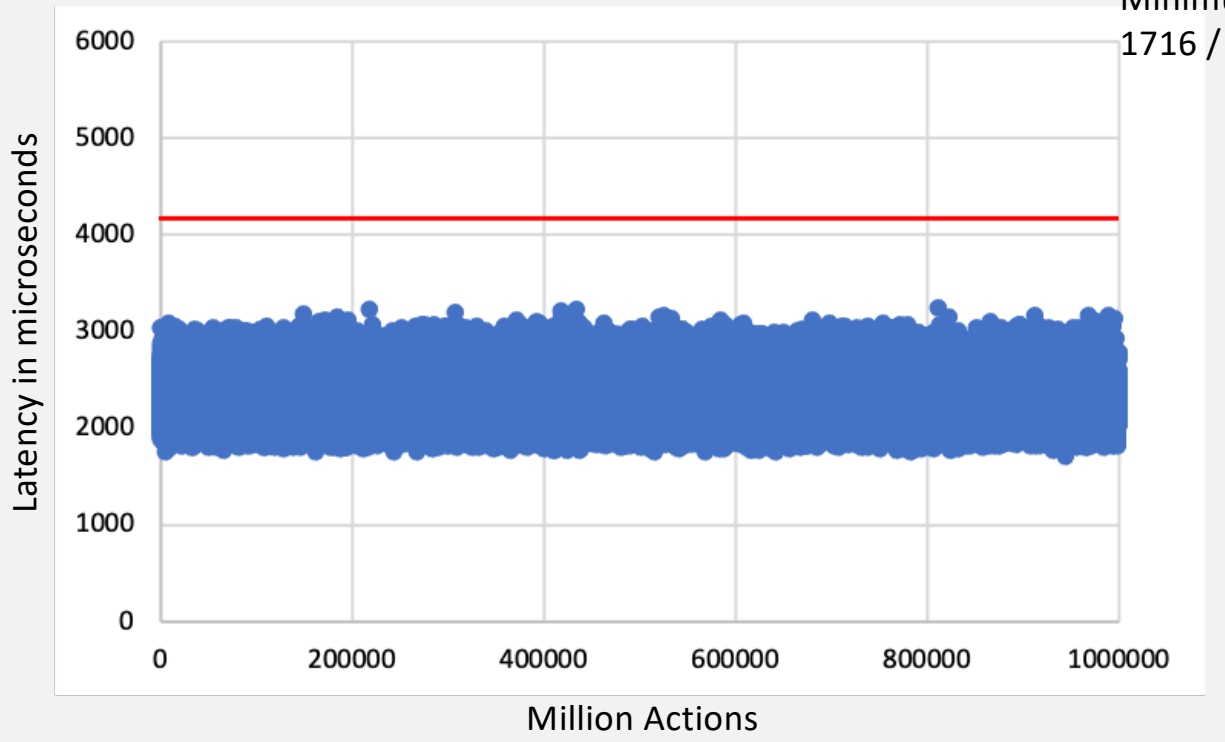
Performance Evaluation : Fail-Stop Fault or Proactive Recovery Operating Condition

Minimum / Average / Maximum
1604 / 2132 / 3135 microseconds



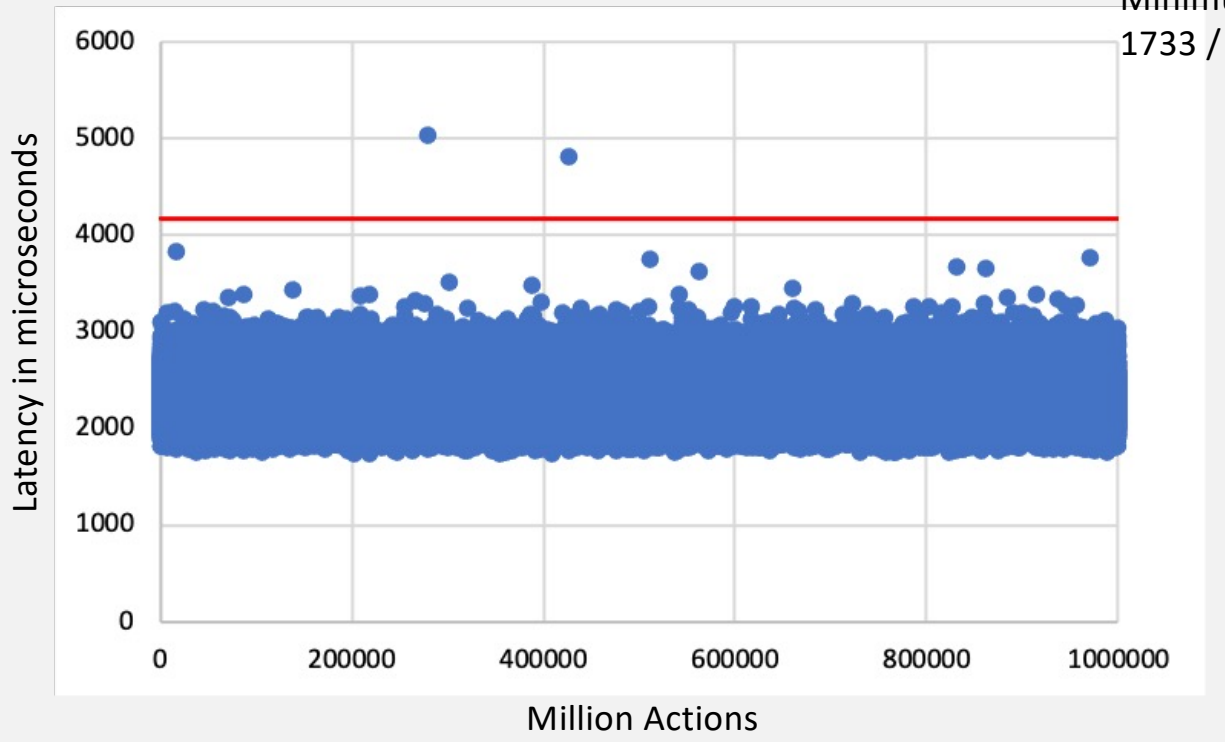
Performance Evaluation : Byzantine Fault Operating Condition

Minimum / Average / Maximum
1716 / 2268 / 3253 microseconds



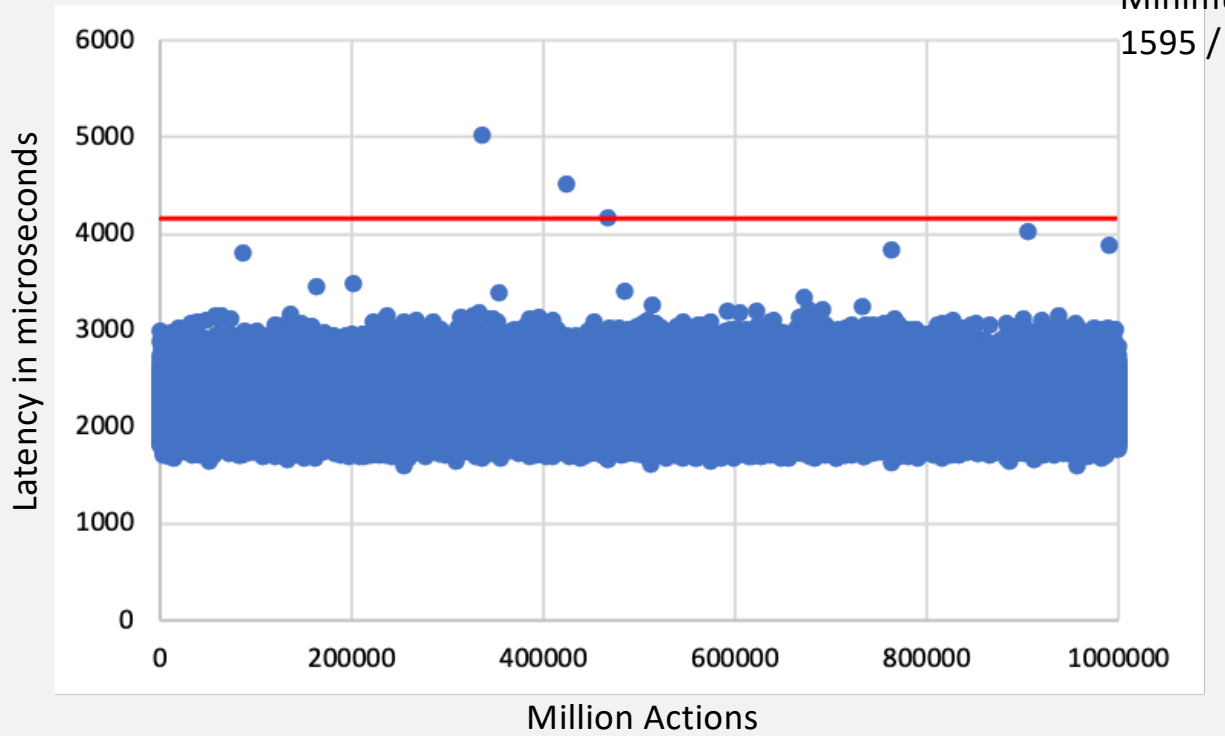
Performance Evaluation : Byzantine Fault and Proactive Recovery Operating Condition

Minimum / Average / Maximum
1733 / 2261 / 5028 microseconds



Performance Evaluation : Fail-Stop Fault and Proactive Recovery Operating Condition

Minimum / Average / Maximum
1595 / 2167 / 5025 microseconds



Real-Time Kernel Option

- With only two nodes available, a random delay on either node (e.g., from network delays, kernel scheduling, or even effects of a Byzantine node's actions) would be reflected in the end-to-end latency
- Real-time kernel is optimized to maintain low-latency consistent response time and determinism
- The determinism and latency stability of real-time kernel help to always meet the real-time requirement in all operating conditions

Sahiti Bommareddy, Maher Khan, David J Sebastian Cardenas, Carl Miller, Christopher Bonebrake, Yair Amir and Amy Babay.
"Real-Time Byzantine Resilient Power Grid Infrastructure: Evaluation and Trade-offs".
In International Workshop on Explainability of Real-time Systems and their Analysis at the IEEE Real-Time Systems Symposium (RTSS 2022).

Machine Learning-based Situational Awareness

- We use machine learning-based intrusion detection
  - Unsupervised Models
  - Bag of Models
  - Out-of-Band Detection
  - Two levels of Modules: Network-level and Power system-level
- Network level Module
  - Packet Analysis-based Models
  - Traffic Flow-based Models
- Power systems level module

Spire for the Substation

- The **first real-time Byzantine resilient architecture and protocols for the substation** that simultaneously address system compromises and network attacks while meeting the strict timeliness requirement (4.167ms)
- Successful red team experiment in 2022 (Sandia National Laboratories @ PNNL)
- Industry Transition (GE 12/2022, Siemens 1/2023, perhaps Hitachi Energy)
- Johns Hopkins open-source release: Spire 2.0 (www.dsn.jhu.edu/spire)

Bommareddy, Sahiti, Daniel Qian, Christopher Bonebrake, Paul Skare, and Yair Amir.
"Real-time byzantine resilience for power grid substations."
In *2022 41st International Symposium on Reliable Distributed Systems (SRDS)*, pp. 213-224. IEEE, 2022.

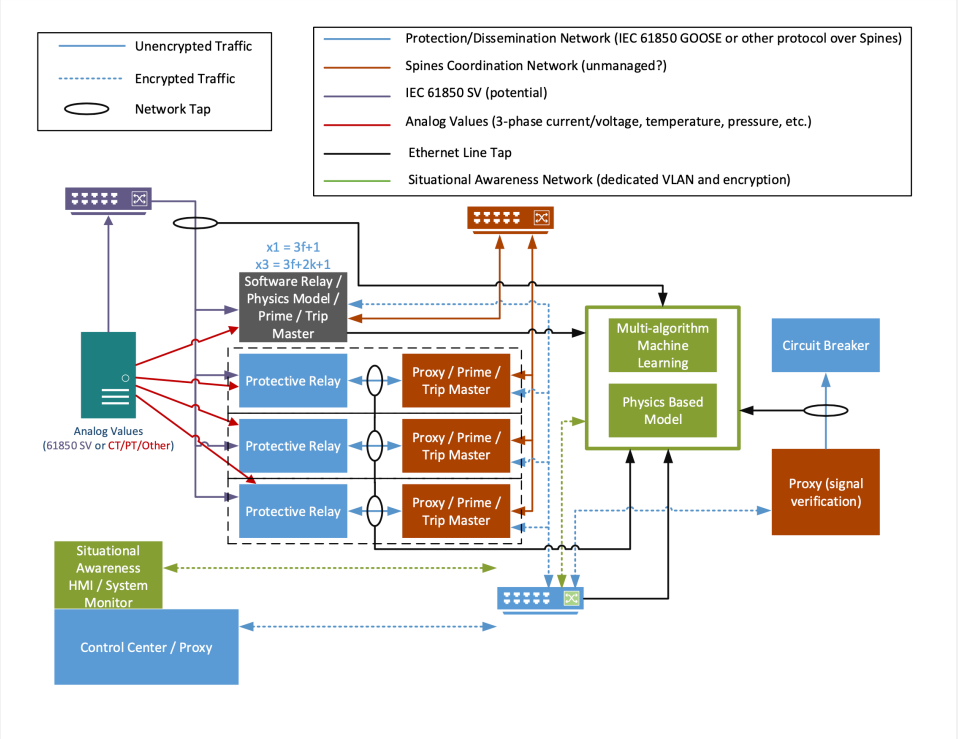
Sahiti Bommareddy, Maher Khan, David J Sebastian Cardenas, Carl Miller, Christopher Bonebrake, Yair Amir and Amy Babay.
"Real-Time Byzantine Resilient Power Grid Infrastructure: Evaluation and Trade-offs".
In International Workshop on Explainability of Real-time Systems and their Analysis at the IEEE Real-Time Systems Symposium (RTSS 2022).

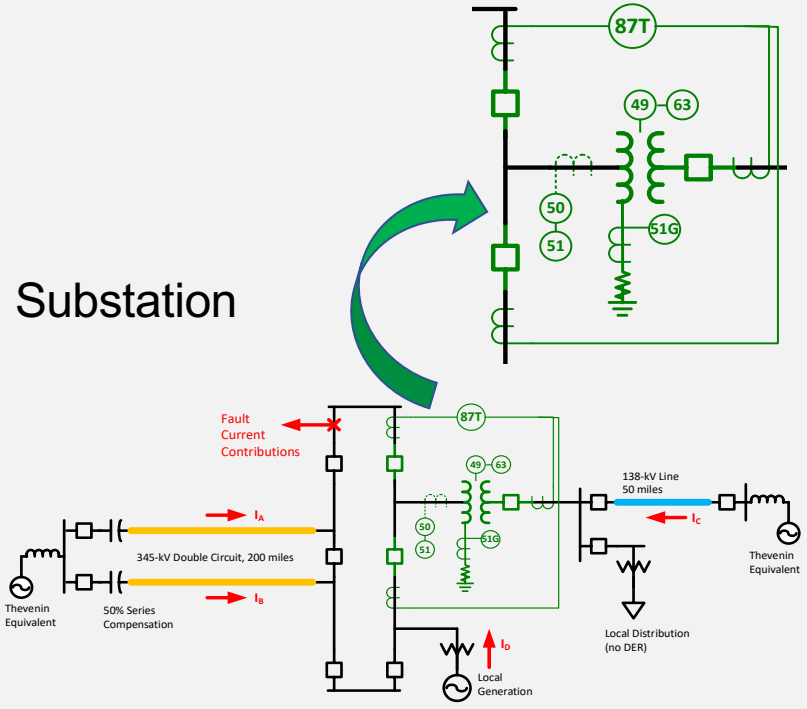
Questions / Comments

—

- www.dsn.jhu.edu/spire
- yairamir@jhu.edu

Backup Slide 1





Backup Slide 2

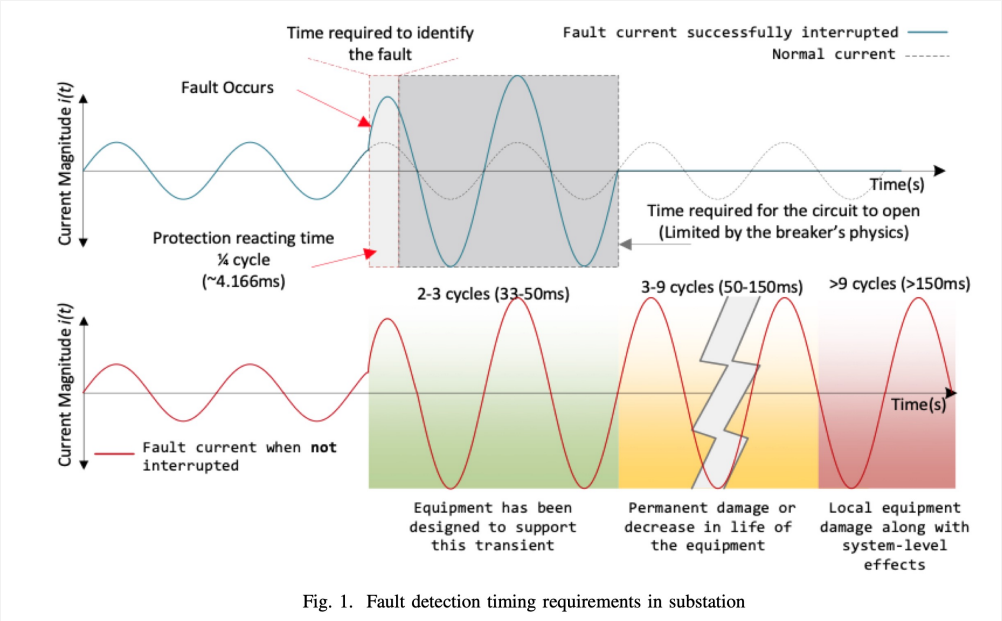


Fig. 1. Fault detection timing requirements in substation

STATE MACHINE