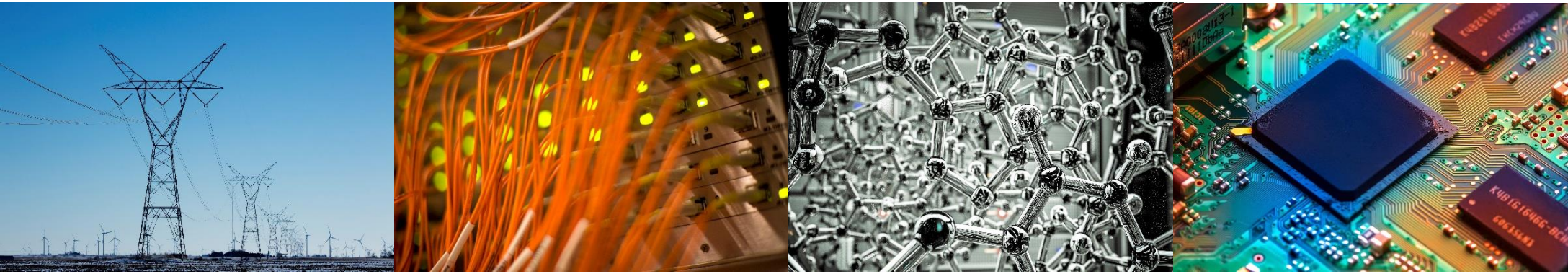
Evaluating the Risk of Ransomware in Energy Systems

Megan Culler

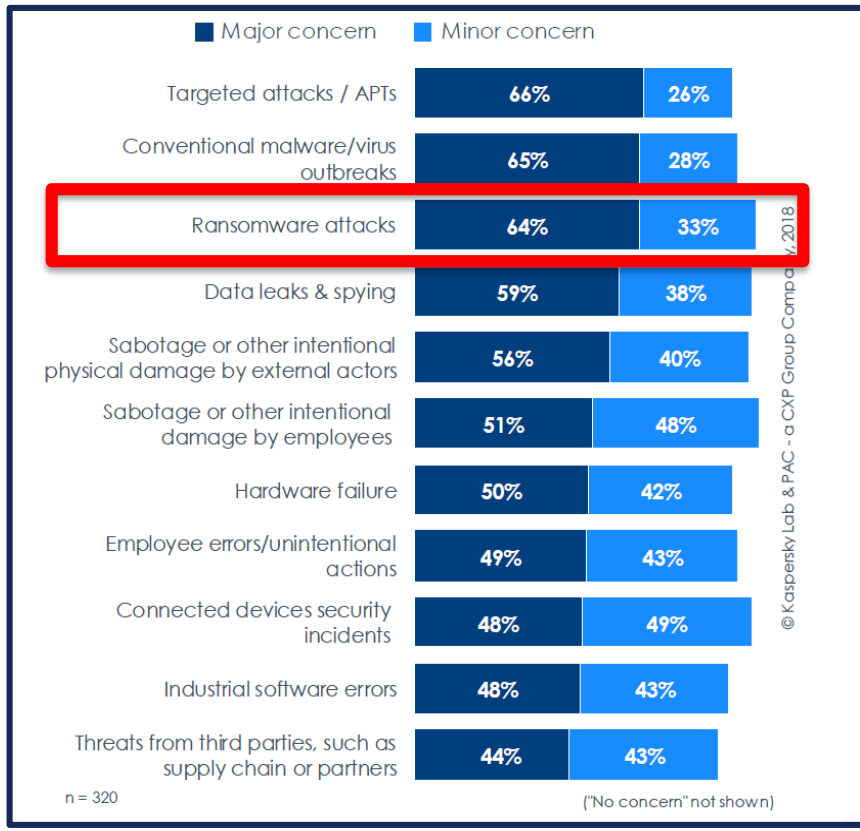


ILLINOIS
Electrical & Computer Engineering
GRAINGER COLLEGE OF ENGINEERING

October 5, 2020
ECE 590I Seminar

The Problem

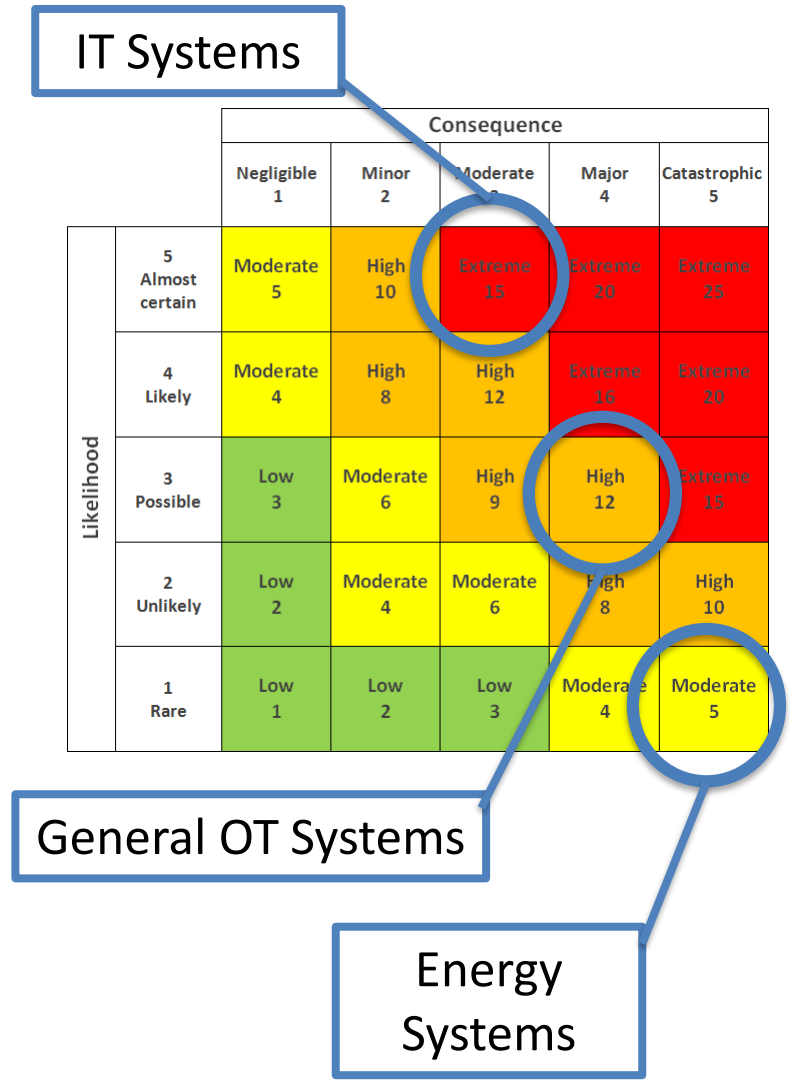
The threat of ransomware targeting **industrial control systems (ICS)** is rising.



https://www.zdnet.com/article/ransomware-attacks-are-now-targeting-industrial-control-systems/
https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/
https://www.infosecurity-magazine.com/news/ekans-ransomware-icsspecific/
https://www.infosecurity-magazine.com/news/us-gas-pipeline-shut-after/
https://latesthackingnews.com/2020/09/14/pakistans-power-utility-k-electric-suffered-ransomware-attack/

What Do We Mean by ICS Ransomware?

- Ransomware is **financially motivated.**
  - 2019 estimate: costs companies $75 billion per year
- Each industry must consider the potential consequences and likelihood of losing data and resources
- Successful campaign against ICS may lead to human health and safety risks
- Energy systems have high public impact if shut down
- Higher investment required to create ransomware that will penetrate to OT systems → less likely



https://phoenixnap.com/blog/ransomware-statistics-facts

Is there evidence that ransomware targeting energy systems is less common?

What types of operational technology (OT) devices would need to be infected to cause operational impacts on a power grid?

Background

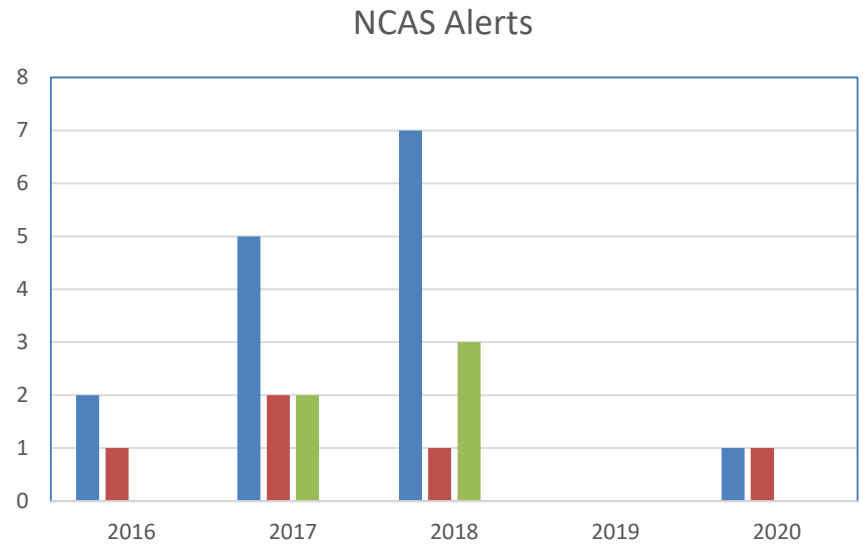
Why is ICS ransomware harder to defend against?

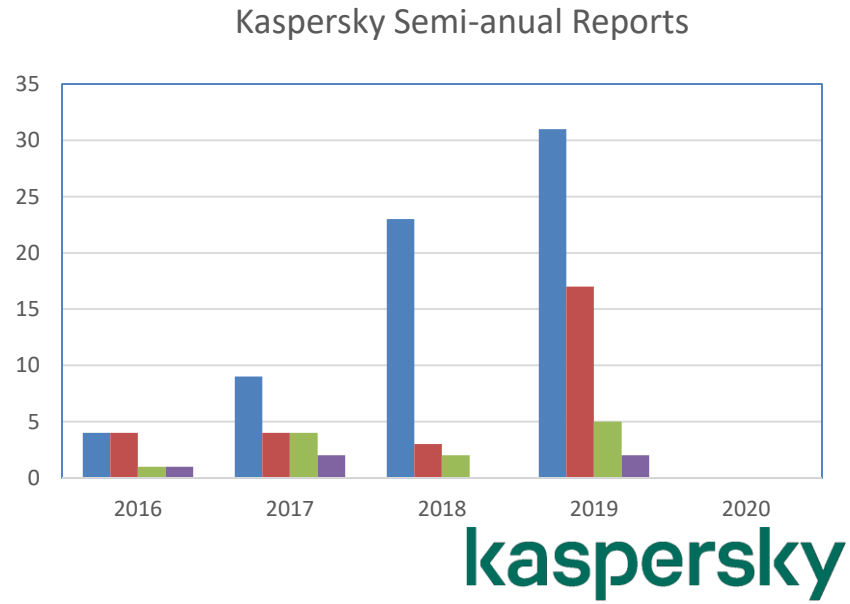
- Legacy systems
- Availability as a security priority

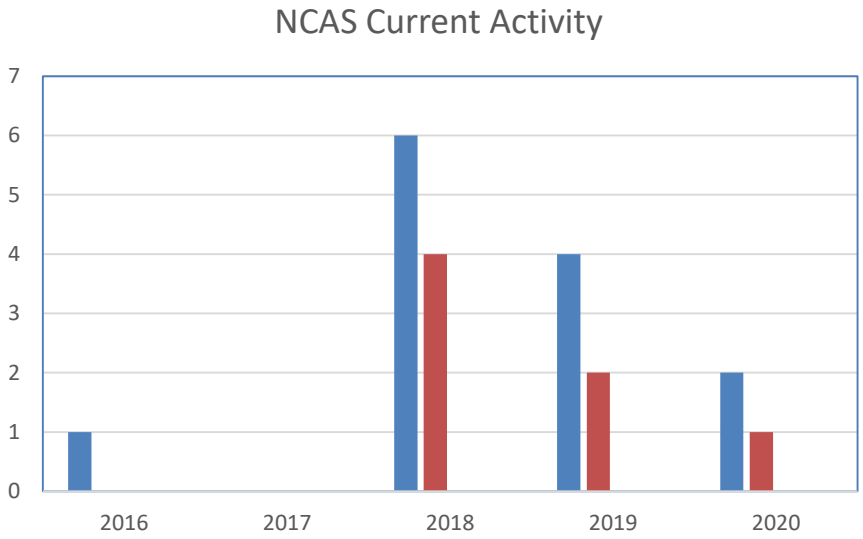
What makes the energy sector unique?

- Loss of availability is extremely costly and a safety risk
- Updating software is rare
- Operating decisions made frequently
- Highest cybersecurity reporting requirements in ICS
- Complexity and uniqueness of systems

Surveying ICS Security Events



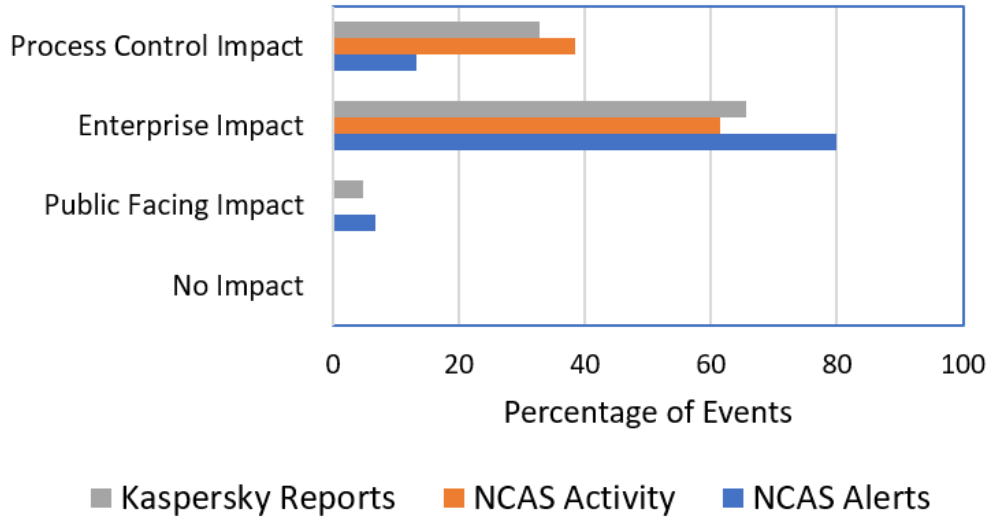




- ICS cybersecurity events are rising
- Ransomware is a significant portion of ICS events
- Energy ransomware is more rare

What Impact Did These Events Have?

- 69.1% impacted enterprise system
- 28.2% of campaigns impacted process control
- 3.7% explicitly impacted a public interface
- 0% reported no impact: unreported or undetected



The Utility Perspective

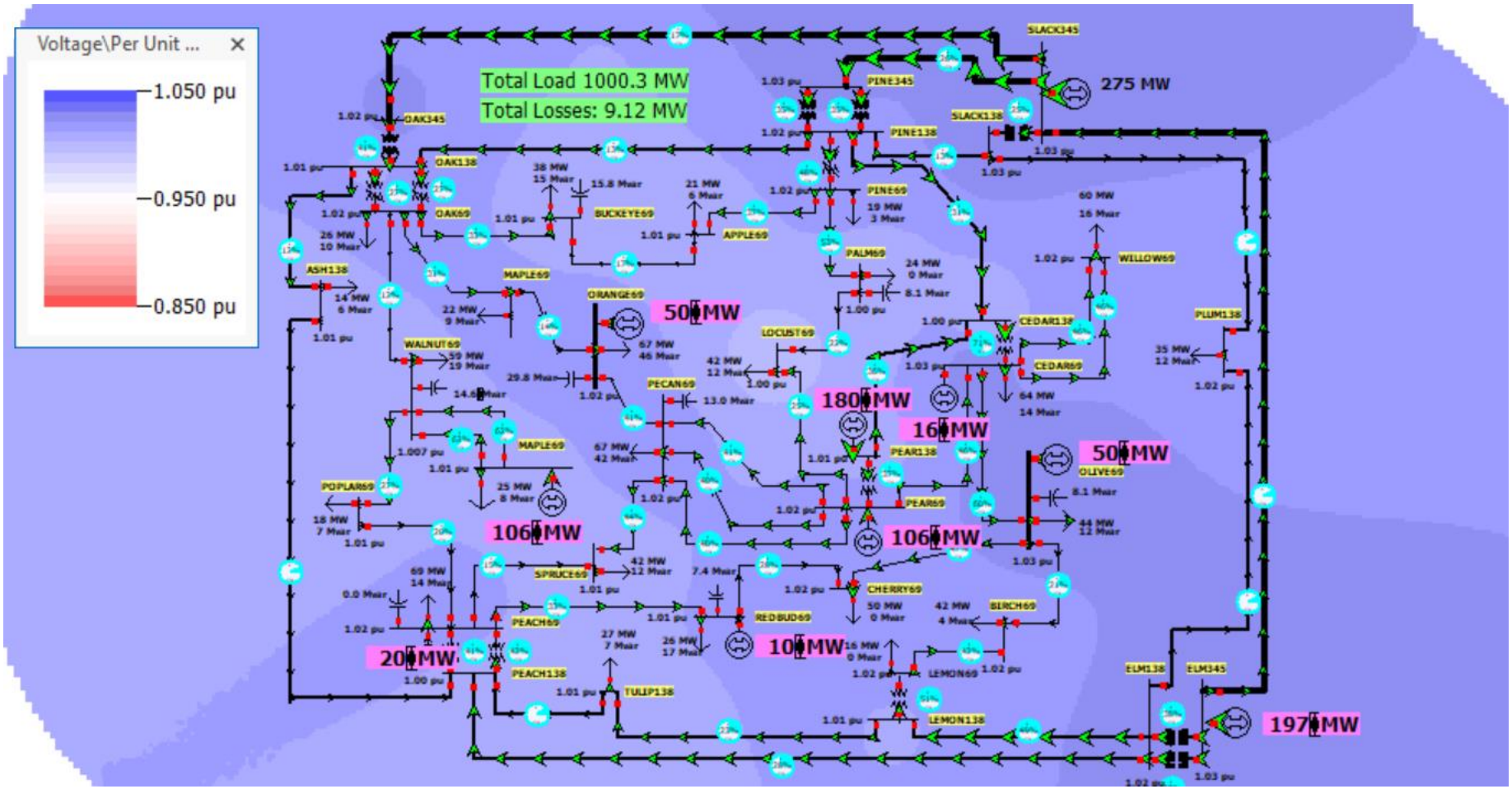
Federal law in the U.S. requires utilities to report all electric disturbance events

We compare cyber events to suspected vandalism or physical attacks:

- Cyber events represent 3% of total reported events
- Only 1 cyber event of 17 reported form Jan. 2016 to Feb. 2020 was known to impact customers; 3 had unknown impact
- 33 physical attacks caused impact out of total 264 physical attacks
    - More customers impacted
    - More load dropped

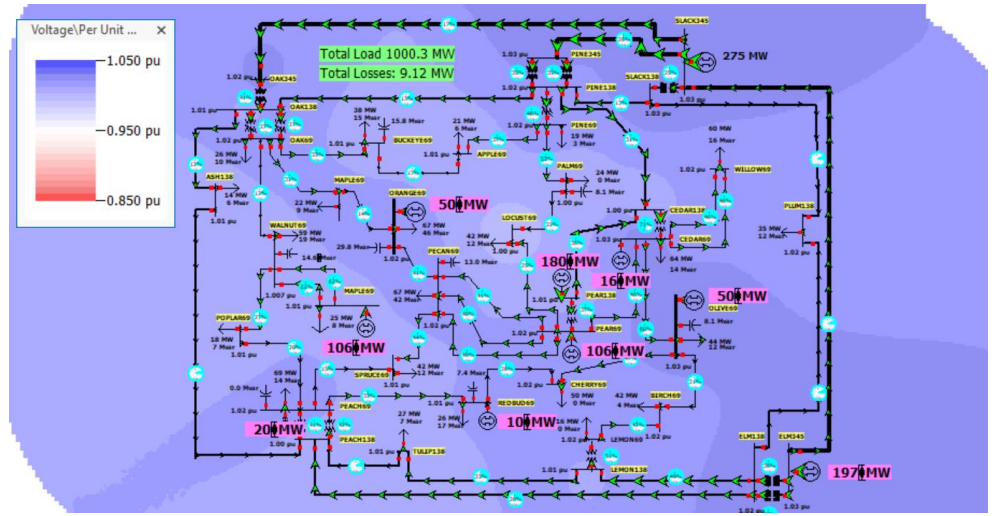
	2016	2017	2018	2019	2020
Total Events	141	150	220	278	42
Total Cyber Events	5	3	4	2	3
Customers Affected	0	0	23007	0	0
Load Lost [MW]	0	0	41	0	0
Total Vandalism/ Physical Attacks	28	41	46	56	92
Events with an Impact	2	8	10	12	1
Customers Affected	11671	21438	8832	4456	97
Load Lost [MW]	24	164	14435	3806	unknown

Simulating Ransomware on Electric Energy Systems

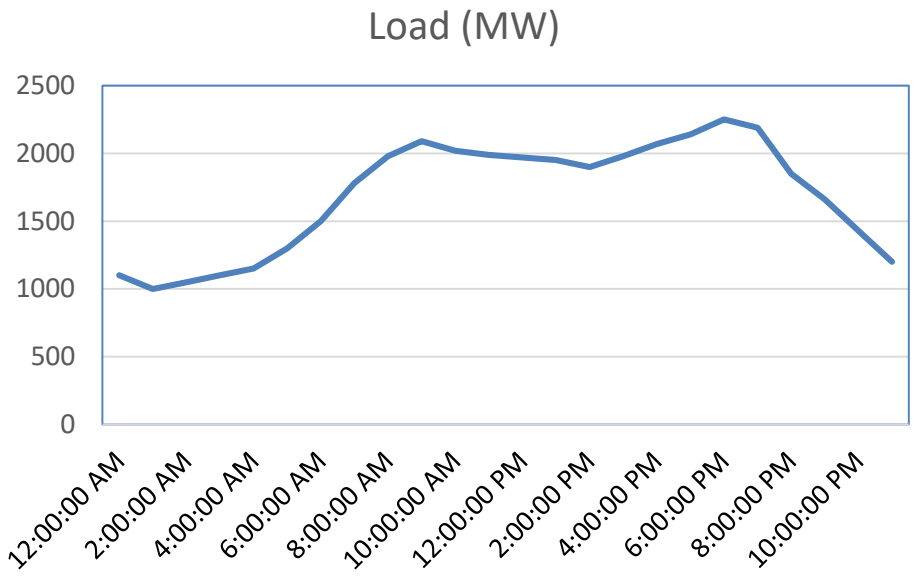


Simulating Ransomware on Electric Energy Systems

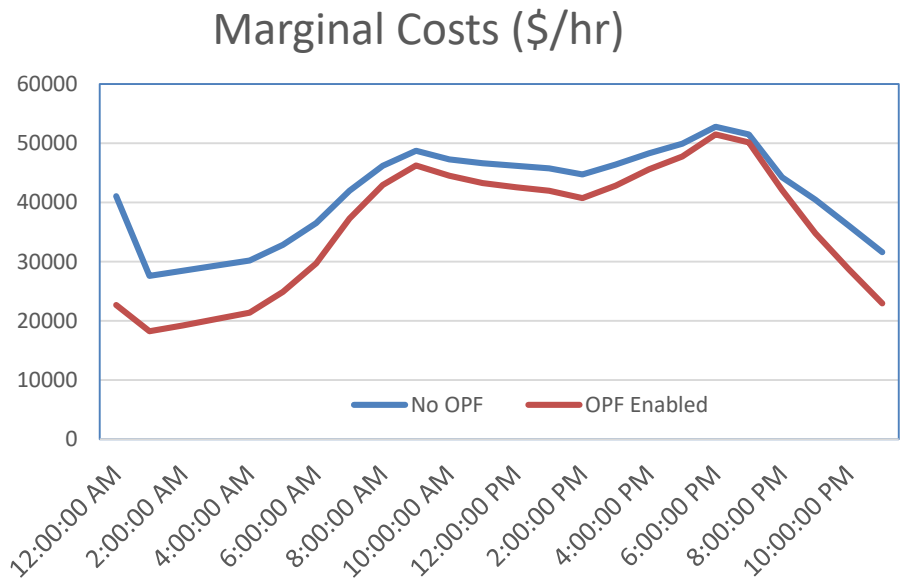
- **Historian:** cannot respond proactively to peak loads, only reactively adjust generation
- **Engineering Workstation:** prioritize generation changes by voltage/frequency measurements (line status unknown)
- **Application server**: Optimal Power Flow **(OPF) disabled**, compare marginal costs of generation
- **Database server:** No central access to voltage/current/frequency measurements, **Centralized SCADA unavailable**



Simulating Ransomware on Electric Energy Systems



Load ranges between 40% and 90% of generation capacity



Application server infected:

- Approximately $110,000 losses over a single day

Takeaways and Future Work

- ICS malware is rising, ransomware keeping pace and evolving.
- Not much evidence of **targeted energy sector** ransomware attacks, but still facing collateral damage
- Easiest ICS devices to compromise have lowest impact on operation
- Even high OT impact devices may not fully compromise ability to operate the grid

- How can we remove ransomware from OT systems without compromising availability?
- What cost-effective methods most efficiently protect ICS energy networks?

Questions?

Thanks for listening!