Cyber Hardening of Nuclear Power Plants with Real-time Nuclear Reactor Operation

Sam J. Root,[1] Porter Throckmorton[2]
Michael Haney,[2] R. A. Borrelli[1]

2023.04.20

University of Idaho
Nuclear Cybersecurity Working Group
[1]Department of Nuclear Engineering and Industrial Management
[2]Department of Computer Science

Idaho Falls Center for Higher Education

Nuclear Power Plants are cyberattack targets

Meltdown, radiological release, and LOCA are practically unrealisable

Financial cost and societal disruption (blackouts) from a reactor trip are more likely

Unplanned shutdown at a conventional utility scale NPP costs $10M [1]

[1] Peterson, J., et al., 2019. An overview of methodologies for cybersecurity vulnerability assessment conducted in nuclear power plants. Nuclear Engineering and Design 346, 75

There are a lot of notable incidents

Really. A lot.

Research is crucial as NPPs built before cybersecurity was a concern are getting their licenses renewed [2]

Davis-Besse Slammer Worm attack – Plant was offline, security was sufficient to protect essential core data, redundant analog controls [3]

Browns Ferry circulating pump failure – Distributed control system was overloaded similar to an DDoS forcing emergency shutdown [4]

---

[2] Brasileiro, A., 2019. Turkey Point nuclear reactors get OK to run until 2053 in unprecedented NRC approval. Miami Herald

[3] Poulsen, K., 2003. Slammer worm crashed Ohio nuke plant net. The Register

[4] NRC, 2007. NRC Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations

We proposed a two-pronged approach to cyber-hardening NPPs

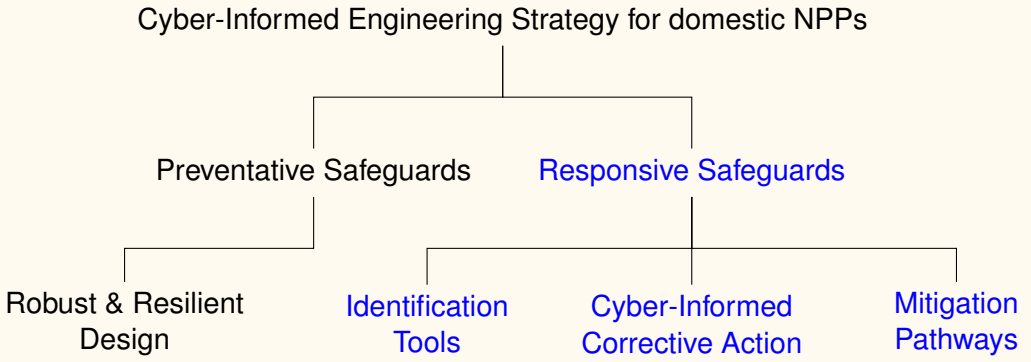

Figure 1. Cyber Informed Digitalization Design Tree

WSC platform

Figure 2. WSC Platform

Simulates nearly all aspects of a Generic PWR

Used for operator training

Affords functionality to simulate potential cyberattacks

Reactor trip

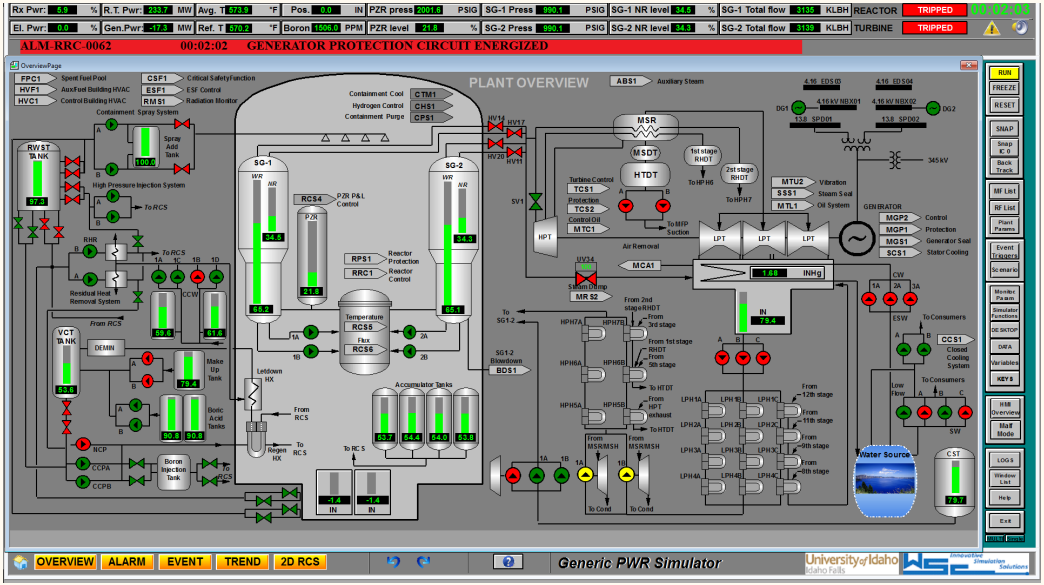

Figure 3. Simulator after Reactor Trip

Preliminary Hazards Analysis

A PHA is nominal measure of risk

Table 1. This framework for the cyber-informed PHA, defines risk as the *vulnerability* of a system to cyberattack as the product of *accessibility* of the system to a cyberattack by the *impact* of the cyberattack on the system. Accessibility is a measure as the ease to mount a successful cyberattack. Impact is defined as the deviation from the normal operational state of the reactor as a result of the cyberattack. The product therefore is nominally a judgment on the vulnerability of the system within the context of operational health of the NPP. Vulnerability then increases from the lower right to the upper left.

Impact	**Accessibility**				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	E	E	H	M	L
Critical	E	H	H	M	L
Moderate	H	H	M	M	L
Marginal	M	M	M	L	L
Negligible	M	L	L	L	L

E - Extreme Risk M - Moderate Risk
H - High Risk L - Low Risk

We applied a PHA to identify vulnerable systems

Table 2. PHA results for selected NPP plant systems. The PHA proposed by Table 1 was modified to include a fifth severity class (Impact) - *Moderate* due to the number of plant systems. The product of Accessibility and Impact nominally reflects the vulnerability of the system as to whether the reactor will be tripped or if the operator can take corrective or mitigating actions to recover operability.

Impact	**Accessibility**				
	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic					Reactor controls
Critical		Spent fuel pool Boron monitoring			
Moderate		Exciter	Steam generator Condenser		
Marginal		Cooling water systems			
Negligible					

Experiment on boron injection system

A LWR is controlled mechanically and chemically

Control rods are used for quick actuation, e.g. Start-up, Shut-down, and power transients

Boron dissolved in the moderator is used to account for fuel reactivity changes over the life of the core (Chemical Shimming)

Adding additional boron to the moderator beyond the equilibrium level makes the core subcritical, causing it to power down

Boron injection ‘fine tunes’ criticality

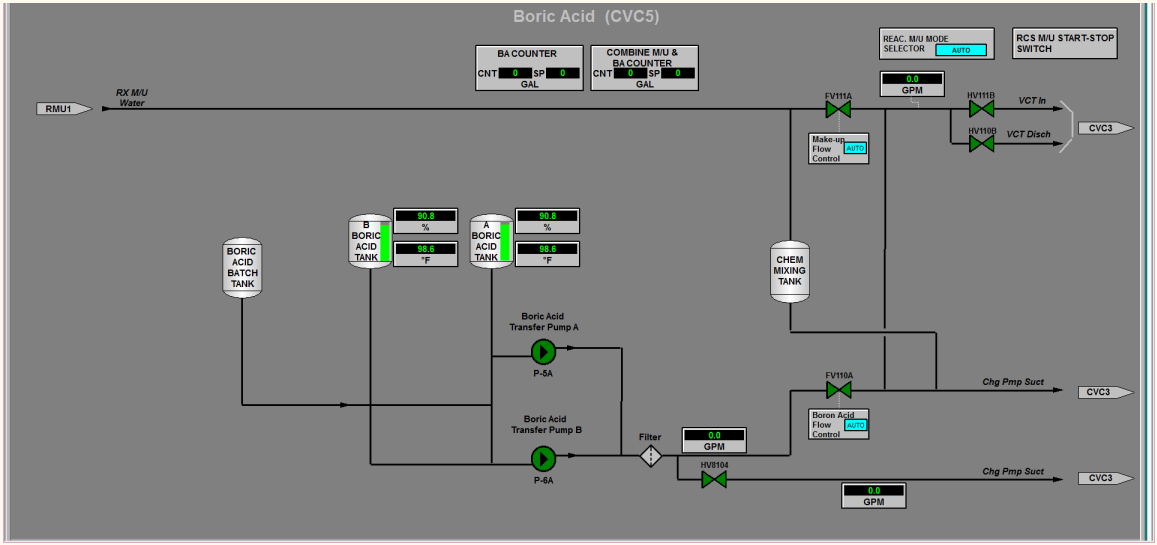

Figure 4. Chemical Shimming System HMI

Boron injection experiment dumped all the boric acid in the coolant

Event Trigger calls Boron Injection *Scenario* after 5 minutes of steady state critical operation

Boron Injection

- Turn on P-5A and P-6A
- Open HV8104

Freeze platform after reactor trips and turbine comes to rest

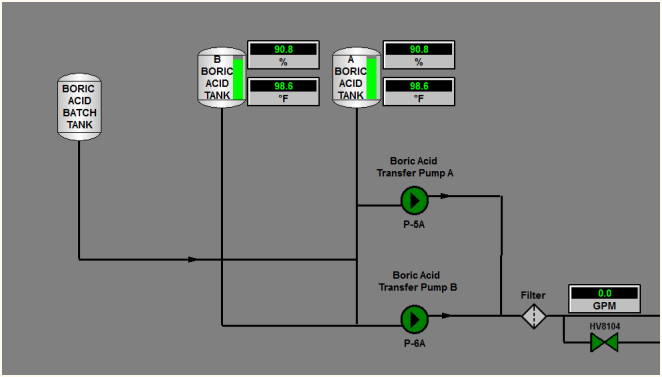

Figure 5. Chemical Shimming System HMI

Reactor tripped quickly because fission could not make up neutron absorption

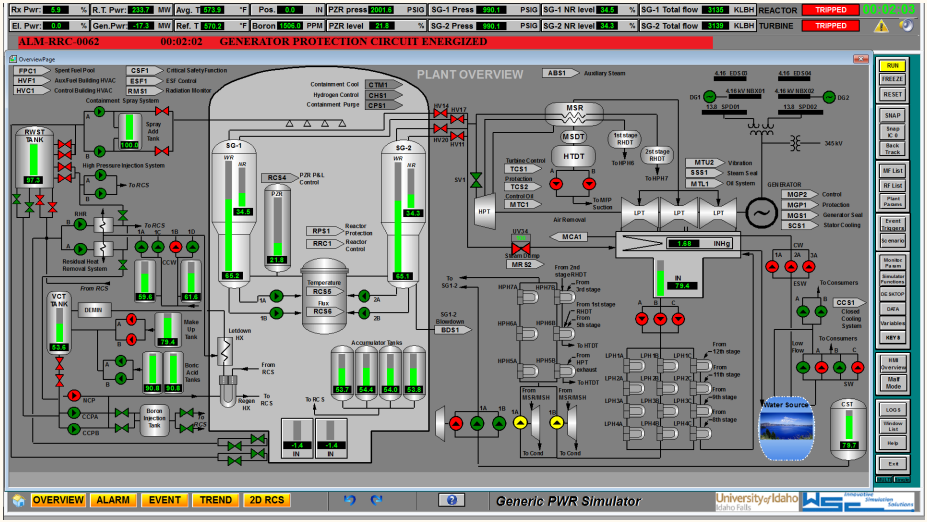

Figure 6. Simulator after Reactor Trip

So what happened?

Excess boron tripped the reactor between 30 and 40 minutes

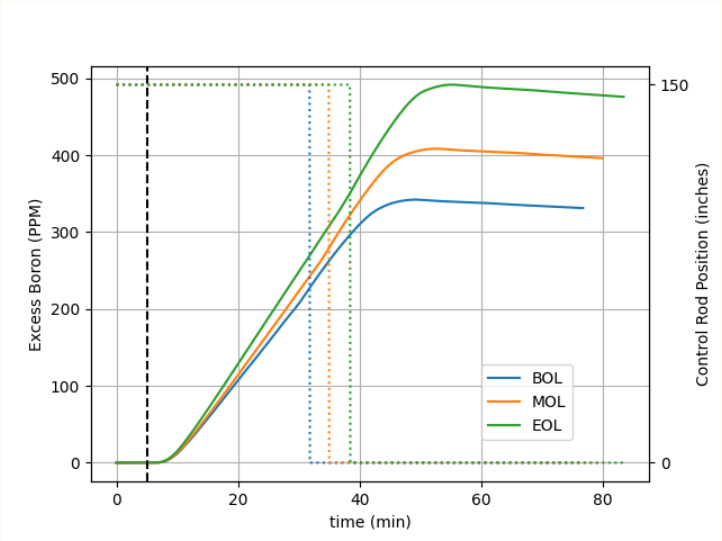

Figure 7. Excess Boron vs. Time

Core power sharply droppped

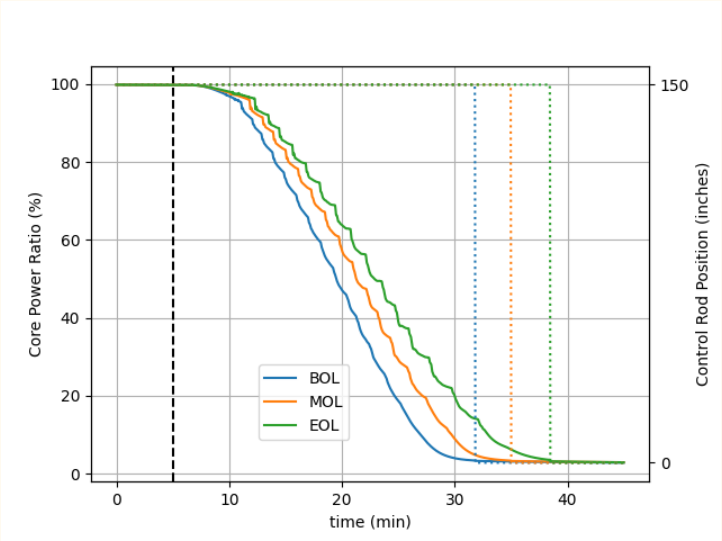

Figure 8. Core Power vs. Time

How would neutron multiplication change?

Calculate neutron multiplication factor (k_{eff}) using the current and previous power level ($\dot{Q}$), along with the number of neutron generations elapsed ($\Delta t / \ell_d^*$).

$$k_{eff} = \frac{\ell_d^*}{\Delta t} \ln \left[\frac{\dot{Q}(t)}{\dot{Q}(t - \Delta t)} \right] + 1 \tag{1}$$

What can be done?

Neutron multiplication does not provide a fingerprint

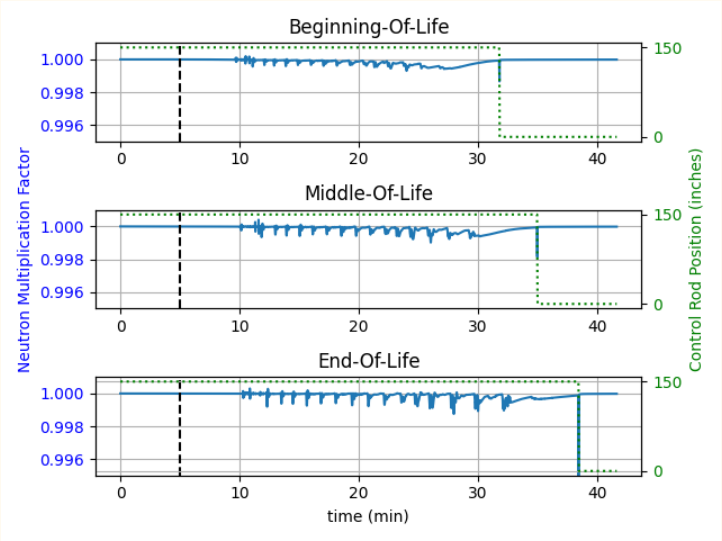

Figure 9. k_{eff} vs. Time

Reactivity provides a fingerprint

Convert k_{eff} to net reactivity (ρ).

$$\rho = \frac{k_{eff} - 1}{k_{eff}} \quad (2)$$

Put through a low-pass filter

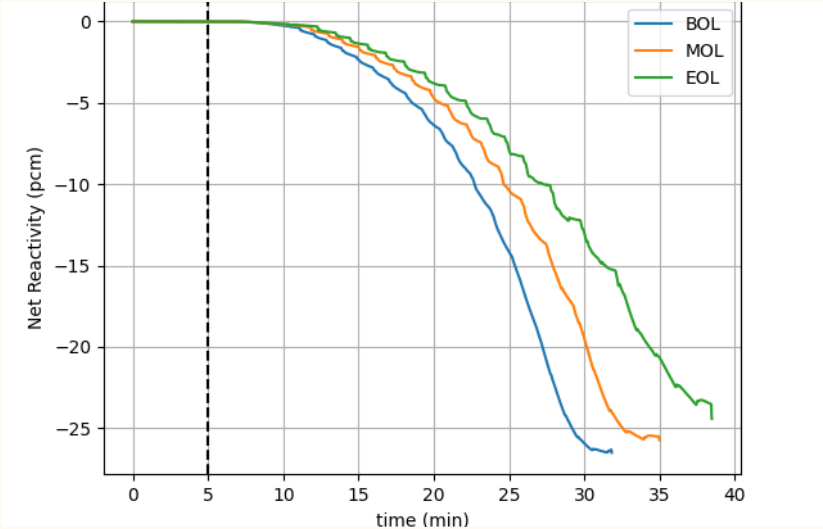

Figure 10. Identification Tool – Filtered Net Reactivity

Responsive safeguards

We need to figure out what the operators can do now

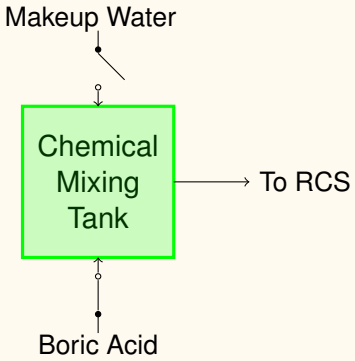

Figure 11. Boron Injection Attack

With the fingerprint, operators shut off boric acid pumps

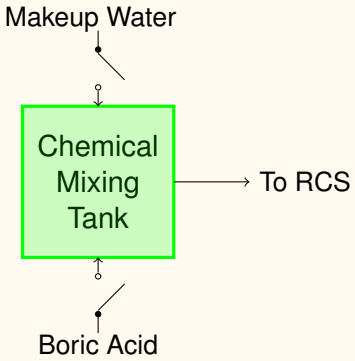

Figure 12. Boron Injection Attack - Cyber-Informed Corrective Action

The time to trip is delayed

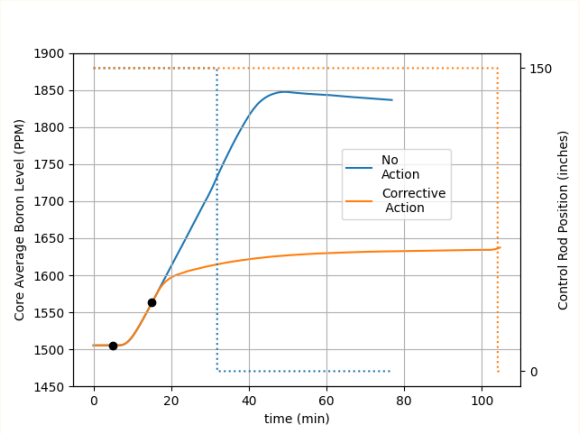

Figure 13. Corrective Action: Boron Level

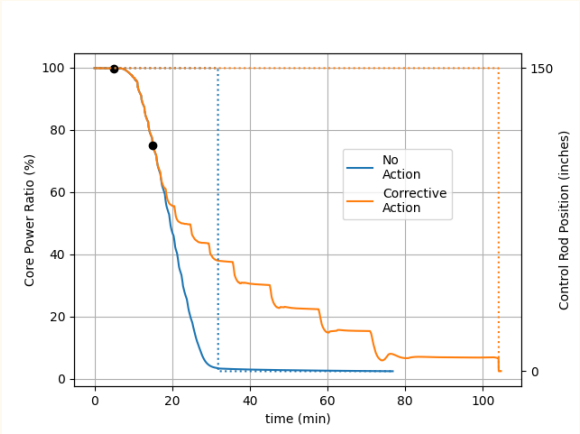

Figure 14. Corrective Action: Core Power

Now dump fresh water into the coolant

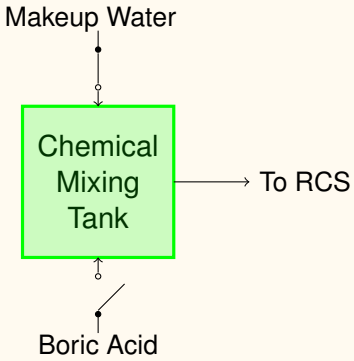

Figure 15. Boron Injection Attack – Mitigation Pathway

It worked! The reactor does not trip

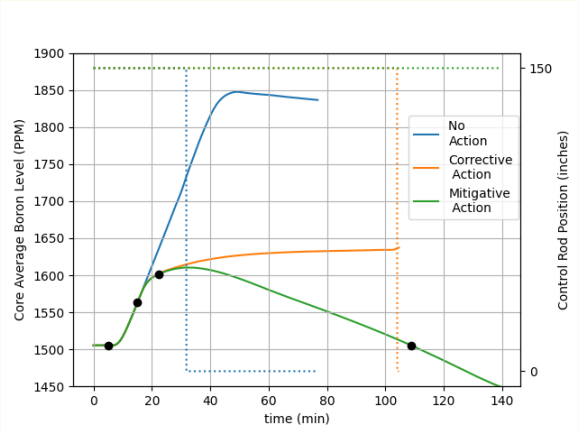

Figure 16. Mitigation: Boron Level

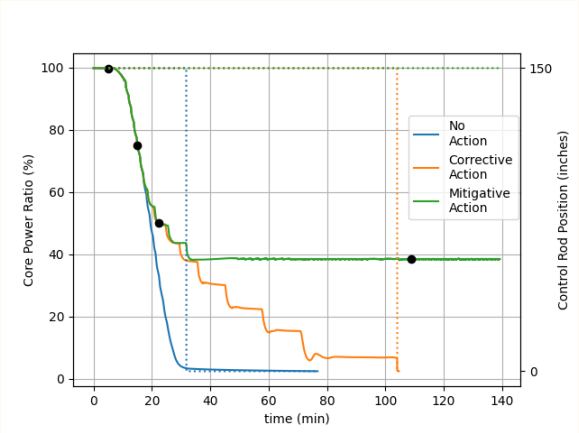

Figure 17. Mitigation: Core Power

Experiment on the Rankine power cycle

We are looking outward to power systems holistically

Stepping away from the core to downstream processes common to most electrical power plants.

Turbine, generator and exciter are common to power plants

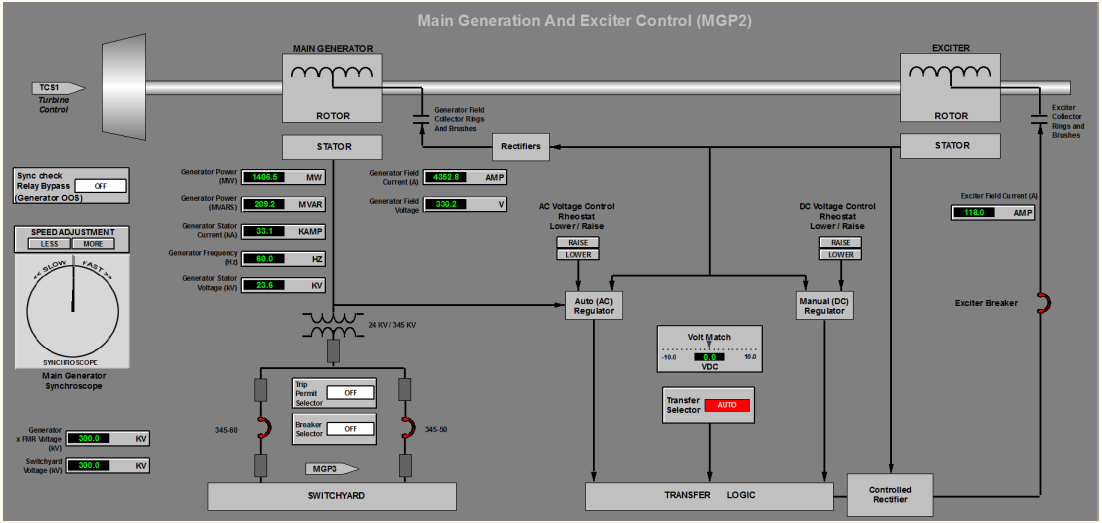

Figure 18. Generator and Exciter Control HMI

False data or noise can be injected into the controller

Injecting false error to the voltage controller

The controller will overcompensate and could fail

False data or noise can be injected into the controller

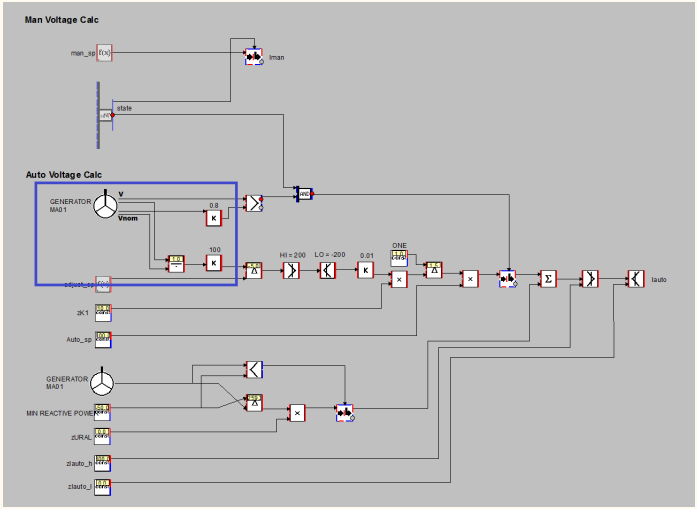

Figure 19. Voltage Control Model.

False data or noise can be injected into the controller

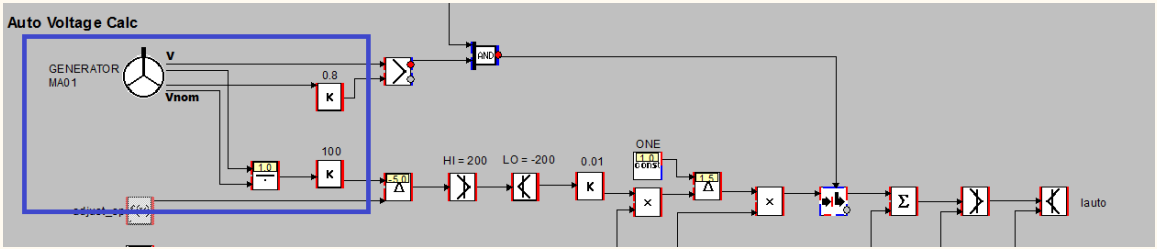

Figure 20. Voltage Control Model.

Decreasing the gain block forces voltage to increase

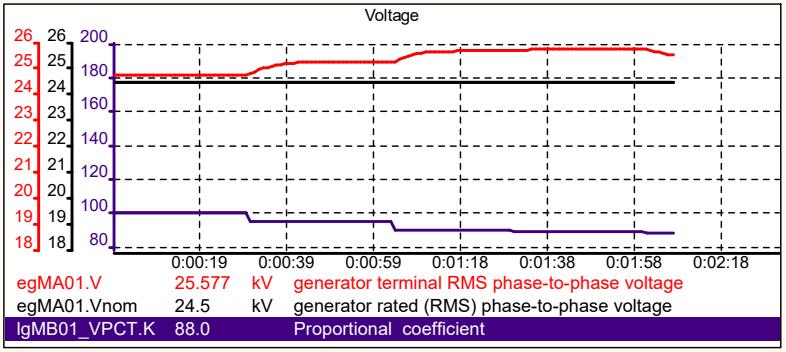

Figure 21. Voltage

Gain (purple)

Voltage measurement (red) and setpoint (black)

First order transfer function dynamics

Decreasing the gain block forces voltage to increase

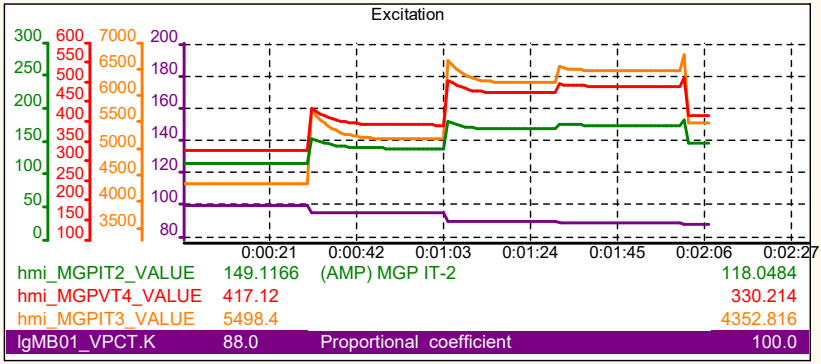

Figure 22. Excitation.

Exciter winding current (green)

Generator winding current (orange)

Generator winding voltage (red)

Exciter activity increases to increase output voltage

Decreasing the gain block forces voltage to increase

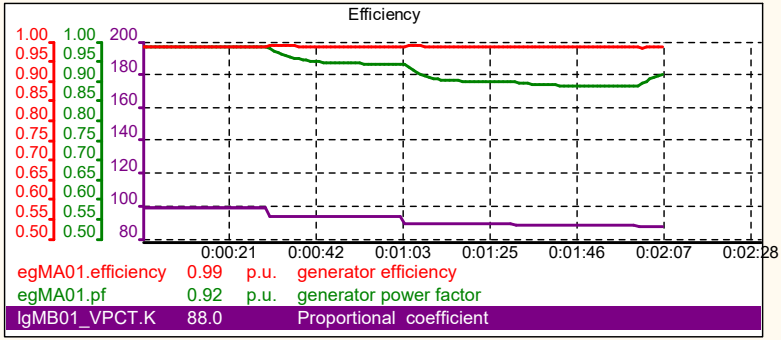

Figure 23. Efficiency

Generator efficiency (red)

Generator power factor (green)

More reactive power is generated

Decreasing the gain block forces voltage to increase

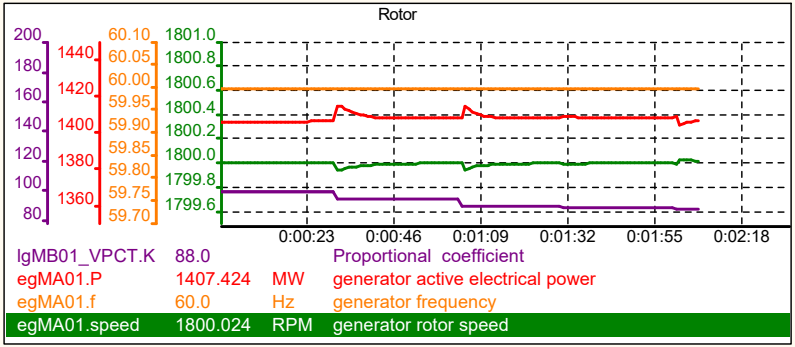

Figure 24. Shaft and Generation

Generator power (red)

Generator rotor speed factor (green)

Generator frequency (orange)

The opposing sawtooth ‘blips’ are caused by action-reaction

Decreasing the gain block forces voltage to increase

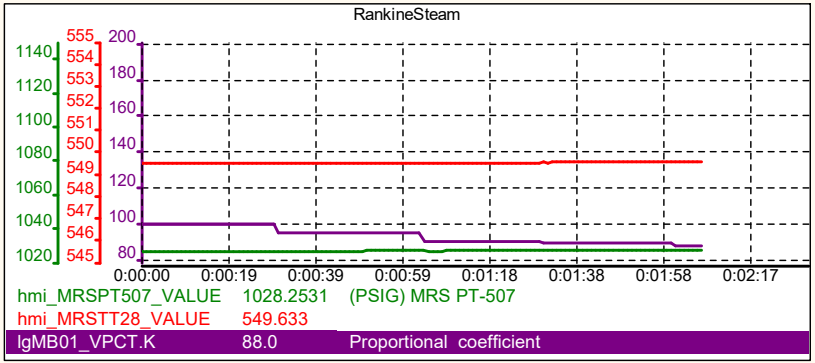

Figure 25. Power Cycle

Turbine inlet temperature (red)

Turbine inlet pressure (green)

Very little effect on upstream processes

Responsive safeguards

Automatic trip to DC control

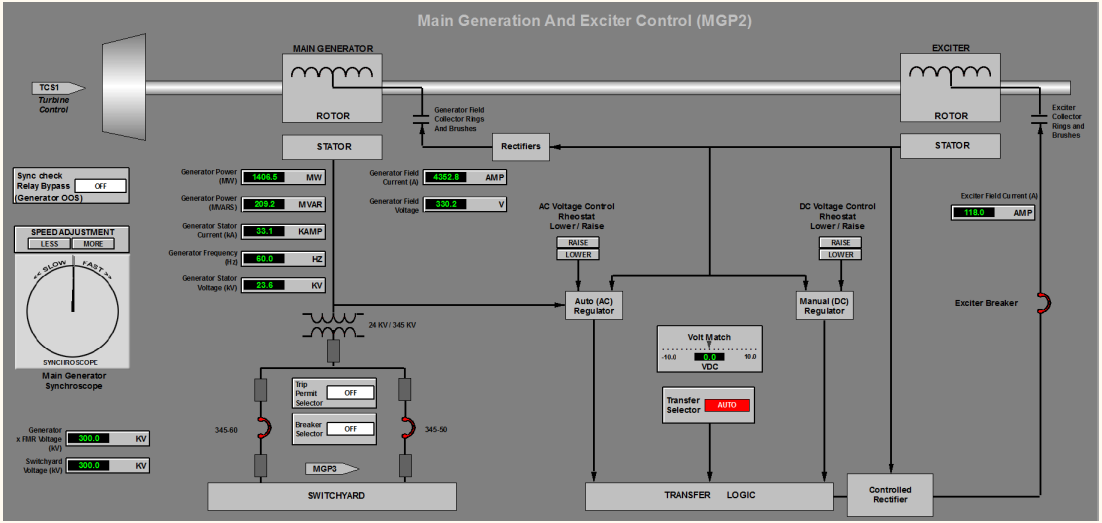

Figure 26. Generator and Exciter Control HMI

Automatic to DC control

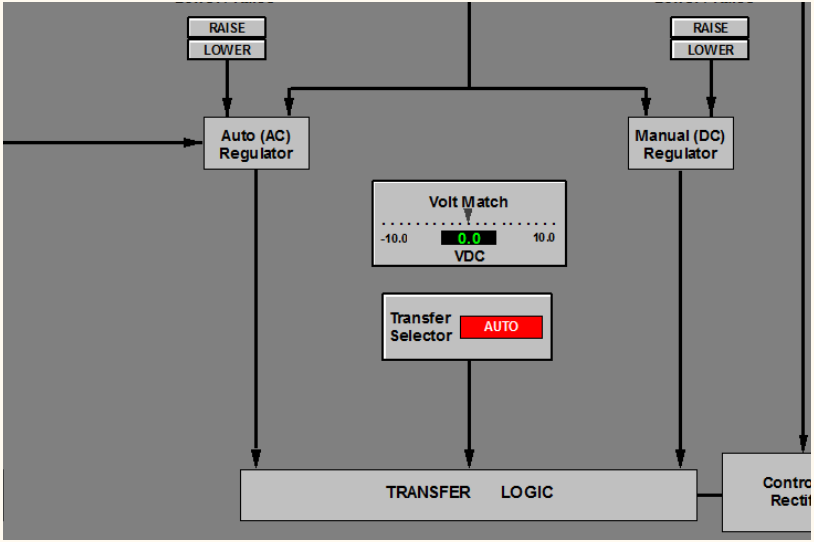

Figure 27. Generator and Exciter Control HMI

Another attempt

Increasing the gain block forces voltage to decrease

Gain (purple)

Voltage measurement (red) and setpoint (black)

First order transfer function dynamics

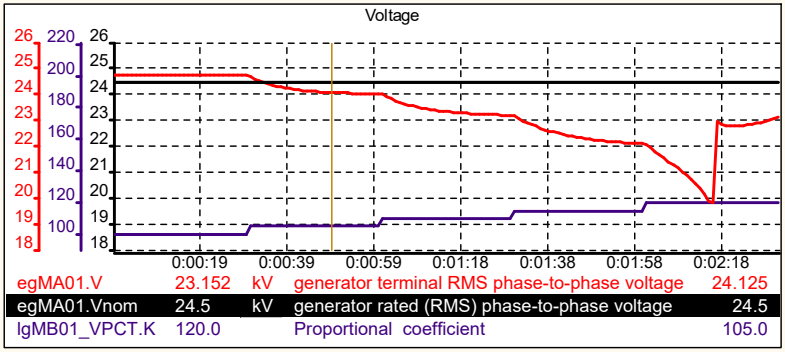

Figure 28. Voltage

Increasing the gain block forces voltage to decrease

Gain (purple)

Exciter winding current (green)

Generator winding current (orange)

Generator winding voltage (red)

Exciter activity decreases to decrease output voltage

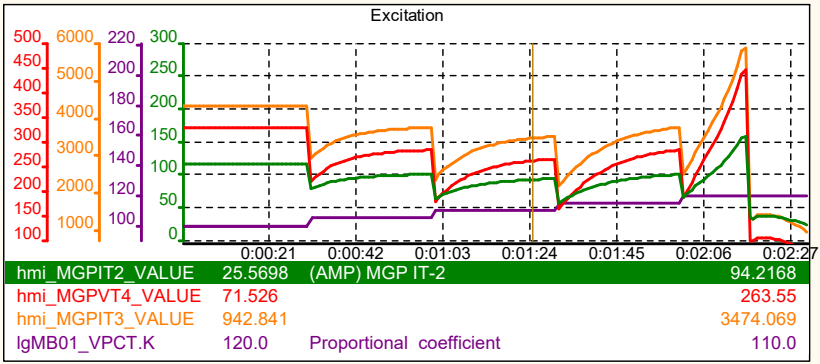

Figure 29. Excitation.

Increasing the gain block forces voltage to decrease

Gain (purple)

Generator efficiency (red)

Generator power factor (green)

More reactive power is generated

Could be indicative of other downstream problems

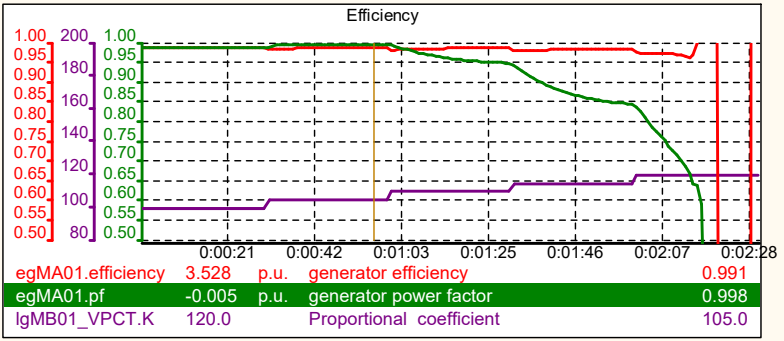

Figure 30. Efficiency

Increasing the gain block forces voltage to decrease

Gain (purple)

Generator power (red)

Generator rotor speed factor (green)

Generator frequency (orange)

The sawtooth ‘blips’ are the fingerprint of this attack

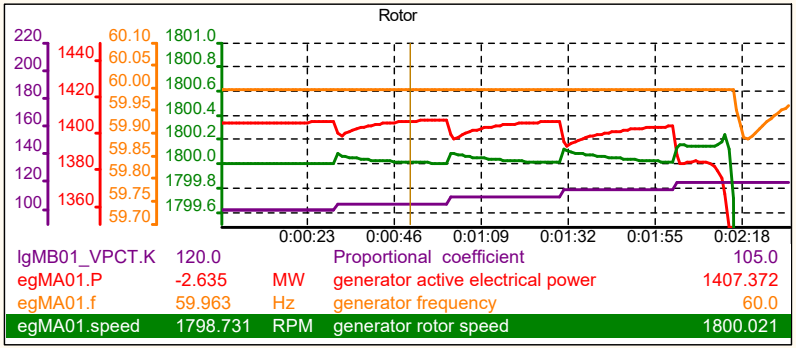

Figure 31. Shaft and Generation

Steam generator pressure provides a fingerprint

Gain (purple)

Turbine inlet temperature (red)

Turbine inlet pressure (green)

Pressure spike just before reactor trip

Compressed liquid unable to effectively remove heat from primary loop

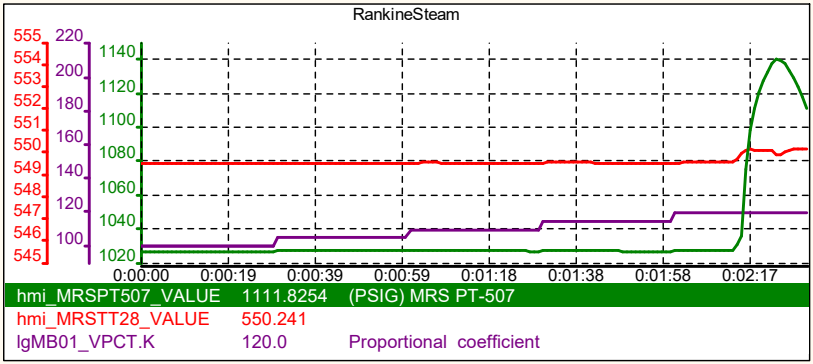

Figure 32. Power Cycle

Responsive safeguards

The fast time to trip provides difficulty

System is resilient to large error insertion

Shaft speed and power blips allow identification

Manually trip to DC control to stop cyberattack

Must find and remove worm to mitigate

Could trip to DC control if enough warning time

Narrow gate logic

Preventative safeguards to design a better controller

Cyberattack simulation proof-of-concept

Cyberattack simulation

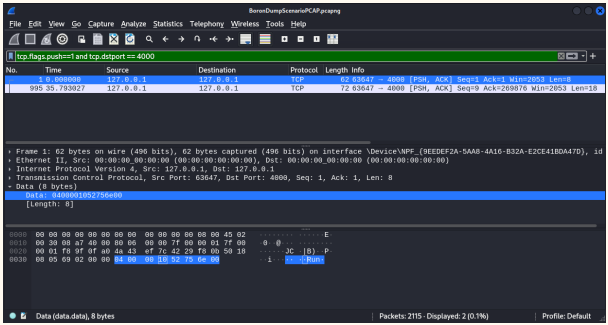

Figure 33. Boron Injection Packet Capture (Wireshark)

Use Wireshark to capture and analyze network traffic

Potential Attacks

- Boron injection scenario[1]
- Distributed Denial of Service (DDoS)
- Man in the Middle (MITM)

[1] Or any operation that can be done by a PLC

Penetration testing

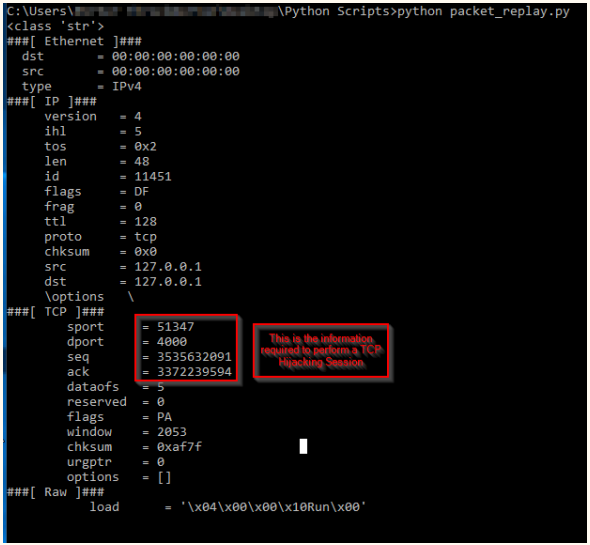

Figure 34. Captured Packet Information

Scapy exploit

```
def scapy_exploit():
  source_port = 49923
  sequence_number = 3522655476
  ack_number = 3648359537
  dest_port = 4000
  source_ip = '127.0.0.1'
  dest_ip = '127.0.0.1'
  ip = IP(src=source_ip, dst=dest_ip)
  tcp = TCP(sport = source_port, dport = dest_port, flags = "PA", seq=
                                        sequence_number, ack=ack_number)
  data = "\x04\x00\x00\x10Run\x00"
  pkt = ip/tcp/data
  send(pkt, verbose=1, iface = (scapy.interfaces.dev_from_index(-1)))
  print("[+] Exploit sent \n")
```

Penetration testing

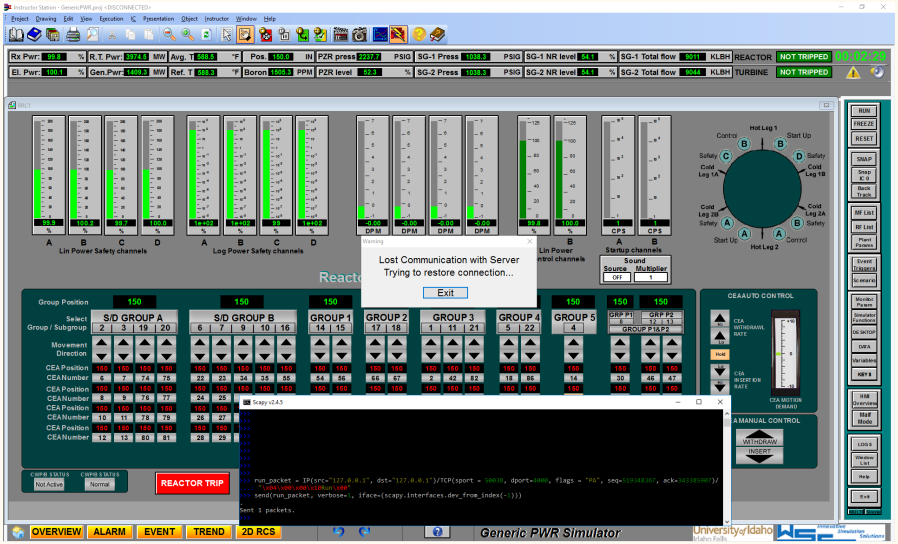

Figure 35. HMI Bypass

Challenges to penetration testing

TCP/IP connection resets itself after running exploit

WSC Platform machine is too powerful and fast

- TCP/IP Hijacking requires extracting information from current session
- Sequence and Acknowledgment numbers change too rapidly

Future work

Testing additional plant systems for vulnerabilities applying the methodology presented

Use Failure Modes & Effects Analysis (FMEA) to identify cyberattack vectors and targets

Simulate additional DDoS and MITM cyberattacks on these systems

Identify data transmission related to the operator display and create spoofed values

Determine the data that we need to provide to operators and plant personnel that are indicative of these cyberattacks

Design displays and data visualization tools on the WSC platform to this end

Final remarks

This work is a novel use of the WSC platform, which is typically used for operator training

By using it for raw data collection during atypical operation, we have identified the tools needed for operators to identify an attack on a high risk target, as well as giving a path to mitigation.

The methodologies adopted for the cyberattacks to be conducted use abnormal conditions that are in scope for the simulator only

The end-state of the attack is the same, but the simulator's method of communication between the client machine and the simulator is unique to the simulator only

The educational value that the cyberattack simulation provides will remain consistent with real-life scenarios that the industry faces

This attack details the broader impacts of the study

Final remarks

The exciter is common to all generation facilities

Artificial Intelligence could be employed to monitor data and identify fingerprints faster than a human operator with dozens of other responsibilities

AI would either warn the operator or take corrective/mitigative action itself

Acknowledgements

Research was funded by the University of Idaho ‘Operation: Resubmission’ program.

References

1. Peterson, J., et al., 2019. An overview of methodologies for cybersecurity vulnerability assessment conducted in nuclear power plants. Nuclear Engineering and Design 346, 75.
2. Brasileiro, A., 2019. Turkey Point nuclear reactors get OK to run until 2053 in unprecedented NRC approval. Miami Herald.
3. Poulsen, K., 2003. Slammer worm crashed Ohio nuke plant net. The Register.
4. NRC, 2007. NRC Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations.