Simulated Boron Shimming Cyberattack on a Pressurized Water Reactor

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

Nuclear Cybersecurity Working Group

University of Idaho · Idaho Falls Center for Higher Education
[1]Department of Nuclear Engineering and Industrial Management
[2]Department of Computer Science

2022.08.06

Nuclear Power Plants as cyberattack targets

- Meltdown, radiological release, and LOCA are practically unrealisable

Nuclear Power Plants as 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 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

Objective

- Risk Assessment
  - Preventative Safeguards
    - Robust/Resiliant Design
  - Responsive Safeguards
    - Identification Tools
    - Cyber-Informed Corrective Action
    - Mitigation Pathways

Cyber Informed Digitalization Design Tree

LWR control

- Control rods are used for quick actuation, i.e. 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

Notable incidents

- There's a lot
- Research is crucial as NPPs built before cyber-security 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 DoS 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

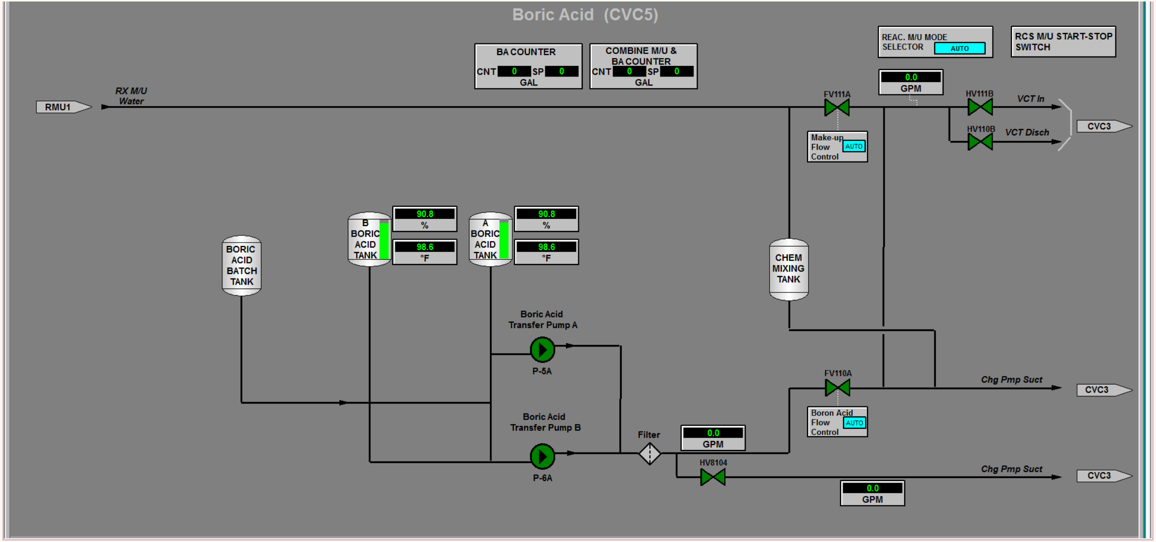
[4]NRC, 2007. NRC Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations

WSC platform

WSC Platform

- Simulates nearly all aspects of a Generic PWR
- Used for operator training
- Affords functionality to simulate potential cyberattacks

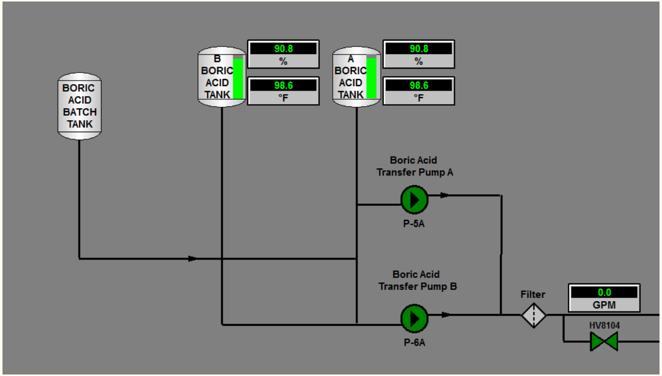
Boron injection



Chemical Shimming System HMI

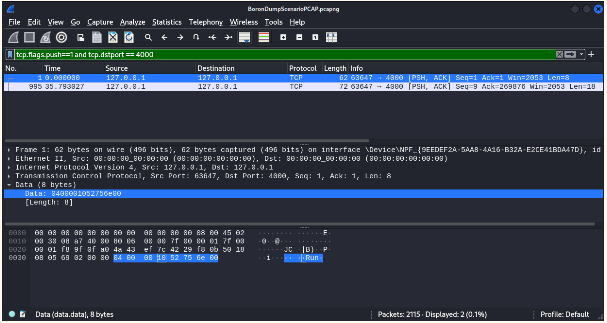
Boron injection

- *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



Chemical Shimming System HMI

Cyberattack simulation



Boron Injection Packet Capture (Wireshark)

- Use Wireshark to capture and analyze network traffic
- Potential Attacks
  - Boron Injection Scenario[1]
  - Denial of Service

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

Penetration testing

```
C:\Users\[redacted]\Python Scripts>python packet_replay.py
<class 'str'>
###[ Ethernet ]###
  dst       = 00:00:00:00:00:00
  src       = 00:00:00:00:00:00
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x2
     len       = 48
     id        = 11451
     flags     = DF
     frag      = 0
     ttl       = 128
     proto     = tcp
     chksum    = 0x0
     src       = 127.0.0.1
     dst       = 127.0.0.1
     \options   \
###[ TCP ]###
        sport     = 51347
        dport     = 4000
        seq       = 3535632091
        ack       = 3372239594
        dataofs   = 5
        reserved  = 0
        flags     = PA
        window    = 2053
        chksum    = 0xaf7f
        urgptr    = 0
        options   = []
###[ Raw ]###
           load      = '\x04\x00\x00\x10Run\x00'
```

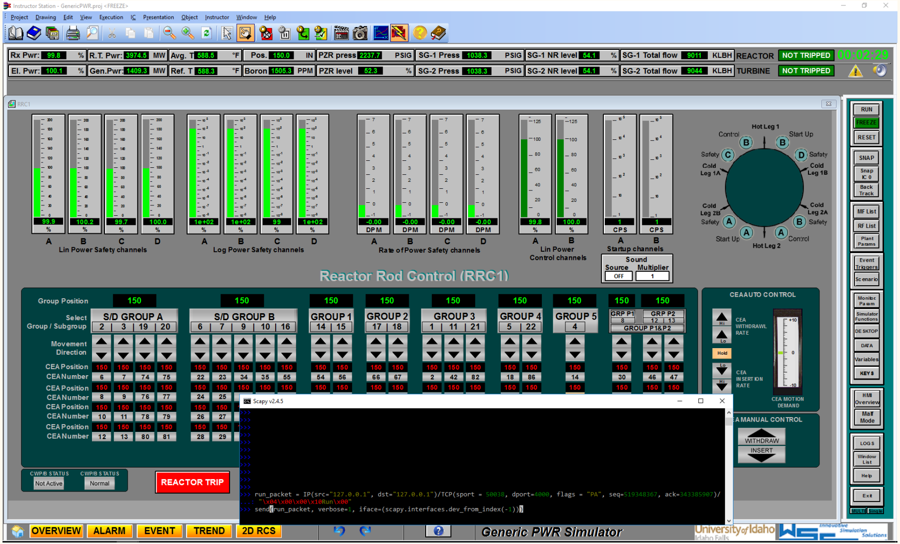
This is the information required to perform a TCP Hijacking Session

Captured Packet Information

Scapy exploit

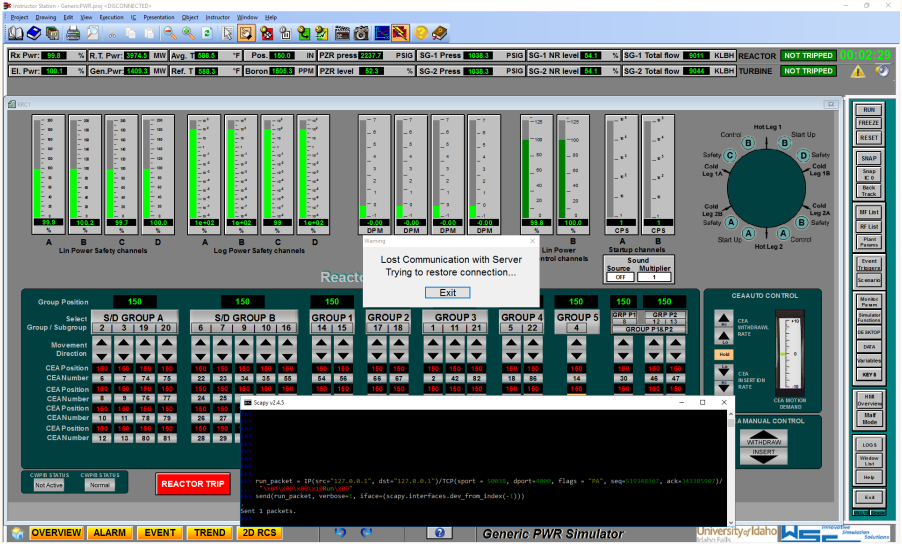
```python
def scapy_exploit():
  source_port = 49923
  sequence_number = 3522655476
  ack_number = 3648359537
  dest_port = 4000
  source_ip = '127.0.0.1'
  dest_ip = '127.0.0.1'
  ip = IP(src=source_ip, dst=dest_ip)
  tcp = TCP(sport = source_port, dport = dest_port, flags = "PA", seq=
                                   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



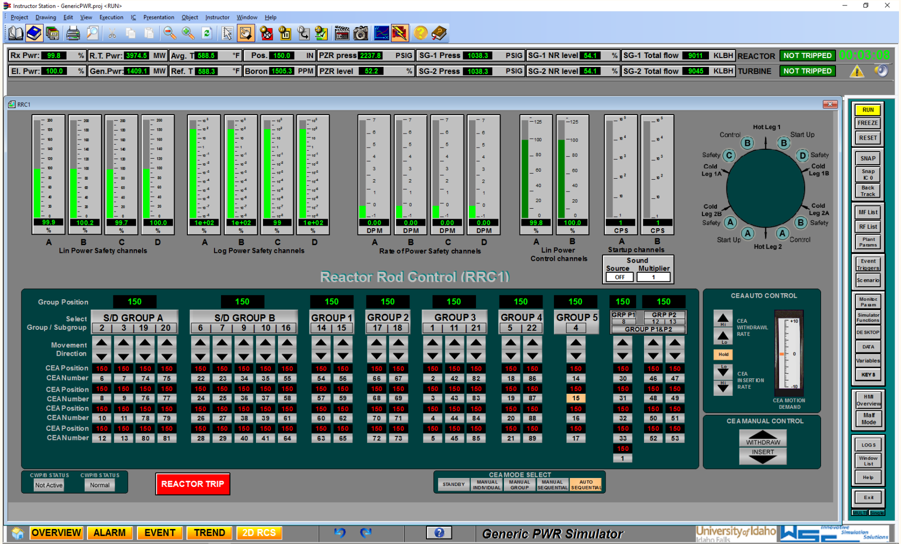
HMI Bypass

Penetration testing



HMI Bypass

Penetration testing

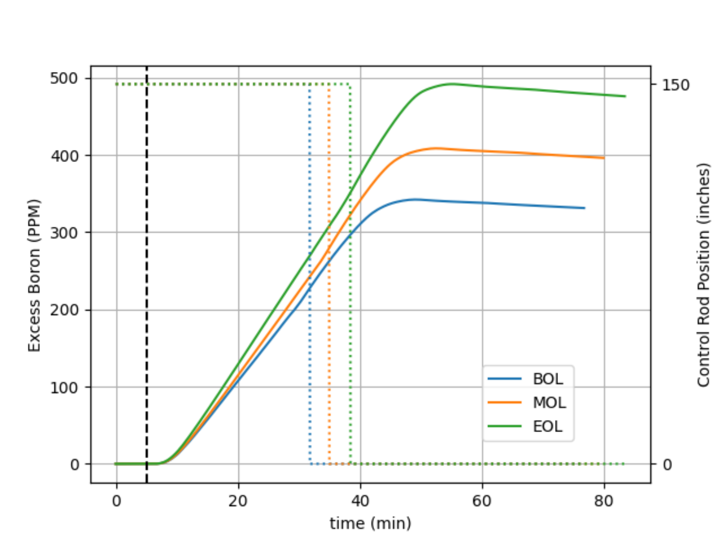


HMI Bypass

Challenges

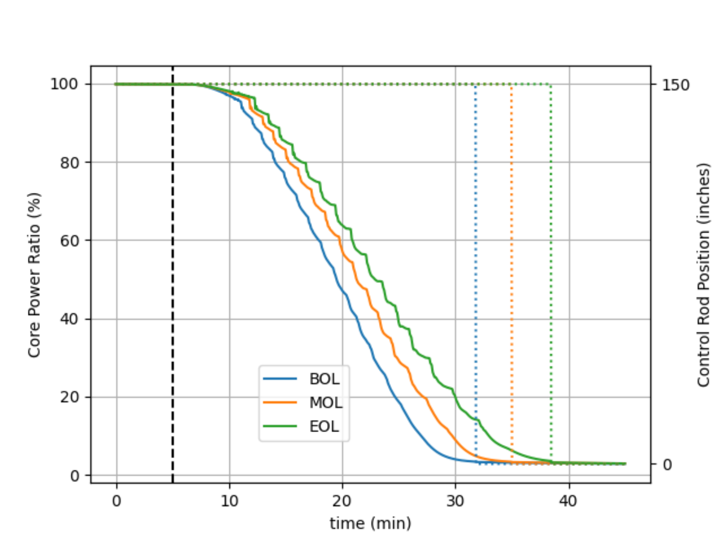
- TCP/IP connection resets itself after running exploit
- WSC Platform machine is too powerful - unrealistic
    - TCP/IP Hijacking requires extracting information from current session
    - Sequence and Acknowledgment numbers change too rapidly

Results and discussion



Excess Boron vs. Time

Results and discussion



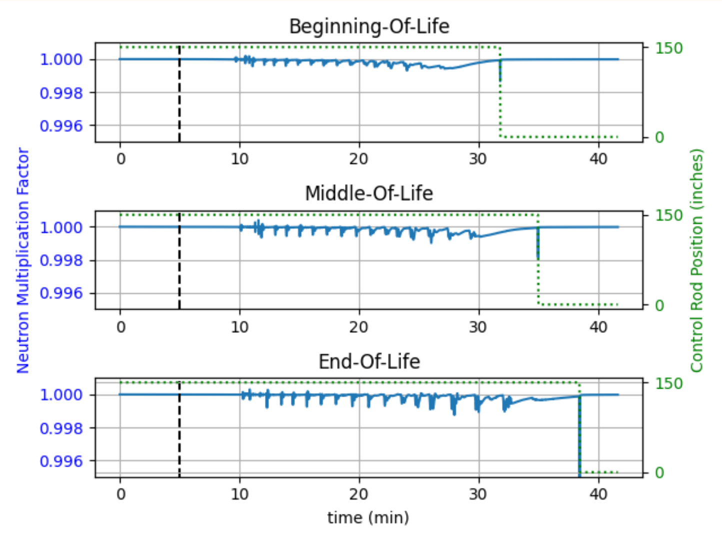
Core Power vs. Time

Results and discussion

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

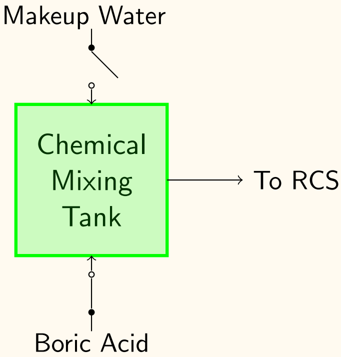
$$k_{eff} = \frac{\ell_d^*}{\Delta t} \ln\left[\frac{\dot{Q}(t)}{\dot{Q}(t-\Delta t)}\right] + 1$$

Results and discussion



k_{eff} vs. Time

Responsive safeguards



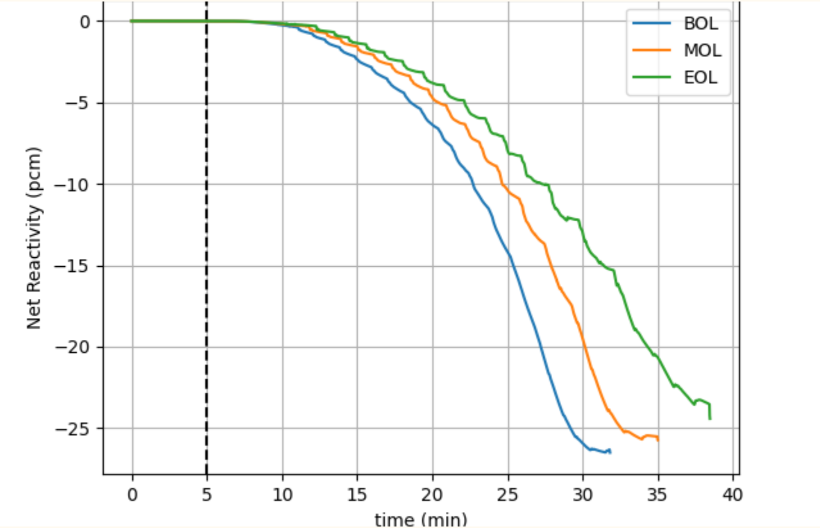
Boron Injection Attack

Responsive safeguards

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

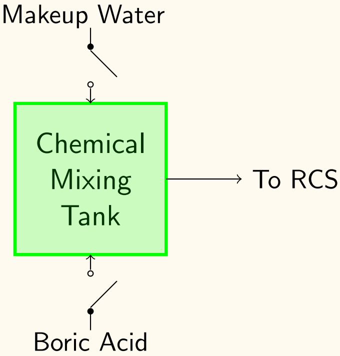
$$\rho = \frac{k_{eff} - 1}{k_{eff}}$$

Put through a low-pass filter



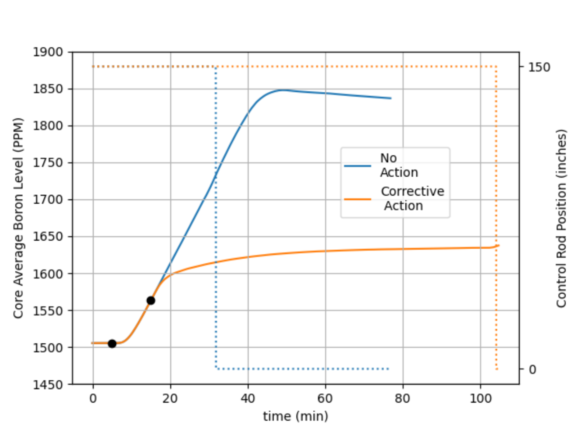
Identification Tool: Filtered Net Reactivity

Responsive safeguards

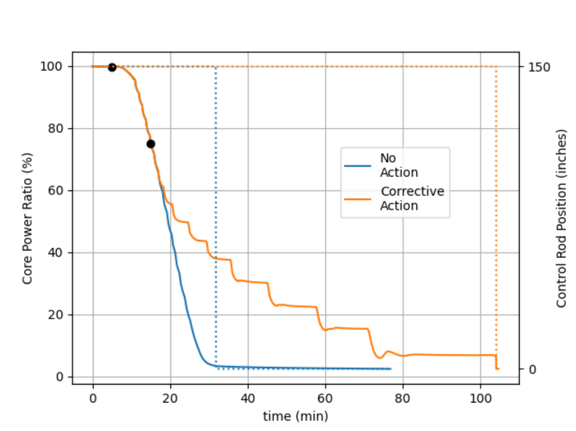


Boron Injection Attack - Cyber-Informed Corrective Action

Responsive safeguards

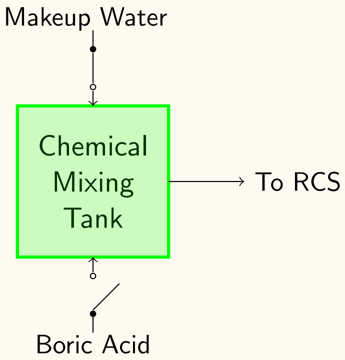


Corrective Action: Boron Level



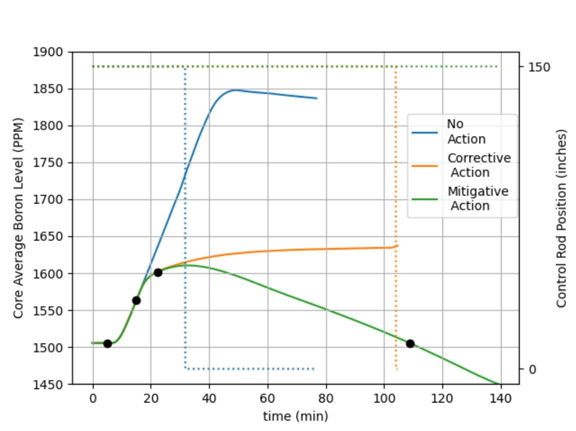
Corrective Action: Core Power

Responsive safeguards

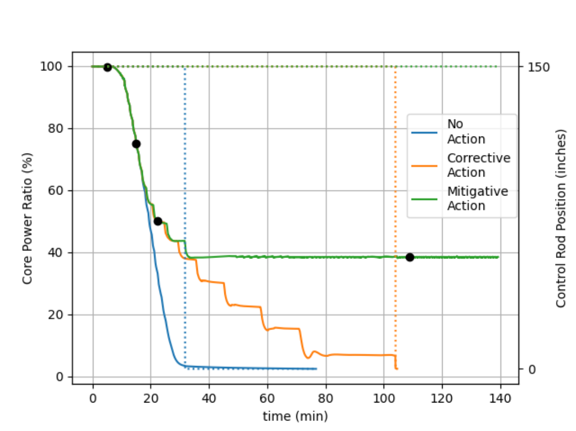


Boron Injection Attack - Mitigation Pathway

Responsive safeguards



Mitigation: Boron Level



Mitigation: Core Power

Final remarks

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

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. This is in essence the **paragon** of cyber-informed design

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. This is in essence the **paragon** of cyber-informed design
- The methodologies adopted for the cyberattacks to be conducted use abnormal conditions that are in scope for the simulator only

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. This is in essence the **paragon** of cyber-informed design
- 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

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. This is in essence the **paragon** of cyber-informed design
- 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

Future work

- Testing additional plant systems for vulnerabilities applying the methodology presented here. Systems will include the used fuel pool and switchyard

Future work

- Testing additional plant systems for vulnerabilities applying the methodology presented here. Systems will include the used fuel pool and switchyard
- Simulate additional DoS and MiTM cyberattacks on these systems

Future work

- Testing additional plant systems for vulnerabilities applying the methodology presented here. Systems will include the used fuel pool and switchyard
- Simulate additional DoS and MiTM cyberattacks on these systems
- Identify data transmission related to the operator display and create spoofed values

Future work

- Testing additional plant systems for vulnerabilities applying the methodology presented here. Systems will include the used fuel pool and switchyard
- Simulate additional DoS and MiTM cyberattacks on these systems
- Identify data transmission related to the operator display and create spoofed values
- Determine the data needed to provide to operators and plant personnel indicative of these cyberattacks

Future work

- Testing additional plant systems for vulnerabilities applying the methodology presented here. Systems will include the used fuel pool and switchyard
- Simulate additional DoS and MiTM cyberattacks on these systems
- Identify data transmission related to the operator display and create spoofed values
- Determine the data needed to provide to operators and plant personnel indicative of these cyberattacks
- Design displays and data visualization tools on the WSC platform to this end

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.