INL/EXP-22-68382-Revision-0

Cyberattack Scenarios for the Rancor Microworld Simulator

August 2022

Georgios Michail Makrakis

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXP-22-68382-Revision-0

Cyberattack Scenarios for the Rancor Microworld Simulator

Georgios Michail Makrakis

August 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cyberattack Scenarios for the Rancor Microworld Simulator

Development of capabilities that allows testing realistic cyber attack scenarios using a simplified nuclear power plant simulator

Abstract

The digitization of new generation nuclear power plants increases the risk of cyber-physical attacks. Hence, the collection of data from operators that respond to realistic cyberattacks can provide a paramount insight on the correlation of cyber evidence and physical alerts. The simplicity and configurability of the Rancor Microworld Simulator [1], enables the training of non-expert operators in a PWR environment, and the extensive and tailored collection of data. Therefore, we develop the necessary tools and infrastructure in Rancor that allow such attacks to take place. Additionally, we perform these attacks to examine the attention and situation awareness of operators during malicious infiltrations.

Steps to Achieve Goal

- Design and development of networking capabilities.
- Identification of PWR subsystems that can inflict disturbances to the plant.
- Development of truthful attacks.
- Creation of an operator-friendly Detection Engine.
- Setup of infrastructure for pilot and full-scale studies.

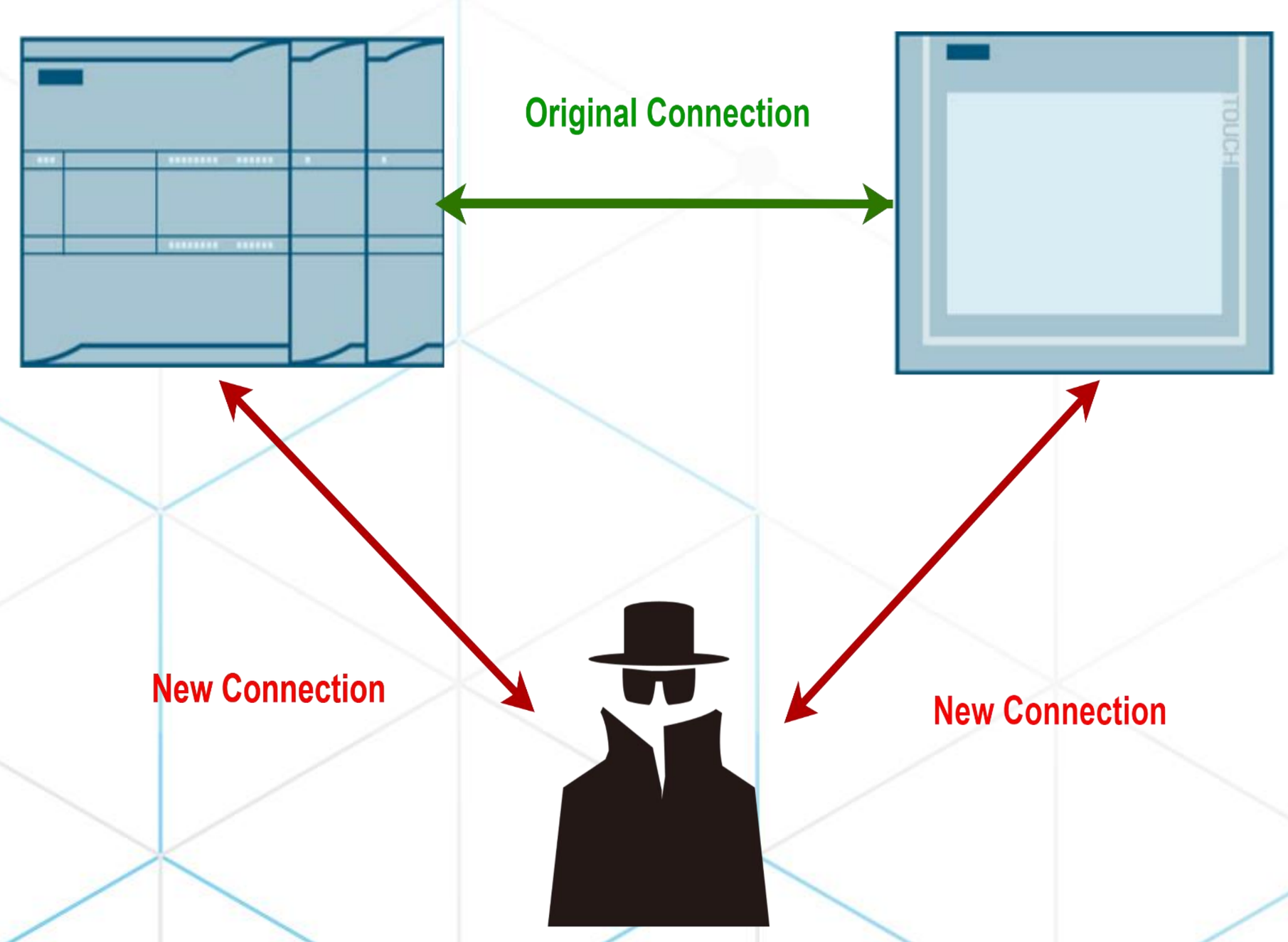
Modbus Communication

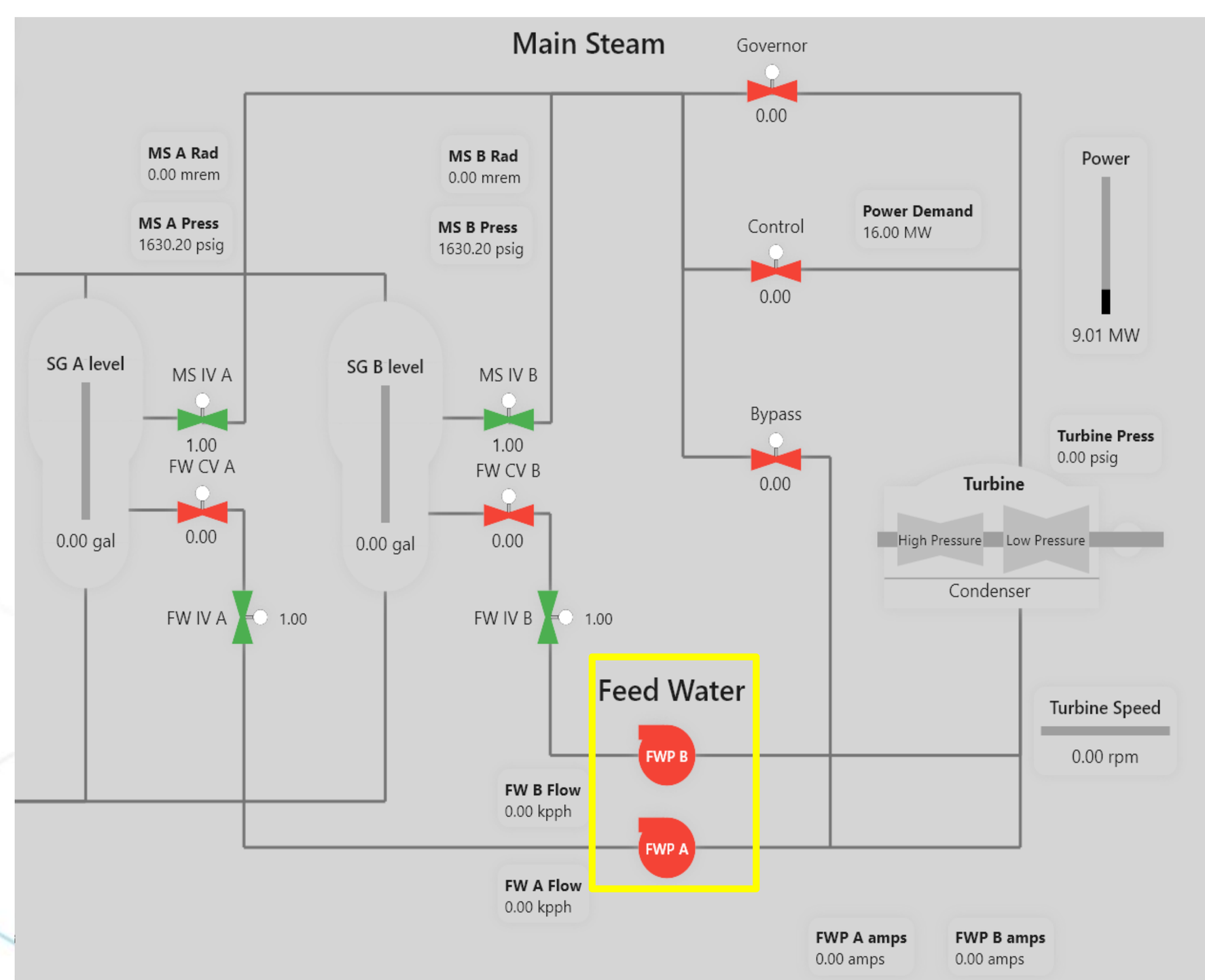
- Creation of Modbus server module for Dart.
- Integration of Modbus communication.
- Components (pumps, valves etc.) can have cyber equivalents.
- Mimicking the communication of PLCs that control such equipment.

Modbus + Dart

Attacks

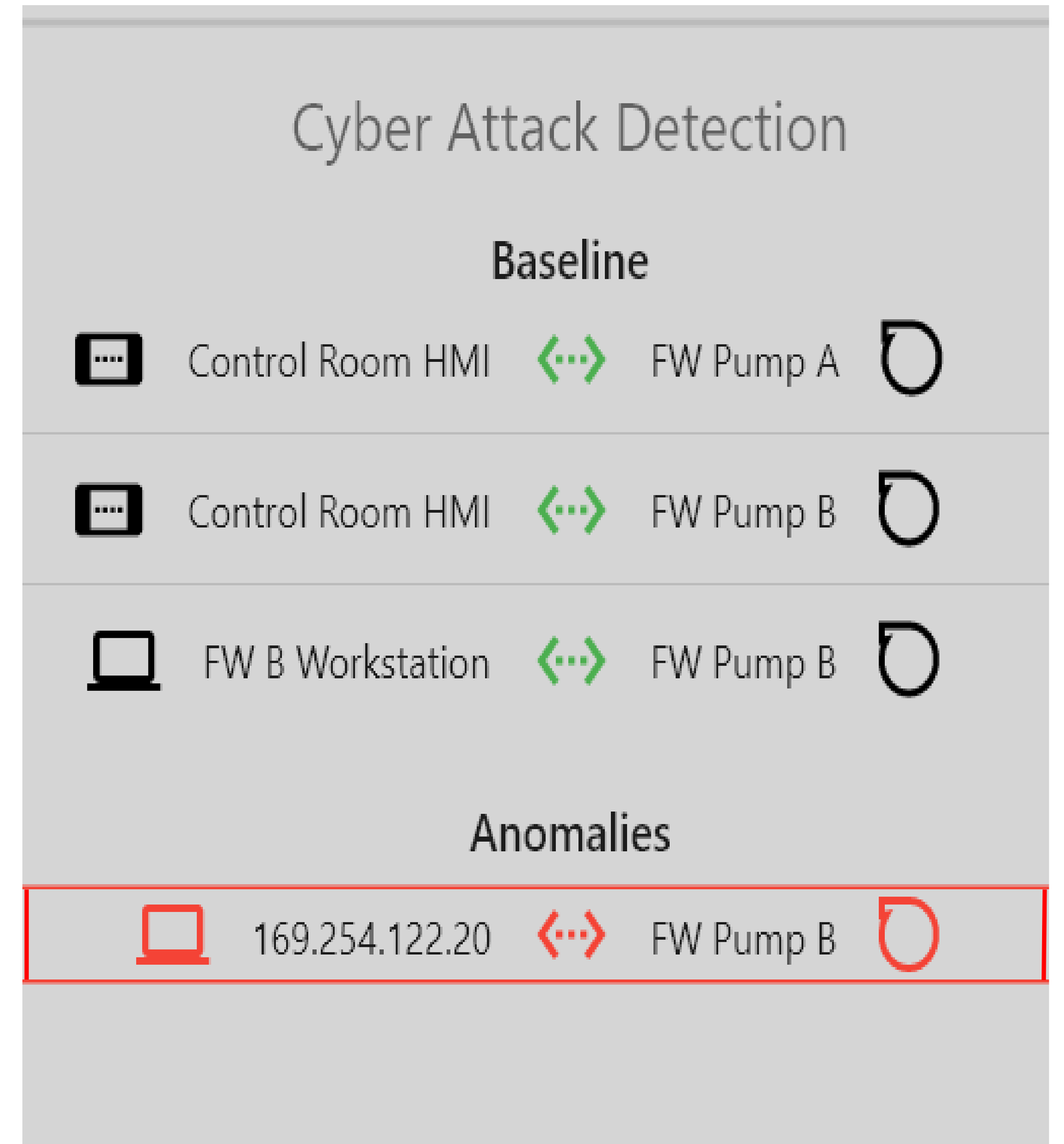
- Development tools for automatic mounting of attacks.
- Spoofing of HMI view and manipulation of parameters.
- Use of "time-bomb" enabled logic.





Situation Awareness Study

- Joined study between UoI and INL in Fall 2022.
- Investigate the participated operators' responses in terms of the power plant recovery actions with regards to the consultation of the Detection Engine and Computer-based Procedures.
- Can the operators distinguish between regular faults and cyber incidents?



References

[1] R. Lew, T. A. Ulrich, R. L. Boring and S. Werner, "Applications of the rancor microworld nuclear power plant simulator," 2017 Resilience Week (RWS), 2017, pp. 143-149, doi: 10.1109/RWEEK.2017.8088663.

[2] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," in IEEE Access, vol. 9, pp. 165295-165325, 2021, doi: 10.1109/ACCESS.2021.3133348.

www.inl.gov

Georgios Michail Makrakis, Control Systems Cybersecurity Intern, Human Factors & Reliability Department

Mentor: Ronald L. Boring, Human Factors & Reliability Department

Collaborators: Timothy A. Whiting, Jinding Xing, Thomas A. Ulrich, Roger Lew

University of Idaho · NEUP Nuclear Energy University Programs · U.S. Department of Energy · INL Idaho National Laboratory