CRADA/NFE-19-07641
CRADA FINAL REPORT

Assessment of the High Flux Isotope Reactor Cybersecurity Initiative

Kevin Shaw

April 2021

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

Research Reactors Division

ASSESSMENT OF THE HIGH FLUX ISOTOPE REACTOR (HFIR) CYBERSECURITY INITIATIVE

Kevin L. Shaw, Oak Ridge National Laboratory
Donald G. Raby II, Oak Ridge National Laboratory
James M. Smith, Oak Ridge National Laboratory
Michael T. Lane, Oak Ridge National Laboratory
Askin Guler Yigitoglu, Oak Ridge National Laboratory

April 2021

Prepared by
OAK RIDGE NATIONAL LABORATORY
P.O. Box 2008
Oak Ridge, Tennessee 37831-6285
managed by
UT-Battelle, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS, ACRONYMS, and INITIALISMS

DOE	Department of Energy
DCS	Distributed Control System
DT	Digital Twin
GAIN	Gateway for Accelerated Innovation in Nuclear
HFIR	High Flux Isotope Reactor
HMI	Human-Machine Interface
IP	Internet Protocol
LAN	Local Area Network
ORNL	Oak Ridge National Laboratory
PCAP	Packet Capture
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol/Internet Protocol

ACKNOWLEDGMENTS

Support for this work was provided by the US Department of Energy, Office of Nuclear Energy Gateway for Accelerated Innovation in Nuclear, Nuclear Energy Voucher program.

1. INTRODUCTION

Recent cyber-attacks on industrial control systems, and inadvertent exposure of nuclear plant systems to cyber-exploits underscore the need for plant operators to adopt and deploy cyber-security defense solutions made for industrial control systems. Of increasing concern is the fact that international cyber hackers are beginning to target critical infrastructure, and because these more modern controls systems depend on advanced use of digital systems, they are more vulnerable than ever before to cyber-attacks. Traditional cyber defense strategies and products that have been available for decades are tailored for use on IT or corporate networks but can cause interruptions and catastrophic damage when deployed on industrial control system networks.

The Department of Energy (DOE) Office of Nuclear Energy established the Gateway for Accelerated Innovation in Nuclear (GAIN) program to provide private companies pursuing innovative nuclear energy technologies with access to the technical support necessary to move toward commercialization.[1]

One of these GAIN small business vouchers was awarded to Dragos, Inc. to enable collaboration with Oak Ridge National Laboratory (ORNL) to evaluate the Dragos Platform on a production nuclear reactor test bed, hence laying the path for future commercial adoption. The vision was to provide a guide for industrial operators on implementing an industrial monitoring solution and to show how these solutions can be deployed without causing safety and reliability issues.

This report documents the results of the collaboration between ORNL and Dragos, Inc.

2. FACILITY DESCRIPTION

The High Flux Isotope Reactor (HFIR) shown at the center of Figure 1, at Oak Ridge National Laboratory, is a light-water cooled and moderated research reactor that began full-power operations in 1966 at the design power level of 100 megawatts. Currently, HFIR operates at 85 megawatts to provide state-of-the-art facilities for neutron scattering, materials irradiation, and neutron activation analysis and is the world's leading source of elements heavier than plutonium for research, medicine, and industrial applications.

Figure 1. HFIR Site

The neutron-scattering instruments installed on the four horizontal beam tubes are used in fundamental studies of materials of interest to solid-state physicists, chemists, biologists, polymer scientists, and materials scientists. Recently, a number of improvements at HFIR have increased its neutron scattering capabilities to 14 state-of-the-art neutron scattering instruments. These upgrades include the installation of larger beam tubes and shutters, a high-performance liquid hydrogen cold source, and a cold-neutron guide system. The installation of the cold source provides beams of cold neutrons for scattering research that are as bright as any in the world. Use of these forefront instruments by researchers from universities, industries, and government laboratories are granted on the basis of scientific merit.

2.1 HIGH FLUX ISOTOPE REACTOR

HFIR is a beryllium-reflected, light-water-cooled and -moderated, flux-trap type reactor that uses highly enriched uranium-235 as the fuel. The preliminary conceptual design of the reactor was based on the "flux trap" principle, in which the reactor core consists of an annular region of fuel surrounding an unfueled moderating region or "island." Such a configuration permits fast neutrons leaking from the fuel to be moderated in the island and thus produces a region of very high thermal-neutron flux at the center of the island. This reservoir of thermalized neutrons is "trapped" within the reactor, making it available for isotope production. The large flux of neutrons in the reflector outside the fuel of such a reactor may be tapped by extending empty "beam" tubes into the reflector, thus allowing neutrons to be beamed into experiments outside the reactor shielding. Finally, a variety of holes in the reflector may be provided in which to irradiate materials for experiments or isotope production.

The original mission of HFIR was the production of transplutonium isotopes. However, the original designers included many other experiment facilities, and several others have been added since then. Experiment facilities available include (1) four horizontal beam tubes, which originate in the beryllium reflector; (2) the hydraulic tube irradiation facility, located in the very high flux region of the flux trap, which allows for insertion and removal of samples while the reactor is operating; (3) thirty target positions in the flux trap, which normally contain transplutonium production rods but which can be used for the irradiation of other experiments (two of these positions can accommodate instrumented targets); (4) six peripheral target positions located at the outer edge of the flux trap; (5) numerous vertical irradiation facilities of various sizes located throughout the beryllium reflector; (6) two pneumatic tube facilities in the beryllium reflector, which allow for insertion and removal of samples while the reactor is operating for neutron activation analysis; and (7) two slant access facilities, called "engineering facilities," located on the outer edge of the beryllium reflector. In addition, spent fuel assemblies are used to provide a gamma irradiation facility in the reactor pool.

2.2 COLD NEUTRON SOURCE

The HFIR was modified in 2006 to add the capability to produce cold neutrons for research. The cryogenic hydrogen lines and support systems building are shown in Figure 2.

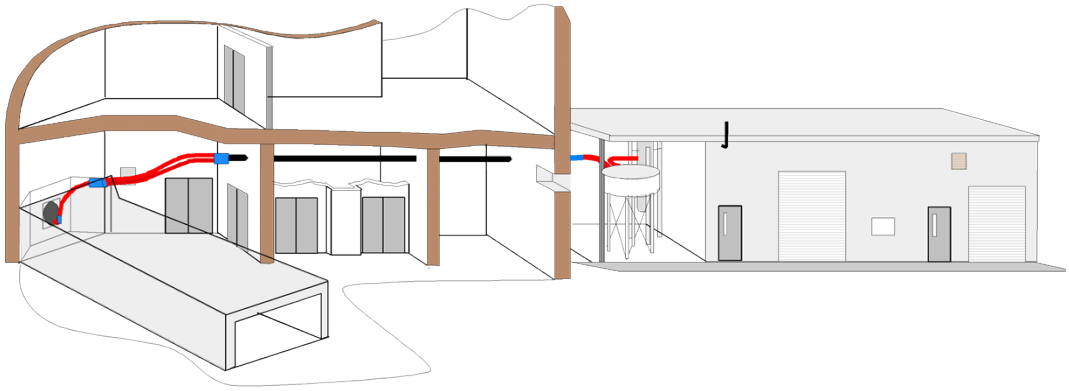

Figure 2. HFIR Cold Neutron Source

With a world-wide demand for increased capabilities to perform research using cold neutrons, the Cold Source was designed to circulate supercritical hydrogen pressurized to 14 bar absolute at temperatures between 14-24°K at a rate of approximately one liter per second through a moderator vessel installed inside the HB-4 beam tube of the HFIR (See Figure 3).

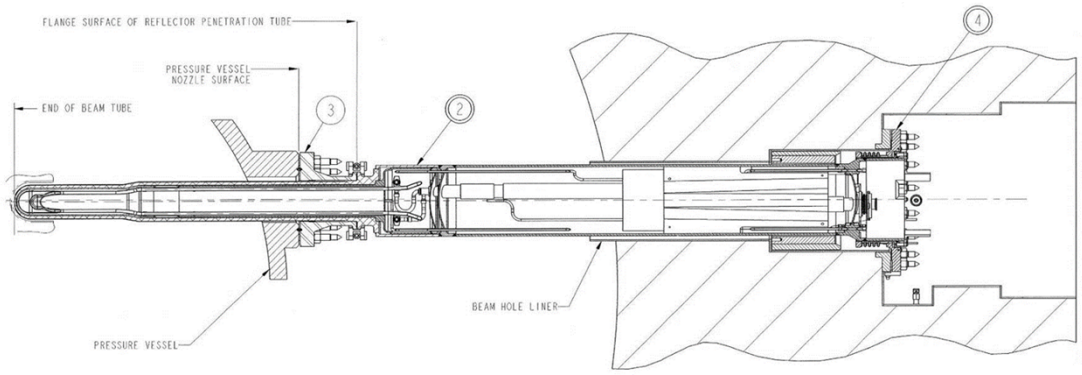

Figure 3. HFIR Beam Tube

The hydrogen cools neutrons emitted from the reactor core causing enhanced production of 4-12 angstrom neutrons which are ideal for significant research applications. The neutrons are conveyed outside of the beam tube using wave guides which terminate in a dedicated cold neutron guide hall constructed next to the HFIR reactor building (Figure 4).

Figure 4. Cold Guide Hall

The hydrogen is cooled by helium. Helium compressors (Figure 5) circulate the helium through the heat exchanger module to the cold box heat exchanger.

Figure 5. Helium Compressors

The helium is cooled with liquid nitrogen in the cold box heat exchanger then flows to the expansion engines. Gas performs work on the engine by forcing pistons to reciprocate inside of cylinders, this work cools the gas. The heat exchanger and expansion engines are considered to be the helium refrigerator (Figure 6).

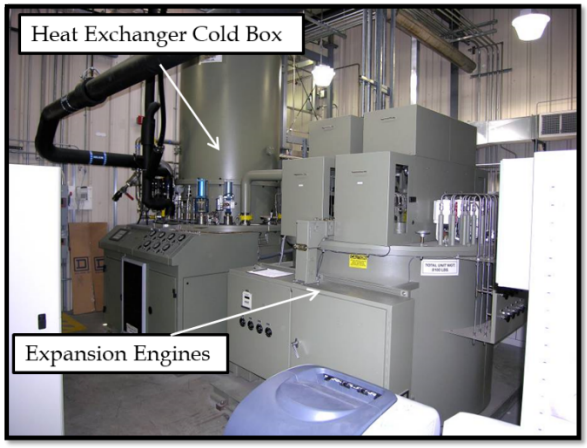

Figure 6. Helium Refrigerator

The hydrogen loop must be carefully monitored to assure pressure, flow, and temperature remain at desired conditions. This function is handled by the control system. The pressurization system is utilized to control pressure of the hydrogen loop at the established set point. The control system also controls loop temperature and minimizes control challenges to refrigerator operation by applying appropriate power to the electrical heaters in the helium refrigeration loop.

The cold source systems are controlled and monitored with a Distributed Control System (DCS). The DCS is comprised of a collection of PLCs, computers, Human Machine Interfaces (HMI), controllers, and network switches. The purpose of the system is to provide real time Supervisory Control and Data Acquisition (SCADA). It monitors plant status and communicates information to the staff, accepts operator commands, activates alarms, and controls plant equipment either automatically or based on staff inputs.

The network switches are inter-connected via an Ethernet Local Area Network (LAN) in a ring configuration to allow for alternate routing in the event of a partial network failure. Each has a unique Internet Protocol (IP) address on the network. There are various switches located through-out the reactor and cold source buildings and the network is expandable to meet future needs. Three of the network switches are attached to PLC's (referred to as nodes). Each node performs a specific set of functions. The fourth switch is connected to the SCADA servers.

Figure 7 shows the main HMIs at the main operator control station. Supervisory control and data acquisition, along with historical archiving, takes place in the servers located in the SCADA cabinet (Figure 8).

Figure 7. Operator Station

Figure 8. DCS SCADA Cabinet

2.3 NETWORK MONITORING SOFTWARE

The Dragos Platform provides asset discovery, threat detection, and reporting capabilities for the DCS and DT. Hardware consists of Midpoint Sensors, which are pre-built appliances used to collect the network traffic from connected switches, and SiteStore Servers, which manage the midpoint sensors and provide the user interface to the sensors.

Asset discovery passively identifies all assets and communications on the network. With this information, the platform creates a map of the network that is accurate, up-to-date, and thorough. New or rogue assets are identified as they appear, as well as assets that have disappeared from the network. Users have the ability to set baselines and to be notified when specific changes or anomalies occur in the environment over time.

The Dragos Threat Detection behavior analytics provides rich context as to what is occurring by collecting, storing, and analyzing logs and data from host systems, logic controllers, and data historians.

3. RESULTS

The following sections discuss the results of this effort.

3.1 DISTRIBUTED CONTROL SYSTEM NETWORK

The first task of this project focused on characterizing the network architecture for the HFIR Cold Source Facility. Understanding this architecture allowed for the development of a monitoring strategy to understand normal network traffic patterns. The Dragos Platform provided the visibility into this cyber-physical network.

The Dragos Platform consisted of the following components:

- Midpoint Sensors – sensors connected to the network switches to capture network traffic
- Sitestore – server which deciphers/decodes the metadata collected by the sensors

The team was able to identify assets and build a holistic view of the cold source control system in a passive manner. The result was both a full list of assets as well as a virtual rendering of the network for normal operation of the control system.

Using the Dragos Platform utilities, deep packet inspection of the traffic resulted in the development of a detailed asset list and a graphical interactive map of the assets (See Figure 9).

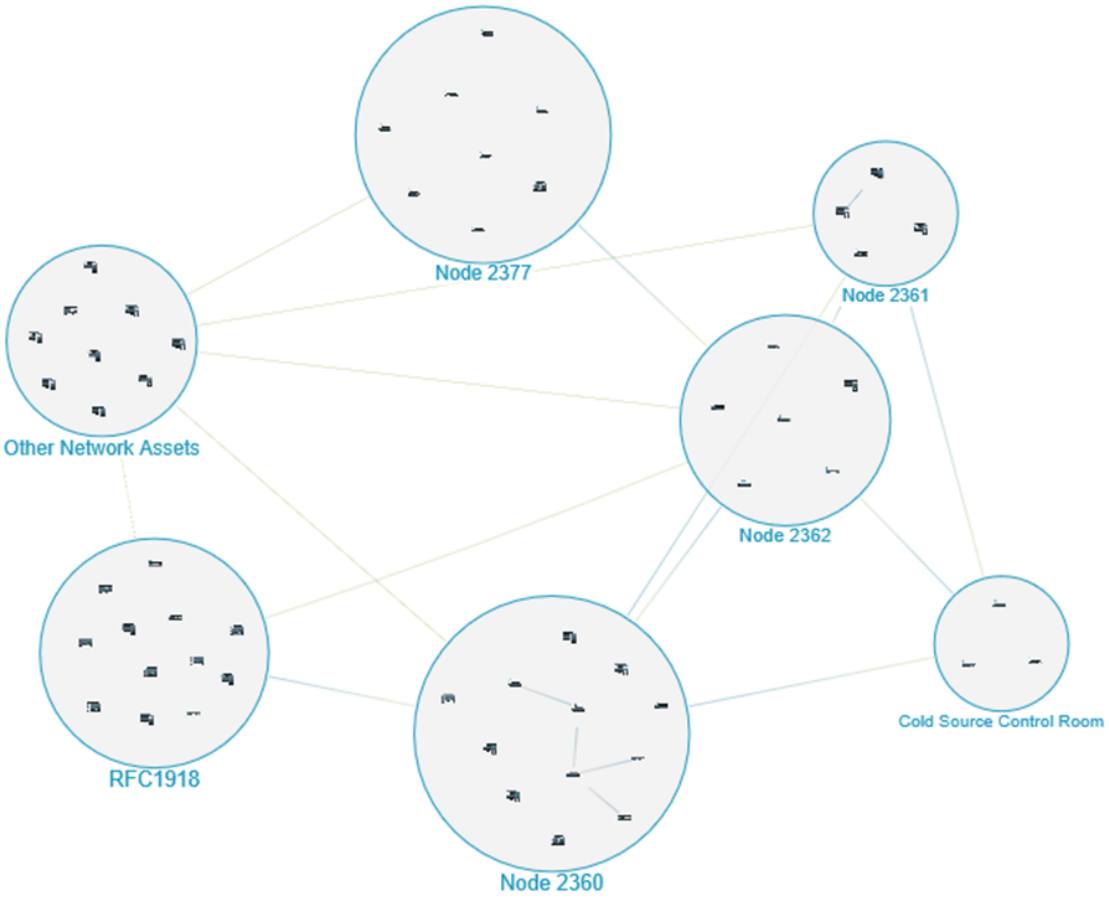

Figure 9. DCS Asset Map

3.2 DIGITAL TWIN NETWORK

The second task for this project involved the development of a Digital Twin (DT) of the cold source network in order to analyze communications and introduce faults to characterize abnormal traffic and establish a test bed for investigation of cyber-physical threats.

A DT, for the purposes of this research, has been defined as a realistic representation of an operating industrial control system, where sensory data can be combined with historical data to provide a test bed for cyber security testing and research.

The DT in the HFIR Software Engineering Lab was assembled to replicate a small subset of the Cold Source DCS, providing a mechanism for re-playing process data to allow for network monitoring of the traffic exchanged between the components.

The DT is comprised of a collection of PLC's, computers, HMI's, controllers, and network switches as listed in Table 1 and identified in Figure 10.

Table 1. DT Asset List

Item	Description	Device Name
1	PLC/Controller	YC-2235
2	PLC/Controller	YC-2237
3	Cold Source View Node	CSView6
4	Network Managed Switch	YT-2362
5	Network Managed Switch	YT-2360
6	Network Managed Switch	YT-2377
7	Cold Source SCADA Server	SCADA1
8	Cold Source Historian Server	CSSERVER

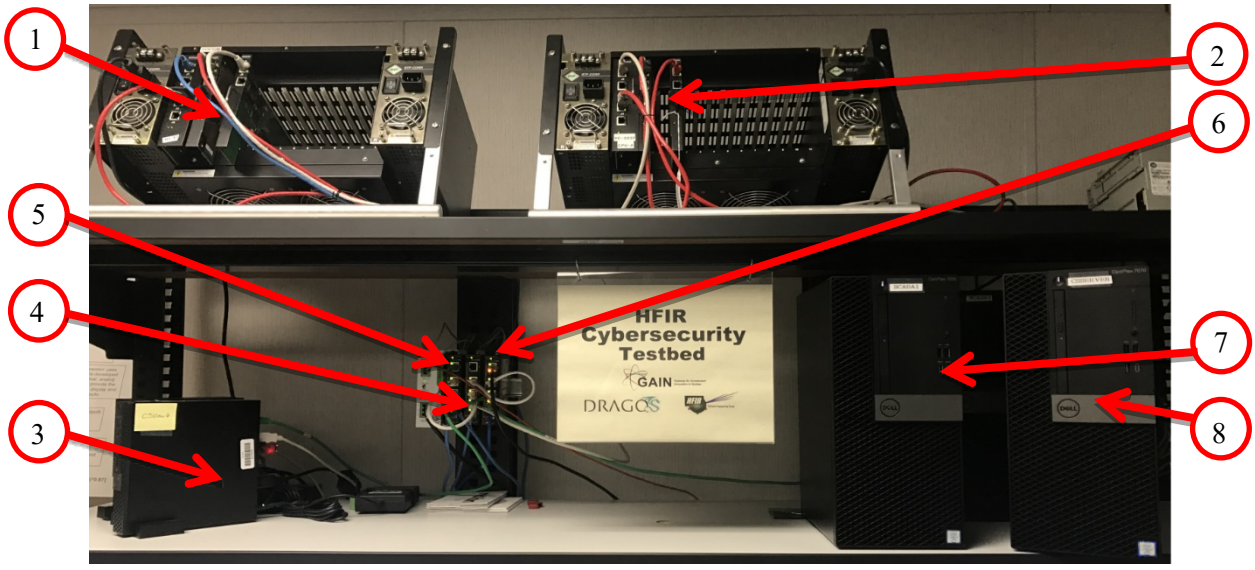

Figure 10. Digital Twin Components

3.2.1 Components

Programmable Logic Controllers

The PLC nodes are the interface between the electronic system and the field devices. The input and output cards of the PLC convert electrical signals to digital data and vice-versa. The PLCs also contain the process programming which controls devices based on staff requests (received from the HMIs) or programmed algorithms.

To operate the DT, a simulator PLC processes recorded historical values and "replays" the values according to their associated timestamp to simulate field devices. The digital data received from field devices (via the simulation PLC) is processed by the node PLC's. Any automatic output actions required, based on the node PLC's programming, is directed to an applicable output card. The PLC's register updates the new configuration of the output card. The new configuration is read by the SCADA computer and the HMI updates appropriately. These actions are communicated through the managed network switches, which are monitored by the Dragos Platform.

Human-Machine Interface (HMI)

The HMI's provide the informational displays to the staff and are the personnel interface to the control system. The staff utilizes touch screen panels to input commands, which are processed and relayed to the appropriate output device. HMI software is used to interface between the PLC and the CS Staff. Touch screen displays inform/provide the following:

- Provide CS process values (flows, temps, pressures, etc)
- Provide CS process equipment status
- Indicate CS operating modes
- Indicate control system hardware status
- Provide Annunciation/alarms
- Provide trending information

Servers

Two SCADA computers and an historian server provide support functions for the system including centralized data storage and back-up functions. SCADA control of the DT is maintained by a primary and a secondary server with HMI software. Historian software is utilized to provide data collection and archiving.

Network Switches

The network switches are inter-connected via an Ethernet LAN in a ring configuration to allow for alternate routing in the event of a partial network failure. Each has a unique IP address on the network. One switch represents a PLC node and one switch represents the SCADA node.

3.2.2 Architecture

The physical architecture is shown in Figure 11 below. It has been setup to mimic the architecture of the actual DCS.

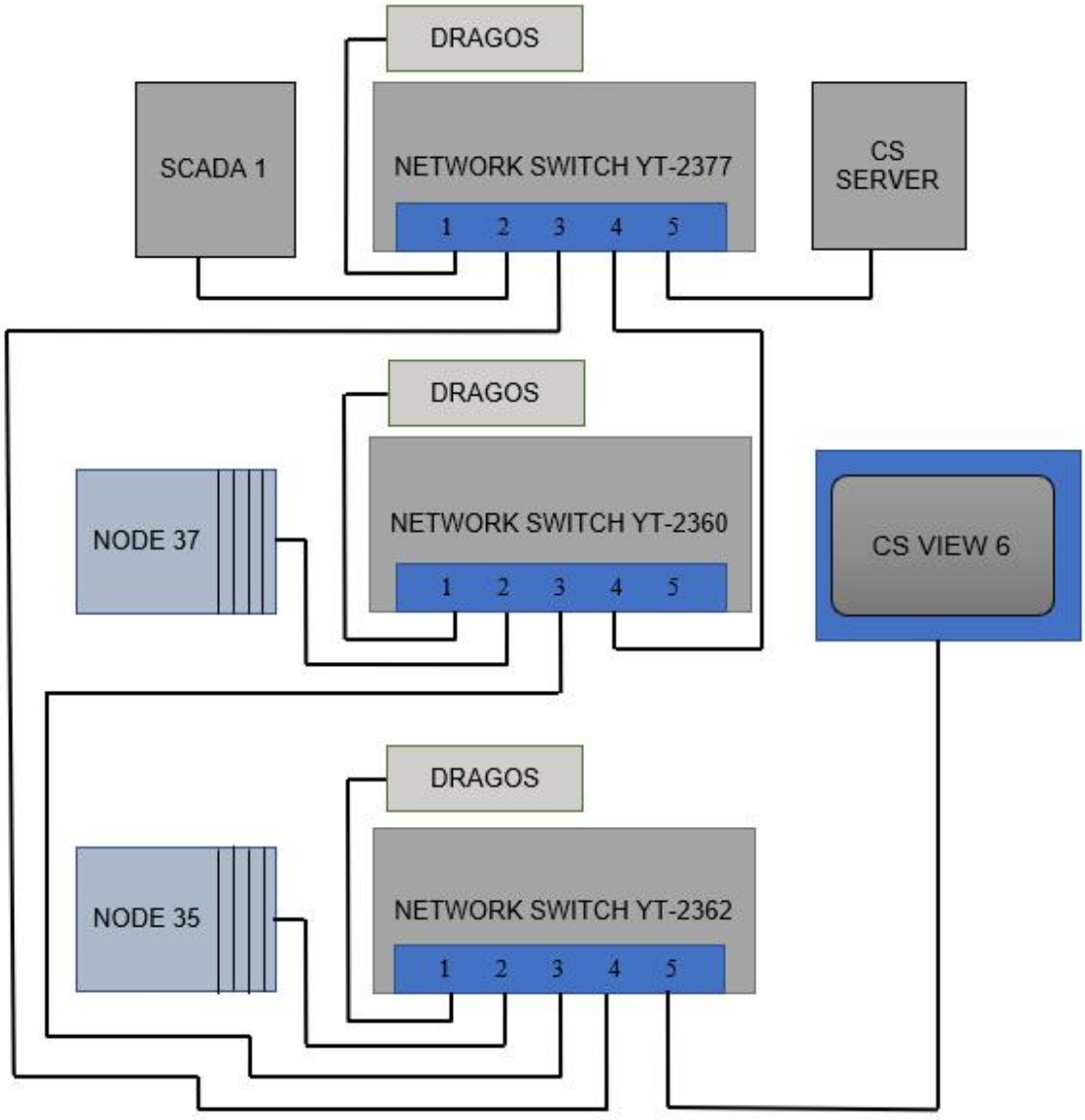

Figure 11. Digital Twin Physical Architecture

The Dragos Platform was used to perform a deep packet inspection of the communications (network traffic) between the assets. From this inspection it created a graphical "Interactive Map" representing the system assets listed above. Figure 12 is the actual interactive map.

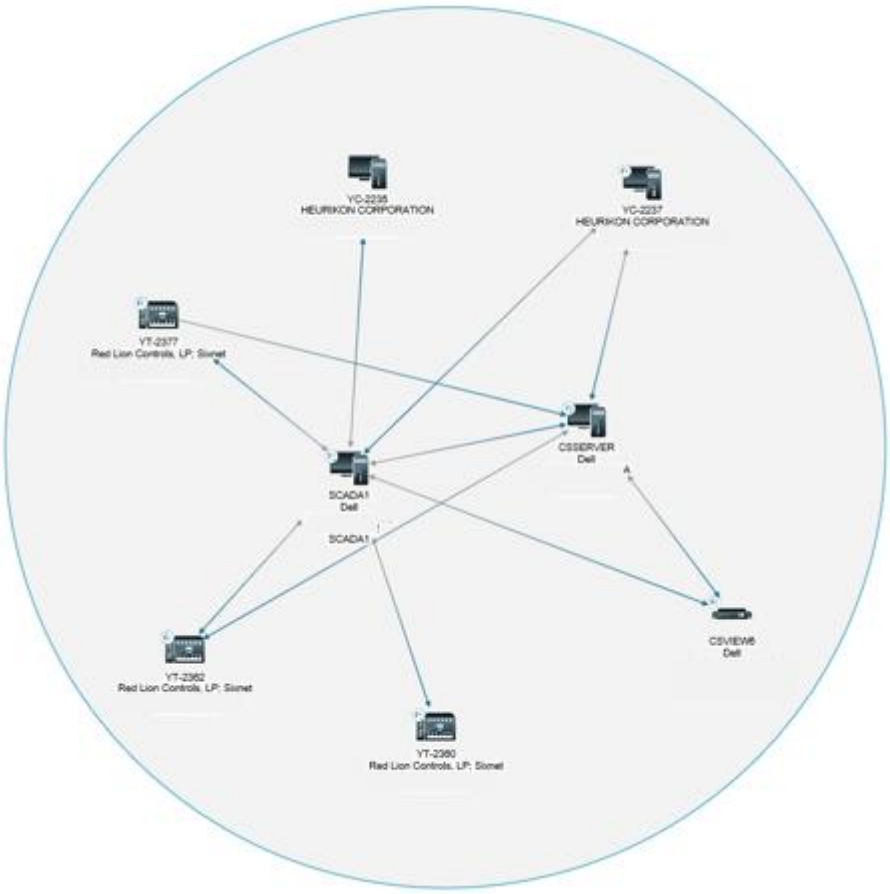

Figure 12. Digital Twin Asset Map

Each of the assets in the map (Figure 12) shows the following information:

- Device Tag Name (assigned)
- Device Manufacturer
- Device MAC Address
- Device IP Address (blacked out for cybersecurity)
- Device Host Name (listed only for computer assets

The lines between the assets on the map represent the communications between assets. This does not necessarily represent the exact physical connections (i.e. – point-to-point) between the assets/devices rather, it simply indicates with which other devices an asset communicates.

The Dragos Platform also displays the assets correctly in tabular form. Table 2 shows an actual Assets List of the DT.

Table 2. Digital Twin Asset List

Asset	Type	Vendor	MAC	IP	Hostname
23	SCADA Server	----------	REDACTED	REDACTED	CSSERVER
19	Historian	----------	REDACTED	REDACTED	SCADA1
27	HMI	----------	REDACTED	REDACTED	CSVIEW6
21	Industrial Switch	----------	REDACTED	REDACTED	
29	Industrial Switch	----------	REDACTED	REDACTED	
25	Industrial Switch	----------	REDACTED	REDACTED	
17	PLC	----------	REDACTED	REDACTED	
31	PLC	----------	REDACTED	REDACTED	

Comparing the list in Table 2 to the information in Table 1, it can be seen that the Dragos System has accurately identified and represented the DT system and its network.

Using both the Dragos Platform on both the DT and the DCS, TCP/IP packet captures (i.e. – PCAPs) were performed.

- A PCAP of the DCS was performed on all network traffic on 3/11/21, from 08:41 AM to 08:46 AM
- The process data for the DCS was obtained for this date/time interval for a select number of process points from the historical archive
- The historical process data was “replayed” through the DT system while the Dragos Platform performed a PCAP on the network traffic
- The raw data content (in hexadecimal format) which is encapsulated in the TCP/IP data packets of these PCAPs was extracted for both the DCS and the DT and placed side-by-side for comparison (see Figure 13)

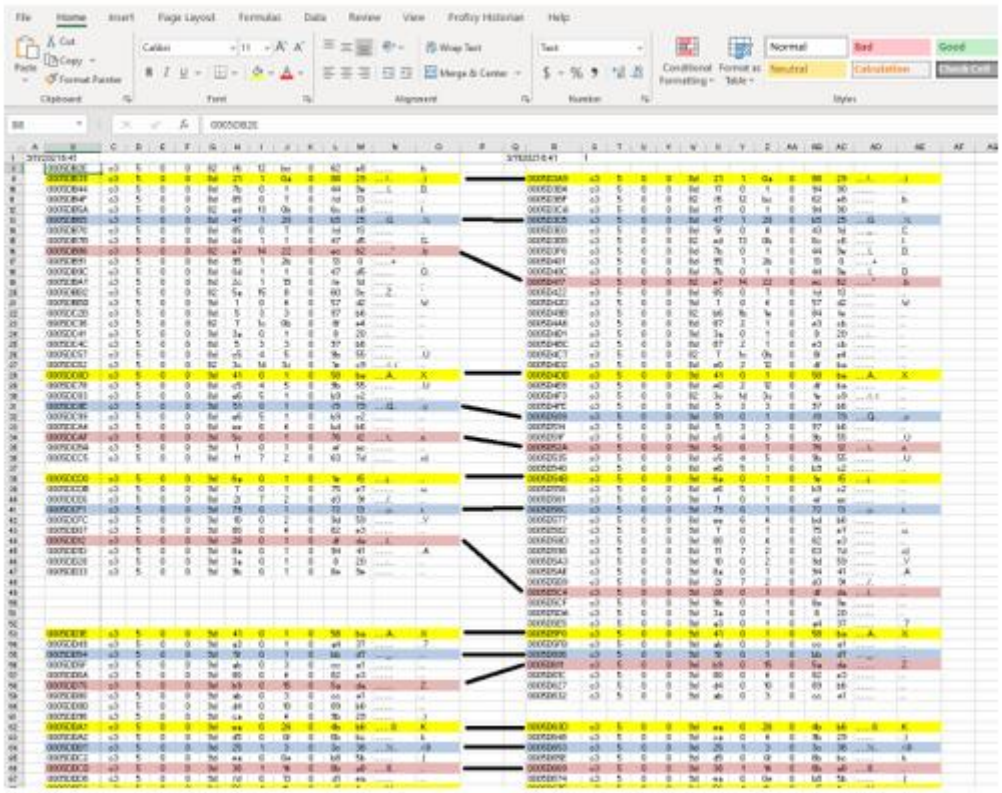

Figure 13. PCAP Data Comparison

In Figure 13, the left half represents raw data captured from the DCS and the right half represents data captured from the DT. Note the lines drawn between matching data packets indicating similarity between the process data seen moving through the network switches during the approximately same date/time interval.

The raw data content obtained from both systems showed similar data patterns. The similarities are expected because the same process values were present in both systems during the above date/time interval. They are not expected to match exactly because the DT, during this time interval, only contained a small subset of process values.

Whereas the two patterns do not match exactly, this pattern clearly establishes the capability of the DT to realistically represent the operating industrial control system (DCS).

3.3 DYNAMIC PROBABILITY RISK ASSESSMENT

Increased use of digital technologies in nuclear facilities, to improve operations, also introduces cyber risk vulnerabilities. Malicious activities could attempt to shut down, cause failure of components, or introduce false indications to the operator control screens, among other interventions of safety functions. Therefore, protection and mitigation from cyber-attacks has been one of the key issues in digitalized nuclear facilities, to assure safety functions are not comprised.

Dynamic event tree (DET) methodology is being used to address and analyze potential cyber vulnerabilities in the cold source using ADAPT software. The HFIR cyber security testbed, a digital twin of the cold source, was established with our collaborator Dragos as a baseline of the operating system and it monitors the network for intrusions. The HFIR safety analysis report probabilistically examines cold source event sequences that could be considered design basis accidents, such as a release of hydrogen to the building. Probabilistic risk assessment models are being used to screen critical components, actions and events to be modelled as cyber-attacks simulated with the digital twin.

The DETs are being coupled with the digital twin to capture cyber-attacks (cyber initiated events) and their potential consequences on the system with possible recovery actions. This study is the first real application of a DET for an operating facility and is a test-bed demonstration of nuclear cyber-physical systems.

Unfortunately, the digital twin setup took longer than expected and little time was available to be devoted to the DET methodology. However, this methodology used in concert with the cyber security testbed holds great promise for future analysis.

3.4 CONTROL SYSTEM OPTIMIZATION

It was a goal to identify optimum mitigation/supervisory control strategies to maintain full/limited operations if possible, or safe state for quarantining and mitigating threats. Specifically, we hoped to leverage previous supervisory control work to identify control strategies for the cold source that include the potential for cyber threat detection.

There has been much written about mitigation/prevention strategies for control systems. Common recommendations include:

- Use of Air-Gaps
- Whitelisting
- Segmentation/Access Controls
- Continuous Incident Detection

Unfortunately, the digital twin setup took longer than expected and little time was available to be devoted to detecting small disturbances or anomalies in expected performance for traffic models. Use of such techniques as "hashcode" or "parity check" comparisons between the plant and digital twin systems hold promising potential for cyber threat detection.

4. SUMMARY AND CONCLUSIONS

Cybersecurity is a major concern within the research and power reactor community. This project, using an ORNL-based, open science research reactor with ready access to reactor operating data, has highlighted the flexibility and possibilities of leading the efforts into cybersecurity defense.

This project focused on the identification and mitigation of cyber-physical attacks on industrial control systems. In-depth analysis of network traffic related to actual operating data and system performance is yet to be completed. Additional operational and cyber-system analyses would help build a stronger defense for reactor security and overall safety.

Although preliminary work has been performed in building and proving the Digital Twin concept, future efforts to fully utilize the DT should be pursued. Initial analysis of the network traffic may be extended to include analysis of specific network packets for the purpose of artificial intelligence (AI) learning. An investigative study into the baselining of sensor data, correlated with environmental data and reactor operating states should be performed.

In the near term, HFIR will continue to improve its understanding of the testbed's capabilities and develop relationships with commercial vendors who may consider partnering with ORNL to improve their cybersecurity product. In the long term, HFIR aims to expand the cybersecurity testbed to further investigate cyber-physical threats and dynamic probabilistic risk assessment. This in turn will allow the development of future technologies and strategies that will defend the nuclear industry against the current cyberattacks threatening our nation.

5. REFERENCES

1. US Department of Energy, "Gateway for Accelerated Innovation in Nuclear," http://energy.gov/technologytransitions/gateway-accelerated-innovation-nuclear
2. Research Reactors Division, HFIR System Description 601.74, Rev. 4, July 2018.