Pacific Northwest
NATIONAL LABORATORY

Nuclear Energy Cyber Security Capabilities and Technology

March 2021

PNNL-31029

U.S. DEPARTMENT OF
ENERGY

Acronyms and Abbreviations

C2M2	Cybersecurity Capability Maturity Models
CRISP	Cybersecurity Risk Information Sharing Program
EIOC	Electricity Infrastructure Operations Center
IIOT	Industrial Internet of Things
IOT	Internet of Things
IT	Information Technology
MEEDS	Mitigation of Externally Exposed Energy Delivery Systems
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NIST	National Institute of Standards and Technology
OT	Operational Technology
PACRAT	Physical and Cyber Risk Assessment Tool
SSASS-E	Safe Secure Autonomous Scanning Solution for Energy Delivery Systems
RMF	Risk Management Framework
VARS	Verification and Validation Assuring Reliability and Security

Contents

Figures

1.0 Introduction

Nuclear power plants (NPPs) and facilities that handle nuclear materials are potential targets for cyber adversaries determined to sabotage the systems and facilities supporting nuclear fuel and nuclear materials. Structures, systems, and components built to protect facilities, nuclear fuel, and nuclear materials are also targets since they prevent and mitigate uncontrolled radiological events or loss of nuclear information or materials. For more than two decades, Pacific Northwest National Laboratory (PNNL) has advanced resilient cyber capabilities to thwart adversaries seeking to infiltrate and damage our national security through digital means. PNNL has established enduring partnerships with government agencies, including the U.S. Department of Homeland Security, Department of Energy (DOE), National Nuclear Security Administration, Department of Defense, Nuclear Regulatory Commission (NRC), the International Atomic Energy Agency, and industry stakeholders, to develop innovative solutions to protect our nation’s critical strategic assets through the performance of research and development in delivering high-impact, "first-of-a-kind" and truly innovative solutions to protect the nation's nuclear assets.

Our extensive cyber security expertise, coupled with advanced domain expertise in assessments, inspections, NPP operations, and policy development, uniquely equips PNNL to address pressing cyber security challenges in cyber-physical systems, industrial control systems, and critical infrastructures within the energy generation sector. Building on $60M plus cyber-related research and development investments to date, PNNL continues to apply its expansive cyber security capabilities, rapidly growing its cyber portfolio and its state-of-the-art cyber research and development facilities to serve critical national security, energy, and environmental missions. To solve our nation’s most difficult problems in innovative ways, PNNL researchers, scientists, engineers, and professionals establish strong multidimensional teams with cyber security architects, information security architects, and domain experts across PNNL’s national security, energy and environment, and fundamental science directorates.

PNNL’s current research and development efforts are focused on understanding, evaluating, and developing trusted and resilient systems for critical infrastructure, such as electricity generated and delivered from commercial NPPs in the continental United States and other renewable energy sources. PNNL understands the importance of proactive research and evaluation of cyber security systems to better defend against adversaries.

2.0 Cyber Security Capability

PNNL develops architectures, methodologies, algorithms, and tools that enable stronger, more resilient technologies and systems that understand, predict, and control complex adaptive systems. PNNL is continuously developing and implementing innovative tools and methods to aid in the discovery and insight of information for greater situational awareness and to ensure that systems can deter, detect, and recover from anomalous activity. To these challenges, we bring expertise in information assurance, computer network defense operations and development, system integration, mission assurance and resilience, assessments and evaluations, software development and the design and deployment of innovative and secure system architectures. The following sections describe cyber security resiliency methods, technologies, and testbed facilities produced by PNNL

2.1 Cyber Security Resiliency Methods

PNNL researchers, scientists and engineers are recognized leaders nationally and internationally in the development of cyber security policies, programs, assessments and training programs that assist organizations in implementing methods to protect facilities, assets, and organizations from cyber threats. These are described below.

2.1.1 Cyber Security Policy and Rulemaking

In response to the terrorist attacks of September 11, 2001, and other intelligence information received from different sources, the NRC issued orders[1] to NPPs to implement interim safeguards and security compensatory measures to address the increased threat environment at the time. Protecting critical digital assets from potential acts of sabotage became a priority. We included cyber-attacks as a part of a design basis threat for NPPs to ensure systems were protected. Cyber security experts from PNNL worked closely with NRC staff to develop interim guidance[2,3] and perform pilot inspections to support development of the current "Cyber Security Rule."[4, 5,6]

[1] NRC Orders EA-02-026, "Interim Safeguards and Security Compensatory Measure for Nuclear Power Plants" and EA-03-086, "Design Basis Threat for Radiological Sabotage"

[2] NUREG/CR-6852, *An Examination of Cyber Security at Several U.S. Nuclear Power Plants*, 2005

[3] NUREG/CR-6847, *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants*, 2004

[4] 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" (Cyber Security Rule) issued March 2009

[5] NUREG/CR-7141, *The US Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors*

[6] Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities*

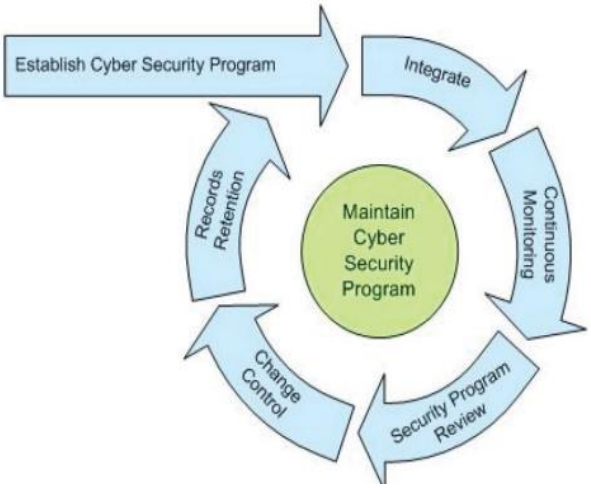

Figure 1. NRC Regulatory Guide 5.71 Security Lifecycle

To assist our nation in securing energy power as a resilient critical infrastructure, PNNL continues to support U.S. government and international agencies, to include the International Atomic Energy Agency and others, in developing cyber security policies and guides throughout the system life cycle (e.g., design, construction, operation, and decommissioning). These guides include, but are not limited to, the following:

- Threat and Vulnerability Analysis
- Cyber Risk Management Frameworks
- Cyber Security Risk Assessments
- Response and Recovery

In addition to providing cyber security policies and guidance documents to support renewable energy sources, such as nuclear, hydropower, marine energy, photovoltaic array, and tidal wind, PNNL assists DOE in securing other critical infrastructure sectors. PNNL has developed policies, contractual language and guides that support the cyber security of commercial facilities, food and agriculture, critical manufacturing, dams, oil and gas industry, and the Federal government to include the Department of Defense. For DoD, PNNL assists in securing military facilities and infrastructure necessary to support energy and water resiliency. PNNL collaborates with industry experts, such as the National Institute of Science and Technology (NIST) in developing methods that follow the NIST Cybersecurity Framework and other guidance documents developed to protect information technology (IT) and operational technology (OT) systems, to include industrial control systems and energy delivery systems.

2.1.2 Training

To ensure our sponsors are equipped with the knowledge and tools to secure their assets from a cyberattack, PNNL continues to develop and provide security training programs. PNNL experts hold international nuclear cyber security training workshops for the DOE Office of

International Nuclear Security, International Atomic Energy Agency, and the State Department Partnership for Nuclear Threat Reduction to address topics such as security awareness, security assessments, security of industrial control systems, security for nuclear and radiological material facilities, and web-based e-Learning. PNNL cyber security experts work closely with NPPs, fuel cycle facilities, regulatory agencies, and nuclear cyber security researchers from around the world, including South Korea, Brazil, Mexico, Romania, and other countries, to develop training programs.

To improve cyber security situational awareness, PNNL has developed highly specialized training by modeling real-world IT and OT enterprise networks. PNNL implements interactive training, testing, and assessment toolkits to assess the security and performance of software, hardware, mobile platforms, and other devices. One of these training tools is the Facility Cybersecurity Framework (FCF) Cybersecurity Training Game.[7]

The FCF Training Game is designed for a spectrum of facility owners and operators. It provides dynamic, game-based cyber security training. Users pick a scenario and are then confronted with a series of real-world cyberattacks on their facility. Cyber security resources that thwart the attack are constrained to mimic real-world limitations. Attacks may affect both IT and OT systems.

2.1.3 Vulnerability Assessments and Threat Analysis Tools

Understanding the cyber security threat landscape for NPPs and nuclear facilities is key in determining the weaknesses in a facility owner's process, procedures, and practices to assess the risks of a cyberattack. Threat modeling is one method to evaluate the risks to different types of cyber threats and develop appropriate mitigating strategies to protect assets from these threats. PNNL maintains extensive capabilities in testing, both static and dynamic, including various software development (and maintenance) offerings refined under the umbrella of Secure Software Central, such as through the completion of Threat Profiles. PNNL develops methods and tools based on insights from known threats and frameworks provided in attack trees, Common Vulnerability Scoring Systems, or STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privileges) models.

The following are methodologies and tools developed by PNNL experts that help validate the acceptability of mitigating strategies and identify opportunities to improve security.

- Physical and Cyber Risk Assessment Tool (PACRAT)

  PACRAT models and analyzes potential attack pathways for a given scenario and demonstrates the possible degradation a cyberattack could have on the physical protection system, including the physical threats to electronic systems. PNNL blends physical- and cyber security assessment processes to assess a facility's ability to protect from four

[7] The FCF Training Game Guide can be accessed at https://facilitycyber.labworks.org/training/trainingGame

potential modes of attacks: physical-only attacks, cyber-only attacks, physical-enabled cyberattacks, and cyber-enabled physical attacks. The scenarios begin in one domain to effect change in the other, and then back outward to take advantage of the reduced system effectiveness before penetrating further into the defenses. PACRAT provides the ability to identify and quantify protection systems in a holistic manner and to thoroughly comprehend the subsystem and component-level interactions and interdependencies that could be exploited by an adversary. PACRAT enables a complete understanding of the security systems in place at a facility or within critical infrastructures and their ability to adequately protect those assets.

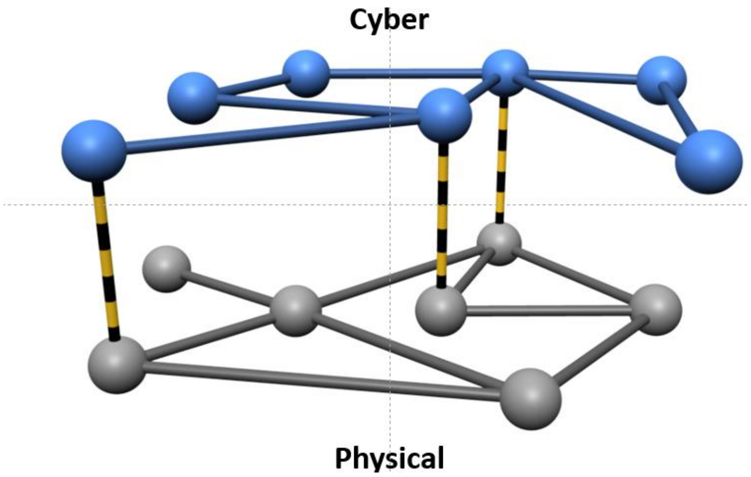

Figure 2. Physical-Cyber Attack Scenarios used by PACRAT.

- Safe, Secure Autonomous Scanning Solution for Energy Delivery Systems (SSASS-E)

  SSASS-E is an innovative tool that continuously scans IT/OT networks installed in critical energy infrastructures for vulnerabilities and provides improved vulnerability discovery compared to passive scans. The sensors and scanners distributed across the energy delivery system inform utility owners and operators managing the devices in their OT systems by notifying them of devices that have been added or removed between scans. This software provides an improved nonintrusive approach to vulnerability management and supports vendor and utility-defined protocols. SSASS-E is a monitoring tool that validates that a system is configured correctly and is a platform for safe and secure autonomous scanning to improve active defense of IT/OT networks.

- Mitigation of Externally Exposed Energy Delivery Systems (MEEDS)

  MEEDS is another innovative software application to solve cyber security vulnerabilities for utilities and other industries that use process control technologies. MEEDS monitors and identifies internet-connected energy delivery systems installed in field devices to find vulnerabilities and send alert notifications to operators. These control system devices include remote terminal units, protective relays, switchgears, and other sensing equipment that collects data and signals for efficient control of power grid operations. MEEDS, not only alerts system operators of vulnerabilities but also provides recommended risk-based mitigation actions. The MEEDS app is available for licensing for use in the utility sector. MEEDS features both basic and advanced features, so both novice-cyber and cyber-savvy users can use MEEDS to safely understand the cyber risks of their electric delivery system.

- Verification and Validation Assuring Reliability and Security (VARS)

  VARS is a cyber security-focused framework that can be adopted throughout the life cycle of a power plant, or other industries that have OT systems, to effectively test the cyber security of the OT assets. This web-based tool provides the framework that utilities (primary users) and vendors (secondary users) can use to determine risk-informed approaches to verify and validate the cyber security of OT assets tailored to the domains and life-cycle phases. VARS provides insights on the potential vulnerabilities and risk exposures of the OT asset and provides guidance to enhance the security and reliability of the OT asset and the overall system.

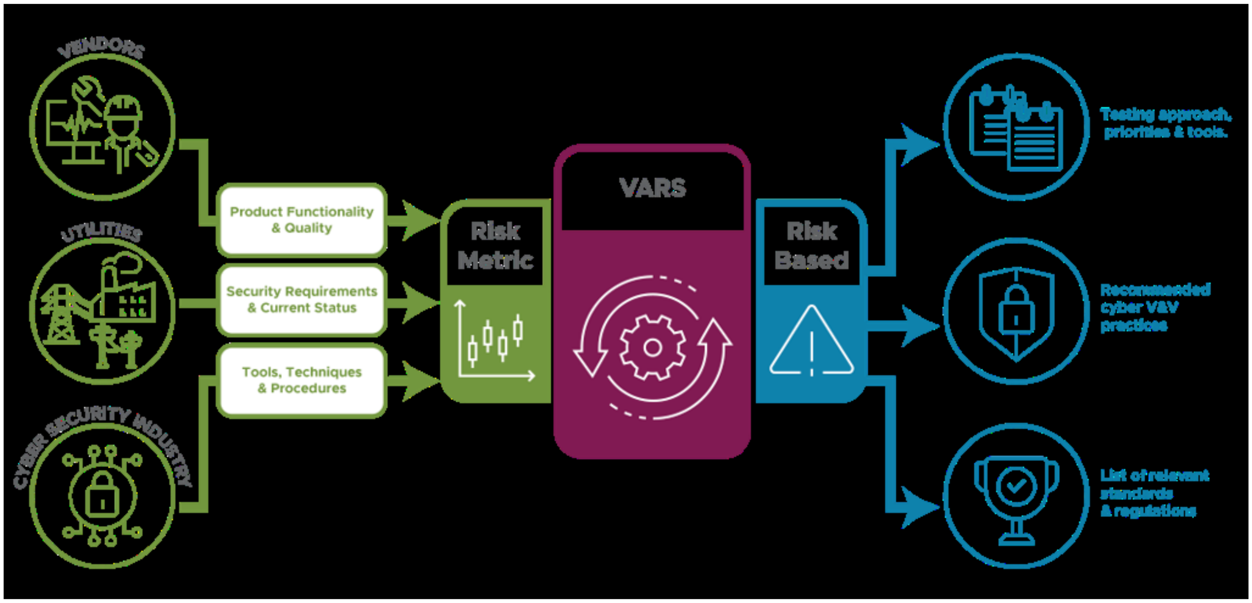
VENDORS
UTILITIES
CYBER SECURITY INDUSTRY
Product Functionality & Quality
Security Requirements & Current Status
Tools, Techniques & Procedures
Risk Metric
VARS
Risk Based
Testing approach, priorities & tools.
Recommended cyber V&V practices
List of relevant standards & regulations

Figure 3. VARS Framework.

- Threat Model-Based Response Tool

  The Threat Model-Based Response tool assesses the behavior of certain types of malware to known threats and successful defensive techniques. The technology uses hierarchical data clustering to identify common patterns, signatures, and distinguishable behavior characteristics.

- OT Cybersecurity Visualization Tools

  Visualization tools are a way to bridge communication taxonomy gaps between control room operators and cyber security professionals. PNNL experts have developed the Operations

Technology Cybersecurity Visualization Tool that provides situational awareness of the conditions.

2.1.4 Cyber Security Assessments and Inspections

Periodic assessments can aid in understanding the effectiveness of a cyber security program and measures. Cyber security maturity models enable organizations to assess the maturity of their cyber security program and identify areas that could be improved to address the evolving cyber threat environment. PNNL scientists and researchers have developed a robust portfolio of maturity models, most of which are free and available for organizations to use. With the use of maturity models built and maintained by PNNL, organizations can improve their cyber security posture, develop roadmaps to prioritize improvements, and help IT teams communicate effectively with senior management to obtain necessary investment support.

Many of the maturity models in PNNL's portfolio are based on the Cybersecurity Capability Maturity Model (C2M2) framework.[8] The C2M2 framework was developed through a public-private partnership effort sponsored by DOE. C2M2 was established to improve electricity subsector cyber security capabilities and to better understand the cyber security posture of the grid. Organizations, regardless of size, type, or industry can evaluate, prioritize, and improve their own cyber security capabilities using the C2M2 framework. The cyber security maturity models that PNNL stewards include the following:

- The Electricity Subsector C2M2[9] assesses a power sector organization's cyber security programmatic maturity. The model can be used to identify areas where cost-effective enhancements can quickly improve an organization's cyber security program. It was developed by energy industry experts from a diverse group of public agencies, private institutes, and industry.

- The Building Systems C2M2[10] assists building managers in evaluating the maturity of their cyber security programs for their building's digital control systems. The model is used to identify specific areas to strengthen and prioritize cyber security actions and investments to maintain the desired level of security throughout the building control system life cycle. The tool is applicable to a wide range of building types, including small, individual buildings and large building complexes (e.g., an office park or college campus).

- The Secure Design and Development C2M2 is designed to assist product vendors, hardware designers, software and firmware developers, and software/hardware integrators in assessing the cyber security maturity of their design and development processes across the organization. This assessment can be instrumental in driving approaches to improve the cyber security of products the organization designs and produces.

[8] The C2M2 models can be accessed at https://www.pnnl.gov/pnnl-maturity-models
[9] The Electricity Subsector C2M2 can be accessed at https://esc2m2.pnnl.gov/
[10] The Building Systems C2M2 can be accessed at https://bc2m2.pnnl.gov/

- The FCF[11] suite of maturity models provides tools to assess the cyber security maturity of facilities based on different standards and guidance. The FCF uses the NIST Cybersecurity Framework to help facility owners and operators better manage cyber security risks. The following are other tools developed from the FCF:
  - The FCF-Risk Management Framework (RMF) Hybrid builds upon the FCF by employing both the NIST Cybersecurity Framework and the RMF to evaluate facilities. This tool can perform a standard RMF assessment and generate both the FCF and RMF compliance/maturity scores.
  - The F-C2M2 Lite Assessment provides flexible guidance to help organizations assess their facility's cyber security maturity using the C2M2 framework. F-C2M2 Lite is dynamic, enabling the tool's set of questions to adapt and self-customize based on user responses.
  - The FCF-Primer enables users to conduct a quick review of their facility's security posture before committing resources to a full FCF assessment. The FCF-Primer can be used prior to a more comprehensive FCF assessment or as a checklist during the post-assessment/gap-mitigation phase to track enhancements.

Other maturity models that PNNL developed to assess the cyber security resilience of an organization or industry include the following:

- The Transmission Resiliency Maturity Model[12] is a tool for electricity transmission organizations to objectively evaluate and benchmark their current transmission resiliency policies, programs, and investments. The objective is to assist the transmission organization to target and prioritize improvements and enhance the overall resilience of the power grid. This DOE-sponsored model was developed through a public-private partnership that included PNNL, Electric Power Research Institution, the North American Transmission Forum, and more than a dozen transmission utilities.
- The Qualitative Risk Assessment[13] tool is designed to assist facility owners and operators in performing risk-based asset management. The Qualitative Risk Assessment tool enables asset owners to qualitatively define the estimated vulnerability of an asset, the potential impact if the asset is compromised, and categorizes the asset in an appropriate risk category: low, medium, or high.
- The Chemical Security Assessment Model[14] is designed to assist chemical facilities and laboratories in identifying the maturity of the chemical security program and to identify

[11] The FCF and the suite of tools can be accessed at https://facilitycyber.labworks.org/

[12] Additional information on the Transmission Resiliency Maturity Model can be found at https://trmm.labworks.org/

[13] Information on the Qualitative Risk Assessment tool can be found at https://facilitycyber.labworks.org/tools/qra

[14] CSAM can be accessed at https://csam.pnnl.gov/

programmatic areas to strengthen and maintain a desired level of security throughout the chemical life cycle.

In addition to developing maturity models and risk assessment tools, PNNL cyber security experts have developed methods that regulatory agencies can use to perform remote or virtual cyber security assessments. These assessments are valuable in situations where health and safety of an inspector would be of concern, such as during the COVID-19 pandemic. PNNL has also developed a nuclear information security continuous monitoring software tool that will ensure as technology and systems change, operators are aware of inappropriate use of normal system processes.

2.2 Cyber Security Technology

The use of rapidly developing new technologies deployed on the electrical power grid, the integration of legacy systems and the transition process makes the electrical power grid an inviting target for a cyber threat actor with malicious intent. A cyber incident on the energy grid could disrupt energy services, damage highly specialized equipment, threaten public health and safety, and adversely affect other national sectors across our nation. To mitigate these risks, both the North American Electric Reliability Corporation and NRC have a responsibility in establishing and enforcing cyber security requirements at commercial NPPs.

The North American Electric Reliability Corporation is focused on protecting the reliability of bulk electric systems, and the NRC is focused on prevention of radiological sabotage (i.e., significant core damage)[15]. PNNL researchers have developed methods and tools that improve the cyber resiliency of our nation's electrical grid and strengthen the reliability of energy delivery systems, improving resiliency of the grid by protecting and creating more resilient, self-defending energy systems for the future. PNNL's current research and development efforts are focused on understanding, evaluating, and developing trusted systems to better defend against adversaries. PNNL employs technical experts focused on cyber security infrastructure research and solutions, helping assure the reliability and security of the nation's power system.

2.2.1 Cyber Security Situational Awareness

Having access to and being aware of cyber threats to the energy sector or specific digital assets generally used at NPPs and knowing typical vulnerabilities and mitigation strategies will inform NPP owners on improvements or enhancements to implement for the cyber security program. PNNL has developed innovative cyber awareness tools and cyber security vulnerability tools, including the Cybersecurity Risk Information Sharing Program (CRISP)[16]. CRISP is a platform

[15] Memorandum of Understanding between the US NRC and North American Electric Reliability Corporation dated July 10, 2007 (https://www.nrc.gov/docs/ML0935/ML093510905.pdf)
[16] Information on CRISP can be accessed at https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity and ttps://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf

for energy sector owners and operators to voluntarily share IT systems traffic in near real- time by installing an information sharing device (ISD) at the border of their IT systems, just outside the firewall. CRISP enables energy sector partners to collaborate and facilitate timely bi-directional exchange of threat information. Using the ISD, CRISP utilities passively share near to real-time network data that DOE analyzes using open and closed information and PNNL's advanced tools. PNNL plays a lead role in CRISP, which uses advanced sensors and data analysis, to identify new and ongoing cyber threats. This information is shared with voluntary utility participants that collectively deliver more than 75 percent of the nation's electricity. CRISP is currently managed by DOE CESER and the Electricity Information Sharing and Analysis Center (E-ISAC) at the North American Electric Reliability Corporation.

2.2.2 Software Defined Networking

Control systems are used to support operation of safety-related or non-safety related equipment and functions at NPPs. They can include a combination of numerous devices and protocols that are likely mission critical and require high availability. In the past few years these systems have increased in complexity with innovative technology as well as increased in size with additional sensors and interconnectivity. To mitigate both the complexity of these systems as well as the increasing threat of sophisticated cyber actors, PNNL has helped commercialize a new-generation of software-defined networking (SDN) and cyber security technology. These SDN solutions can proactively detect and quickly thwart cyberthreats thus transforming cyber security from reactive to proactive. They bring robust protection to operational technologies in the field that may be decades old. Instead of detecting cyberattacks from a known list of threats and their associated attributes, PNNL's solution utilizes a positive security model to proactively detect any unauthorized devices or traffic on the network in real time and takes immediate defensive actions to address the threat while also providing awareness of the event for system operators.

In addition to the cyber protections that SDN brings, SDN allows the collection of system information of deployed network elements and enables a global view of the network topology, with near real-time knowledge of network activities. With this capability, SDN enables controls over key network communication ensuring that only previously approved communication affects systems on the network. This provides heightened security for critical systems.

PNNL has deployed SDN to reduce both the attack surface of systems and to improve response time to cyberattacks on energy delivery systems across the Department of Defense, US Coast Guard, Veterans Administration and others within the energy sector. They are also in initial discussions with other operational technology systems across our Nation's critical infrastructure sectors.

2.2.3 Built-in Resiliency and Controls

Defense and protection are important weapons for thwarting attacks. In collaboration with industry, PNNL engineers and scientists are creating innovative designs and systems with built-in resiliency and cyber security controls that enable energy delivery systems to keep working regardless of threats. NPP owners can implement these types of technology to help monitor and manage the security of their networks. Examples of these tools include:

- Hardware Only Controllers

General-purpose computation has improved the lives of billions around the globe. Critical infrastructures, including the nuclear industry, depend on the ubiquitous use of networked computerized devices. Due to the commodity components used in their design, these devices have excess capabilities and processing capacity that provide an attractive attack surface for nefarious actors. To reduce this attack surface, PNNL has designed and tested a prototype hardware-only controller. This hardware-only controller is a deterministic system that performs its intended design function and nothing else. This type of controller can be a viable replacement for software-based, programmable controllers, especially when the consequences of compromise are dire.

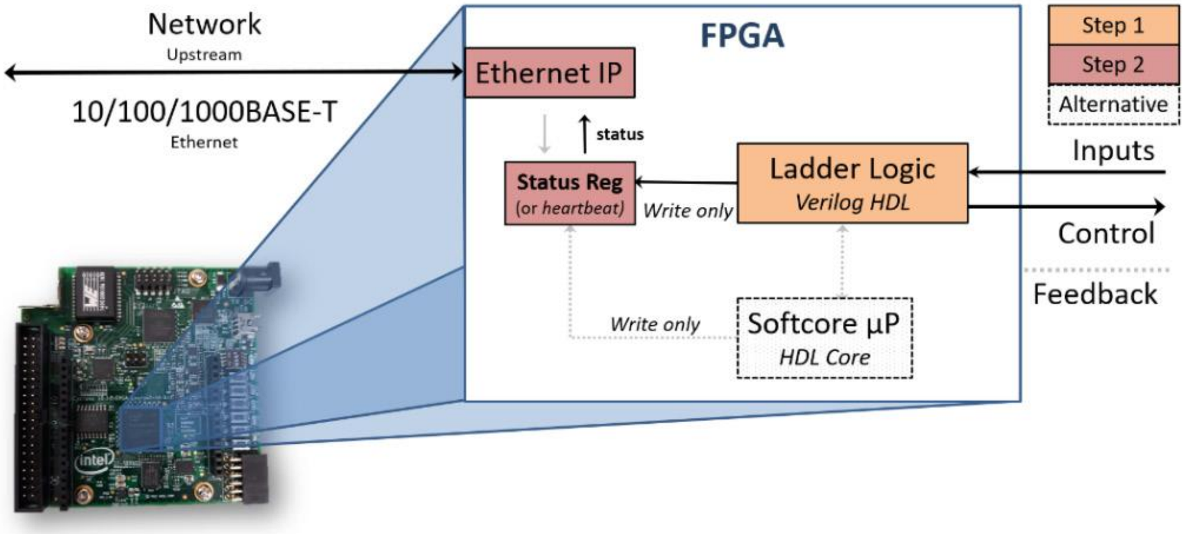

Figure 4. High-level design for the hardware-only controller.

- The Cymbiote

The Cymbiote detects cyberattacks in embedded field devices for real-time event recovery. Embedded field devices that sense and control physical processes in critical infrastructure are soft targets for cyberattack because they lack the fundamental features for cyber security monitoring and control. The Cymbiote is a combination of hardware and software, and the only device of its kind, that collects data from multiple sources, synthesizes them to detect events of importance, and enables dynamic and real-time device reconfiguration for event recovery. It includes hardware to allow data to flow between pieces of equipment without disrupting normal operations or communications.

- Shadow Figments

This PNNL-developed tool generates deceptive systems to foil cyberattacks on control systems. This “deception” approach is a defense tactic that slows attackers by diverting their attention and increases detection when attackers interact with the deceptive systems. Because control systems rely on physical rather than data processes, this approach is difficult for them to mimic, allowing attackers to easily reengage and penetrate the real system. Shadow Figments generates and runs high-fidelity deceptions of control systems. Using a model of the real process, the software generates controllers and sensors that respond to an attack in realistic ways to deceive intelligent attackers targeting control systems.

- Kritikos/Caddy

Cyber defenders in an industry are often unaware of dependencies between various IT assets. Kritikos/Caddy determines cyber dependencies between various information and technology assets by using network monitoring data pattern recognition. The technology uses an artificial neural network that groups and labels patterns to pinpoint dependencies. Understanding dependencies gives an organization better situational awareness and the ability to assess, triage, and recover from cyberattacks. Such knowledge also supports planning for business continuity, disaster recovery, and development of infrastructure investment strategies.

3.0 Cyber Security Testbeds and Facilities

Cyber networks are constantly under attack by bugs, bots, and nefarious actors. While system owners may understand the need to secure their networks, they may not always be sure of the best actions to take. Rigorous exploration of the cyber security domain, in a controlled testbed environment, enables researchers to understand risks and testing mechanisms for defense and deterrence. Testbeds provide the ability to run controlled and repeatable experiments in an environment that identify engineered solutions with predictable results. PNNL's testbed capabilities provide realistic testing and adversarial training capabilities to assess the security and performance of software, hardware, mobile platforms, and commodity devices. In addition, PNNL researchers can model real-world IT and OT enterprise networks. These testbeds enable PNNL to develop interactive training, testing, and assessment toolkits to assess the security and performance of software, hardware, mobile platforms, and other devices. The testbed facilities allow cyber defenders to test and evaluate technology, detect and repair vulnerabilities, monitor and isolate adversaries, and predict and prevent cyberattacks. The following subsections describe the different types of facilities and testbeds that PNNL manages.

3.1 Electricity Information and Operations Center

NPPs use more of our nation's available generating capacity annually than other types of energy generating facilities. Per the U.S. Energy Information Administration,[17] in 2019, the nuclear share of the total electricity generating capacity in the United States was 9%, while the nuclear share of total electricity generation was about 20%. Modern technologies and lifestyles have cultivated a reliance on power, and therefore, there is a national need to better manage and control the grid. However, the nation's power grid has become a major target for sophisticated attacks from nation-states and cyber criminals.

PNNL has answered this call by bringing together industry software, real-time grid data, and advanced computation into a functional control room, the Electricity Infrastructure Operations Center (EIOC) [18]. Shaped with input from utilities, technology vendors, and researchers, the EIOC serves as a unique platform for researching, developing, and deploying technologies to improve grid management. Researchers conduct incident response exercises and simulations at the Electricity Infrastructure Cybersecurity and Resilience Center at PNNL. The EIOC integrates hardware and software, real-time grid data, and advanced computation in two control rooms. Utilities, vendors, government agencies, and universities use the facility for development, integration, validation, testing, and training.

[17] Data from the Energy Information Administration was retrieved from https://www.eia.gov/energyexplained/nuclear/us-nuclear-industry.php#:~:text=In%202019%2C%20the%20nuclear%20share,electricity%20generation%20was%20about%2020%25

[18] Information on the EIOC can be accessed at https://www.pnnl.gov/electricity-infrastructure-operations-center

Figure 5. PNNL’s Electricity Infrastructure Operations Center

At the EIOC, researchers focus on developing additional and more robust data to improve situational awareness and by developing tools that ingest that information to enable timely analyses and quick and appropriate action. The facility features:

- Access to real data from North America's eastern and western power grids
- Physical security and cyber security for equipment, information, personnel, and data
- Leading energy management system software
- Industry standard virtualization infrastructure
- 30 workstations, 25 special-purpose computers, and more than 50 servers
- A 452-square-foot video screen in the EIOC East room
- A 115-square-foot video screen in the EIOC West room
- Video and audio capture and recording of room and operations

By using the resources available at the EIOC and by drawing upon its industry partnerships, PNNL researchers are obtaining and studying more in-depth data from extreme weather events and other grid disruptions to understand how to prevent future catastrophes. The EIOC is available to utilities, vendors, government agencies, and universities interested in research, development, or training.

3.2 Power Networking, Equipment, and Technology Testbed

Energy from nuclear power contributes to our nation’s critical infrastructure. However, the energy control systems, both physical and digital, face an ever-increasing amount of scrutiny and cyber threats by adversaries. Investigating these threats to understand and mitigate them is difficult to do on operational systems since inappropriate actions during investigation can potential disrupt the control systems' normal function. Simulation testbeds enable research and development of new tools and methods that will harden our current and future infrastructure in a safe and reliable environment isolated from operational systems supporting our nation's energy grid.

Figure 6. Visualization of grid simulation capabilities.

PNNL's Power Networking, Equipment, and Technology (PowerNET) testbed is a remotely accessible, multiuser, experimental testbed for collaborative power system and smart grid research. The testbed integrates real-world equipment with virtual and simulation capabilities to create an environment that can dynamically configure into many experimental setups to meet the varied needs of the research community. PNNL's PowerNET testbed helps researchers analyze and evaluate current power grid technologies and environments to unearth vulnerabilities and develop new protection and mitigation measures or systems. Fusing data among simulated, virtualized, and physical equipment leads to the creation of realistic and scalable environments where new functionality and ideas can be exercised.

The EIOC has also been used to explore improved cyber security defense methods. Engineers have tested applications for high-performance computing and the GridOPTICS™ PowerNET Testbed–a multi-user, remotely accessible, experimental laboratory focused on testing and evaluating power systems for smart grid research.

3.3 Energy Communications Cyber Test Range

One component of energy systems is the communication systems that ensure systems effectively share critical information. To test the reliability and integrity of those communication systems, PNNL operates an Energy Communications Cyber Test Range. The Energy Communications Cyber Test Range is a software-defined radio test range with a two-mile-plus radio frequency range and more than six miles of optical fiber. This test range is used to develop capabilities that prevent cyber security risks including man-in-the-middle and spoofing attacks. As an example, this test range is used to protect global positioning systems (GPS) to secure data synchronized over large geographic areas. The Energy Communications Cyber Test Range is configurable and has typical urban characteristics, reconfigurable antennas, software defined radio expertise, radio frequency communications expertise, and energy equipment, such as synchrophasors.

3.4 CyberNET Testbed

NPP and nuclear facility owners may want to implement unique methods and tools to test a unique or customized type of cyber security technology. These devices should be assessed in a scientific testbed for generating cyber models, collecting data for analysis, and documenting the experiment for repeatable and reproducible results. PNNL researchers developed the CyberNET[19] testbed to improve and enhance cyber security research. CyberNET is a scalable testbed that accelerates cyber research while reducing costs, time, and redundancies across the cyber security domain. Enhanced modeling and simulation, supported by real-world data sets, increase realism in models and lead to more impactful research. CyberNET offers an isolated and dynamic testbed that is easily configurable and customizable. This testbed is where researchers can build, test, evaluate, or otherwise conduct research in an enterprise-like environment. CyberNET also leverages cloud technology to offer a configurable and controlled cyber environment where realistic models can be executed using real software. This testbed builds from OpenStack software with scientific modifications, using Xen and KVM hypervisors, and the cyber range toolkit from the Massachusetts Institute of Technology's Lincoln Labs.

3.5 Internet of Things Common Operating Environment Testbed

To improve plant operations, maintenance and monitoring capability, plant operators may use internet of things (IoT) and industrial internet of things (IIoT) devices, such as drones, smart building controllers, security cameras, lightbulbs, appliances, and health tracking devices. These devices combine OT with IT and provide a means to connect the physical world with the internet. Iot/IIoT devices can store, compute, and transmit large amounts of data to and from other devices thorough network connectivity. These devices are equipped with sensors, processors, and communication hardware embedded into the architecture to acquire data from

[19] Information on CyberNET Testbed can be obtained from https://www.pnnl.gov/projects/cybernet-testbed

their surrounding environment and communicate (e.g. wireless etc.) to other endpoints, such as a handheld device or desktop computer. The data is then processed using advanced analytics to determine the cyber security risks introduced by these devices.

Figure 7. Cyber analysts testing IoT devices in the IOTCOE Testbed

For this research, PNNL has established the IoT Common Operating Environment (IoTCOE)[20] testbed as a platform for solving current and future challenges with research and development. This effort focuses on new technologies, cyber security, and the development of connected devices to visualize a 360-degree view of the interconnected devices. This approach to IoT/IIoT experimentation is unique and accommodates a myriad of research needs, including the exploration of cutting-edge chemical, physical, and cyber challenges using visual analytics, artificial intelligence, and machine learning.

The IoTCOE Testbed is made up of two physical spaces deploying over 60 different IoT and IIoT devices for experimentation individually and collectively—and the device list is steadily growing. Each testbed is a full-scale replica of a residential environment. The IoTCOE Testbed will provide important data sets that industry can use to advance security best practices, energy sustainability, and more. The IoTCOE Testbed can also isolate devices from interference by competing signals such as Bluetooth, infrared, ZigBee, wireless, cellular, Ethernet, and radio frequency, thus providing an ideal collaborative space for unique and innovative research experiments. PNNL's IoTCOE team has also identified normal device behavior as a baseline for

[20] Information on IoTCOE can be accessed at https://www.pnnl.gov/internet-things-common-operating-environment

experiments, providing a sanitized test environment to conduct experiments and eliminate false positives. Equipped with residential and commercial IoT devices, the IoTCOE Testbed delivers insight into untested hypotheses of IoT/IIoT experiments, including those in cyber security vulnerability detection, threat prevention and identification, energy usage functions, and more. PNNL's IoTCOE Testbed will strengthen our national cyber security posture in an interconnected world and inform our understanding of the IoT/ IIoT connections of the future.

3.6 Radiological Security Cyber Range

As traditional physical security continues to merge with IT, an NPP's physical protection system are merging with OT and as a result it inherits the cyber security risks that are prevalent with these systems. Security upgrades, such as access controls, alarm and assessment systems, and remote monitoring systems, are increasingly dependent on the networks and cyber security capabilities of the host sites. PNNL's Office of Radiological Security has developed Cyber Range as part of the ongoing training for physical protection experts. Cyber Range provides a hand-on opportunity to work with security equipment being deployed in the field. This Office of Radiological Security testbed is equipped with access control, intrusion detection, and video surveillance systems.

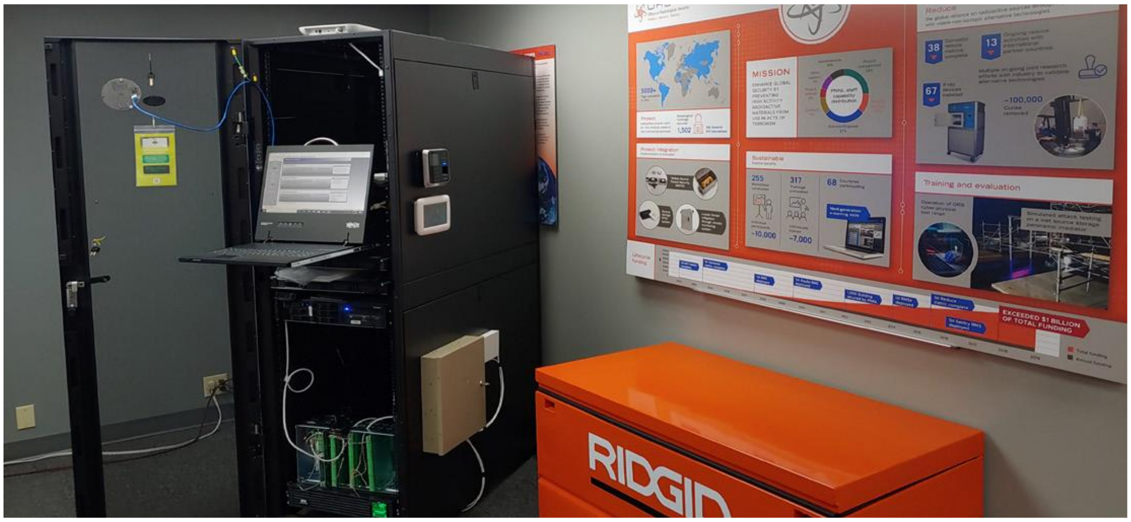

Figure 8. The Office of Radiological Security Testbed

About PNNL

Pacific Northwest National Laboratory, located in southeastern Washington State, is transforming the world through courageous discovery and innovation. PNNL's science and technology inspires and enables the world to live prosperously, safely, and securely. Our researchers collaborate to advance science and solve complex problems in energy, the environment, and national security — as well as move technology solutions to market. PNNL employs more than 4,000 staff members with a $1 billion annual budget. Since 1965, PNNL has been operated by Battelle on behalf of the U.S. Department of Energy.

Contact Information:

Mark Nutt
Nuclear Energy Sector Manager
Energy and Environment Directorate
Email: mark.nutt@pnnl.gov
Tel: 509-375-2984
Cell: 630-596-7365
https://nuclear.energy.pnnl.gov

Tara K. O'Neil
Nuclear Regulatory Sub-Sector Manager
Energy and Environment Directorate
Email: Tara.o'neil@pnnl.gov
Tel: 541-738-0362
Cell: 541-602-3958

Fleur de Peralta, P.E.
Senior Advisor
Risk and Environmental Assessment Group
Earth Systems Science Division
Email: Fleurdeliza.deperalta@pnnl.gov
Tel: 509.375.3323
Cell: 360.601.6563

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov