Pacific Northwest
NATIONAL LABORATORY

PNNL-39500

Programmable Digital Devices used in Advanced Reactors

September 2026

William J. Hutton
Corinne G. Roth
Fleurdeliza A. de Peralta

U.S. DEPARTMENT of ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-39500

Programmable Digital Devices used in Advanced Reactors

September 2026

William J. Hutton
Corinne G. Roth
Fleurdeliza A. de Peralta

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Programmable Digital Devices used in Advanced Reactors

Dr. William Hutton, Corinne Roth, Fleur De Peralta

Pacific Northwest National Laboratory
Richland, WA
will.hutton@pnnl.gov, corinne.roth@pnnl.gov, fleurdeliza.deperalta@pnnl.gov

***Abstract*—This paper introduces the concepts of *common cause failure*, *diversity*, and *defense-in-depth* used by the nuclear industry to analyze resilience in reactors. A survey of publicly traded and private companies building advanced reactors and their licensing status is presented. Safety and non-safety systems found in the NuScale Power design are summarized and the likely hardware and software categories used by those systems are enumerated.**

The importance of industry partners is highlighted. This paper also identifies an alternate path forward without industry partners to advance the knowledge needed to use artificial intelligence to analyze HBOMs and SBOMs to better understand reactor resiliency.

***Index Terms*—Advanced reactors, cybersecurity, programmable digital devices**

I. Introduction

The Advanced Reactor Safeguards & Security (ARSS) program is a multi-lab effort funded by the U.S. Dept. of Energy. ARSS was established to provide research support to address near term challenges that advanced nuclear reactor vendors will face in meeting domestic Material Control and Accounting (MC&A), Physical Protection System (PPS), and cybersecurity requirements for U.S. construction [19].

The "AI/ML Models for CCF & D^3 Analysis" research project under ARSS is exploring how artificial intelligence and machine learning algorithms may be used for analysis of common cause failures (CCF) and diversity and defense-in-depth (D^3) issues based on hardware and software bills of material (HBOM and SBOM).

II. Background

Modern programmable digital devices contain multiple hardware and software components and often complicated supply chains. Vendor diversity in programmable digital devices is no guarantee of diversity and may hide CCF issues. Comparing programmable digital device HBOMs and SBOMs is a crucial step in assuring true diversity and defense-in-depth and performing CCF analysis. However, HBOMs and SBOMs may be viewed as proprietary or a competitive advantage by vendors and system designers, leading to repeat work to generate HBOMs and SBOMs for widely-used programmable digital devices in advanced reactors. Without HBOMs and SBOMs, programmable digital devices may be opaque to subject matter experts. High-fidelity HBOMs and SBOMs may contain thousands of entries, making human analysis impractical.

A. Common Cause Failure (CCF)

In the nuclear industry "common cause failure" (CCF) refers to the simultaneous failure of two or more redundant components, systems, or safety functions due to a single shared cause or coupling mechanism. Failures occur when diverse elements, which are intended to provide independent layers of safety or reliability, are all affected by a shared root cause–such as a design flaw, environmental stressors (e.g., temperature, humidity, etc.), manufacturing defect, or human error. CCFs create positive dependency among components, which can critically undermine redundancy and defeat defense-in-depth strategies.

From the perspective of cybersecurity, unquantified risk of CCF can arise when different vendors use the same software libraries or chipsets resulting in a shared vulnerability.

Recognizing and mitigating CCFs is essential in nuclear probabilistic risk assessments and design reviews. Nuclear industry standards that specifically address CCF include NUREG/CR-5485 and IEC 62340.

B. Diversity and Defense-in-Depth (D^3)

In the nuclear industry, diversity and defense-in-depth are complementary design principles used to ensure that no single failure, error, or unforeseen event can compromise reactor safety. These concepts are deeply embedded in the safety philosophy [7] of the U.S. Nuclear Regulatory Commission (NRC) and have been applied to reactor design, operation, and emergency preparedness for decades [10]. Defense-in-depth seeks to provide multiple, independent layers of protection against accidents and radiological releases, while diversity reduces the likelihood that a common cause could disable multiple safety systems simultaneously. Together, these principles increase the resilience of nuclear power plants.

Defense-in-depth is based on the premise that safety should not rely on any single protective barrier. Instead, nuclear reactors employ successive layers of protection, including inherent design features, engineered safety systems, physical barriers, operating procedures, and emergency response capabilities [10]. For example, radioactive material is contained by multiple physical barriers, such as the fuel matrix, fuel

TABLE I
PUBLICLY TRADED COMPANIES

Company (Ticker)	Reactor Type	Status
BWX Technologies (BWXT)	Fuel and components (RISO, naval, micro)	Supplier across SMR supply chain
Centrus Energy (LEU)	HALEU enrichment	Key fuel enabler for advanced reactors and SMRs
GE Vernova Hitachi Nuclear Energy (GEV)	BWRX-300 (VOGTLE)	Commercial build at TVA/ORNL
Nano Nuclear Energy (NNE)	HTGR micro-reactor (KRONOS)	NRC licensing in progress
NuScale Power (SMR)	Light-water SMR (VOYGR)	NRC certified
Oklo Inc. (OKLO)	Sodium-cooled fast reactor (Aurora)	Targeting 2028 deployment
Rolls-Royce Holdings PLC (RR)	PWR-style SMR	UK-backed by £2.5B, Generic Design Assessment (GDA)
X-energy (XE)	HTGC reactor using TRISO fuel (Xe-100)	Pre-application engagement with NRC [11], targeting 2030 construction

TABLE II
PRIVATELY HELD COMPANIES

Company	Reactor Type	Status
Aalo Atomics [1]	Sodium-cooled modular reactors (XMR)	
Antares Nuclear [2]	Sodium-cooled TRISO-fuel microreactor	First criticality under DOE pilot in June 2026
Kairos Power [4]	Low-pressure molten fluoride salt (KP-FHR) (HERMES)	NRC construction permit (2023) Construction at Oak Ridge, TN (2024) License application preparation
TerraPower [3]	Sodium-cooled Natrium SFR (molten salt storage) fast reactor	NRC construction permit March 2026

TABLE III
OTHER ORGANIZATIONS

Company	Reactor Type	Status
Nuclear Energy Institute (NEI)	N/A	Works with industry to identify vulnerabilities, defense-in-depth designs

cladding, reactor coolant pressure boundary, and containment structure. Likewise, critical safety functions such as reactor shutdown, decay-heat removal, and electrical power supply are supported by redundant and physically separated systems. The NRC describes defense-in-depth as a fundamental safety strategy that uses multiple safeguards to prevent accidents and to mitigate their consequences should prevention fail [9].

The concept of diversity addresses a different but related challenge: the potential for common-cause failures. A common-cause failure occurs when multiple systems fail simultaneously because they share a common vulnerability, such as a design defect, software error, environmental condition, or human error. Diversity mitigates this risk by implementing safety functions using different technologies, physical principles, equipment types, or actuation methods. For example, a reactor protection system based on digital instrumentation and control equipment may be supplemented by an independent and technologically distinct backup system capable of performing the same safety function. By ensuring that safety systems are not susceptible to the same failure mechanism [18], diversity reduces the probability that a single defect could defeat multiple layers of protection [12].

Modern reactor licensing reviews frequently evaluate diversity and defense-in-depth together, particularly for advanced digital instrumentation and control systems. NRC guidance requires designers to assess whether credible common-cause failures could impair reactor protection functions and whether sufficient diverse means exist to maintain safe operation or safely shut down the reactor. In this context, defense-in-depth provides multiple layers of protection, while diversity strengthens those layers by ensuring they do not share the same vulnerabilities [18]. The combined application of these principles is intended to provide high confidence that essential safety functions can be maintained even under unlikely or unforeseen conditions.

C. Hardware and Software Bills of Material (HBOM, SBOM)

A Hardware Bill of Materials (HBOM) and a Software Bill of Materials (SBOM) are structured inventories that document the components comprising a hardware or software product, respectively. Similar to a manufacturing parts list, these digital artifacts provide visibility into the constituent components of a system and the relationships between them.

An HBOM typically identifies physical components such as processors, memory devices, integrated circuits, firmware-bearing modules, suppliers, and part numbers. In the context of cybersecurity and supply chain risk management, HBOMs improve transparency regarding the provenance and composition of hardware products, enabling organizations to assess risks associated with counterfeit, vulnerable, or untrusted components. Recent U.S. government guidance has promoted HBOMs as a mechanism for strengthening supply-chain assurance and supporting procurement decisions for critical technologies.

An SBOM is the software equivalent of an HBOM. The U.S. National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technol-

ogy (NIST) define an SBOM as a formal record containing details about the software components, dependencies, and supply-chain relationships used to build a software product. An SBOM typically includes information such as component names, versions, suppliers, dependency relationships, authorship, and timestamps. By providing a machine-readable inventory of software ingredients, SBOMs enable organizations to identify affected systems when new vulnerabilities are disclosed, support license-compliance activities, and improve software supply-chain transparency. These capabilities have become increasingly important following major software supply-chain incidents and the U.S. government's broader cybersecurity initiatives under Executive Order 14028 [6].

Together, HBOMs and SBOMs provide complementary visibility into the hardware and software layers of modern information systems. When maintained throughout a product's lifecycle, they support vulnerability management, incident response, asset management, and supply-chain risk assessment by enabling organizations to understand exactly what components are present in a system and where those components originated. As a result, BOM-based transparency is increasingly recognized as a foundational practice for cybersecurity, critical infrastructure protection, and secure technology acquisition [5].

III. Potential Industry Partners

Multiple organizations were contacted to participate as an industry partner. Industry partners are important to ensure our research is relevant and actionable. Despite multiple emails, telephone calls and in-person meetings, no industry partners have been identified as of May 2026.

An operational organization expressed great interest in participating in this project. However, as a "customer", the reactor design is basically a *black box* to them. Further, the vendor is responsible for the cybersecurity of the reactor. The operational organization facilitated contacts with the vendor.

As of May 2026, the vendor is still several years away from the construction phase of the advanced reactor deployment. They have expressed great interest in participating in this project, but will not have finalized system designs within the timeframe of this project (i.e. by October 2026).

A common cause for lack of participation by industry partners appeared to be that system designs were not yet finalized and lists of programmable digital devices to be used in those systems did not exist. The license status in Tables 1-3 supports this claim.

For this reason, an open-source literature search based on the NuScale Power design will be used for the rest of this paper. If a significant number of programmable digital devices are not identified by this literature search, the project will be forced to use a proxy industry application to validate our approach to using artificial intelligence and machine learning to analyze cybersecurity. When the nuclear industry is ready– this project will have identified the necessary steps to use HBOMs and SBOMs in the analysis of cybersecurity for advanced reactors.

A. Publicly Traded Companies

See Table I for a list of publicly traded companies that are in some stage of developing an advanced reactor. Use Table I to compare reactor type and license status. This project contacted multiple companies in Table I but all declined to participate in our research project for various reasons.

B. Privately Held Companies

This project also reached out to several privately held companies, including some in Table 2. While discussions are ongoing, we have passed a "go/no-go" decision date and must begin experimentation with HBOM and SBOM extraction to provide analysis data for AI and ML algorithms. A list of programmable digital devices provided by an industry partner is our preferred source of data. In absence of that, this project's hypothesis is that the domain source of HBOM and SBOM data is an independent variable in the success or failure of the analysis approach. The goal of this project is to advance AI/ML methods that can be applied by the nuclear industry to analyze cybersecurity of advanced reactors using HBOMs and SBOMs.

C. Other Organizations

This project even reached out to organizations like NEI, which attempted to help us make progress with collaborating with one or more industry partners.

IV. Common Advanced Reactor Systems

Advanced reactors still have the functional equivalent of a Nuclear Steam Supply System (NSSS) that produce heat and transfer it to a power conversion system. However, in Gen-IV and advanced non-LWR (i.e. light water reactors) the architecture and terminology used have shifted. While not explicitly labeled "NSSS", these types of reactors universally have:

- a reactor module or core system
- a primary coolant system (e.g., sodium, lead, molten salt, gas, or water in some SMRs (i.e. small modular reactors)
- heat transport systems
  - intermediate loops
  - primary-to-secondary heat exchangers
- safety-related shutdown and residual heat removal systems

This group of systems still functions identically to what LWRs have historically called the NSSS. Some advanced reactors avoid the term NSSS. Often systems like:

- Primary Heat Transport System (PHTS)
- Reactor Module or Reactor System
- Primary / Intermediate Circuits
- Reactor Coolant System (RCS) in some LWR SMRs

These systems fulfill the same role as the classic NSSS, but are designed around *loops* for passive safety.

There are two important concepts to keep in mind about advanced reactors when thinking about cybersecurity. First, is that advanced reactors have been designed to assume an

adversary will be able to successfully execute an effective cyber-attack against the advanced reactor at the time and place of the adversary's choosing. Second, advanced reactors are designed to be so resilient that the worse-case scenario of a cyber-attack is a safe shutdown of the reactor. Therefore, the only impact of a cyber-attack on an advanced reactor is a loss of availability (i.e. generation of power) due to safe shutdown.

Advanced reactors use digital systems as a first line of defense and passive systems that do not rely on any power or air for a safe shutdown using gravity [20]. Reactor systems are categorized into *safety* and *non-safety* categories. Programmable digital devices reside primarily in non-safety systems, further lessening the impact of a cyber-attack. Passive methods are used to perform critical functions in safety systems (e.g., gravity to drop control rods) [20].

V. Programmable Digital Devices Found in Advanced Reactor Systems

Realistic data informed by industry partners is important to this project. Although several organizations expressed a desire to participate, none felt they could contribute the data we needed before the end of our project in September 2026. Therefore, this project will attempt to use information about programmable digital devices found in NuScale Power systems based on a literature review of design documents filed with the NRC. The NRC maintains a publicly searchable database known as *ADAMS* [8].

NuScale does not use the term NSSS, but the functional architecture is still present. The NuScale **Power Module** integrates the equivalent systems directly within an integral PWR reactor vessel with passive safety features. This is how the NuScale architecture maps to the classical NSSS components [17]:

*A. **Reactor Core** (NSSS equiv.: Core and support structures)*

The NuScale Power Module (NPM) is a standard PWR fuel assembly configuration housed inside an integral reactor vessel. The safety-related monitoring and actuation of temperature, neutron flux, coolant level, etc. are handled by the Module Protection System (MPS).

*B. **Reactor Coolant System (RCS)** (NSSS equiv.: Pumps, piping loops and steam generators)*

NuScale eliminates the large-loop RCS entirely–no primary coolant pumps and no external piping. Instead, the NPM's RCS is fully contained within the integral vessel. The reactor coolant boundary sensors are managed by the MPS.

*C. **Steam Generation System** (NSSS equiv.: Steam generators, moisture separators, steam lines)*

NuScale uses integral helical-coil steam generators inside the reactor pressure vessel. The steam produced is delivered via short penetrations to the containment and then to the balance of plant. Instrumentation and control of steam generator parameters are handled by the MPS and non-safety related Module Control System (MCS) / Plant Control System (PCS).

*D. **Pressurizer** (NSSS equiv.: External dedicated pressurizer)*

NuScale integrates the pressurizer into the reactor vessel top head. Pressurizer heaters and their breakers are explicitly listed as MPS-managed components. Traditional pressurizer functions still exist–but temperature/pressure control and relief strategy are internalized.

*E. **Engineered Safety Features (ESF)** (ECCS, safety injection, emergency feedwater, etc.)*

NuScale uses passive safety systems instead of an active Emergency Core Cooling System (ECCS). Passive safety systems include; reactor vent valves, depressurization valves, passive containment cooling, and decay heat removal through steam condensation and natural circulation.

*F. **Reactor Protection System (RPS)** (NSSS equiv.: Trip logic, scram system)*

NuScale integrates the RPS into the MPS, built on the Highly Integrated Protection System (HIPS) Field-Programmable Gate Array (FPGA) platform, including:

- four separation groups of trip determination
- four reactor trip breakers
- manual actuation switches in the Main Control Room (MCR)

G. Safety Systems

Given its importance, this project will first focus on the MPS for a list of programmable digital devices lists. If that approach is not successful, the project will shift focus to the Nuclear Measurement System (NMS),which is directly responsible for trip, engineered-safety feature actuation, and critical reactor / steam-generator measurements.

H. Non-Safety Systems

Because safety systems tend to be passive by design, the MPS and NMS may not have enough programmable digital devices for our research experiments. In that case, the project will focus on the MCS and PCS.

I. Programmable Digital Devices in the MPS

NRC's ADAMS database, which is publicly searchable, reveals that NuScale's Module Protection System (MPS) is implemented using the Highly Integrated Protection System (HIPS) platform [13]–[16]. NuScale Power and Rock Creek Innovations co-developed the HIPS. Ultra Electronics built and tested a working HIPS prototype. Paragon Energy Solutions acquired Rock Creek Innovations and licensed the HIPS technology.

The HIPS platform is implemented using Field Programmable Gate Arrays (FPGAs) instead of conventional microprocessor-based safety computers. Because the HIPS is an FPGA, it does not rely on traditional runtime software or operating systems. The use of FPGA configured logic is intended to reduce the cybersecurity attack surface of safety-related systems.

Public records related to software used by the MPS and HIPS are sparse. Microprocessors, operating systems, runtime environments, etc. are not identified. Use of an AI chatbot to perform extensive searches of Chapter 7 Instrumentation & Controls filings reveal system names, system functions, and system vendors (as identified above), but does not provide the detail needed to research HBOMs and SBOMs for the MPS. Information useful to the creation of an HBOM and SBOM for the MPS would include:

- FPGA manufacturer
- Board-level hardware part numbers
- Embedded firmware development tools
- Verification and validation tool chain
- Detailed software inventory
- Operating system
- Network devices

J. Programmable Digital Devices in the NMS

The NMS is also a safety-related system and is similarly described in NuScale documents found in ADAMS. Therefore, the same lack of specificity outside of hardware vendors is a problem for establishing a list of programmable digital devices for use in this project's research experiments. This was expected to a certain degree given that safety systems have high consequences for cyberattack.

K. Programmable Digital Devices in the MCS

The NRC ADAMS database does not expose underlying Chapter 7 PDFs and many detailed I&C documents regarding implementation of the MCS are withheld as proprietary information. However, major MCS functions that would require hardware and software components can be identified from the design documents submitted by NuScale Power [16].

- Reactor power control
- Plant startup and shutdown sequencing
- Normal operating control
- Monitoring and control of module process variables
- Interface to operator workstations and the main control room
- Data exchange with safety systems and the PCS system

Recall that the MCS is not a safety system.

The following hardware and software categories were identified from the final safety report filed by NuScale Power [16].

1) MCS Hardware Categories:

- Distributed Control System (DCS) controllers
- Human-Machine Interface (HMI) workstations
- Engineering workstations
- Network communication equipment
- Input/Output (I/O) processes
- Remote interface units
- Plant data Historian servers
- Time synchronization equipment

2) MCS Software Categories:

- Automatic reactor power control
- Startup/shutdown sequencing
- Control loop algorithms
- Alarm processing
- Historian (i.e. data logging) functions
- HMI display software
- Diagnostic and self-test software
- Configuration management software

Some vendors make HBOMs and SBOMs available directly to customers. Vendors were not publicly identified. To create useful HBOMs and SBOMs this project would need to work with vendors to identify the specific hardware and software produces and their versions. In absence of this information, this project could work with vendors that market similar hardware and software components that are not associated with a specific advanced reactor design for the purpose of researching the effectiveness of HBOMs and SBOMs as a crucial input into the AI/ML analysis of CCF and D^3.

L. Programmable Digital Devices in the PCS

Like the MCS, the PCS is not a safety system, but vendors are not publicly identified nor are exact controller model numbers, programmable logic controller (PLC) model numbers, server hardware models, operating system versions, network component vendors or HMI products in NRC ADAMS.

REFERENCES

[1] Demonstrating the future of nuclear x ai. Aalo-X. [Online]. Available: https://www.aalo.com/aalo-x

[2] Department of energy celebrates first advanced reactor criticality. Department of Energy. [Online]. Available: https://www.energy.gov/articles/department-energy-celebrates-first-advanced-reactor-criticality

[3] Nrc issues construction permit for terrapower's natrium advanced reactor. Department of Energy. [Online]. Available: https://www.energy.gov/ne/articles/nrc-issues-construction-permit-terrapowers-natrium-advanced-reactor

[4] Advanced nuclear energy, delivered. Kairos Power. [Online]. Available: https://www.kairospower.com/

[5] Software security in supply chains: Software bill of materials (sbom). National Institute of Standards and Technology. [Online]. Available: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-supply-chain-security-guidance-20

[6] The minimum elements for a software bill of materials (sbom). National Telecommunications and Information Administration. [Online]. Available: https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

[7] M. D. (NRC), B. W. (NRC), J. L. (BNL), and V. M. (BNL), "Historical review and observatgions of defense-in-depth (nureg/km-0009)," Brookhaven National Laboratory, Tech. Rep., April 2016.

[8] Adams public search. Nuclear Regulatory Commission. [Online]. Available: https://adams-search.nrc.gov/home

[9] Defense in depth. Nuclear Regulatory Commission. [Online]. Available: https://www.nrc.gov/reactors/operating/ops-experience/fire-protection/defense-in-depth

[10] Defense in depth - a war for safety. Nuclear Regulatory Commission. [Online]. Available: https://www.nrc.gov/reading-rm/basic-ref/students/history-101/defense-in-depth

[11] X-energy llc - xe-100. Nuclear Regulatory Commission. [Online]. Available: https://www.nrc.gov/reactors/new-reactors/advanced/who-were-working-with/pre-application-activities/xe-100

[12] R. W. (ORNL), R. (ORNL), M. C. (ORNL), D. H. (ORNL), K. K. (ORNL), A. L. (ORNL), G. M. (ORNL), M. M. (ORNL), J. M. (ORNL), I. O. W.P. Poore, A. Q. (ORNL), T. W. J. (ORNL), and M. W. (NRC), "Diversity strategies for nuclear power plant instrumentation and control systems (nureg/cr-7007, ornl/tm-2009/302)," Oak Ridge National Laboratory, Tech. Rep., February 2010.

[13] N. Power, "Safety evaluation with open items (phase 2) (adams accession: Ml19191a196)," Nuclear Regulatory Commission, Tech. Rep., December 2019.

[14] ——, "Advanced safety evaluation (phase 4) (adams accession: Ml19192a011)," Nuclear Regulatory Commission, Tech. Rep., August 2020.

[15] ——, "Nrc-approved nuscale topical reports and associated safety evaluations (adams accession: Ml20197a370)," Nuclear Regulatory Commission, Tech. Rep., July 2020.

[16] ——, "Nusale final safety evaluation report (adams accession: Ml20023a318)," Nuclear Regulatory Commission, Tech. Rep., August 2020.

[17] ——, "Nuscale power, llc submittal of the nuscale standard design approval application part 2 - final safety analysis report, chapter 7, "instrumentation and controls," revision 0," Nuclear Regulatory Commission, Tech. Rep., December 2022.

[18] G. G. Preckshot, "Method for performing diversity and defense-in-depth analyses of reactor protection systems (nureg/cr-6303, ucrl-id-119239)," Lawrence Livermore National Laboratory, Tech. Rep., December 1994.

[19] X-energy llc - xe-100. Sandia National Laboratory. [Online]. Available: https://www.nrc.gov/reactors/new-reactors/advanced/who-were-working-with/pre-application-activities/xe-100

[20] F. D. P. W. Hutton, "Advanced reactor safeguards & security: Cybersecurity scenarios," Pacific Northwest National Laboratory, WA, Tech. Rep., October 2025.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov