Final Technical Report

Project Title: Methodology Development for Cybersecurity Robustness and Vulnerability Assessment of University Research Reactors

Covering Period: October 1st, 2015 through September 30th, 2018

Date of Report: February 28, 2019

Recipient:

North Carolina State University
P.O. Box 7909
Department of Nuclear Engineering
Raleigh, NC 27695-7909

Project Number: NEUP 15-8338

Principal Investigators:

Bernard W. Wehring
bwwehrin@ncsu.edu

Ayman I. Hawari
ayman.hawari@ncsu.edu

Collaborators:

S. A. Lassell (North Carolina State University)
J. S. Benjamin (Idaho National Laboratory)
K. T. Barnes (Idaho National Laboratory)
V. L. Wright (Idaho National Laboratory)

Executive Summary

In 2012, the U.S. Nuclear Regulatory Commission (NRC) formed a working group in collaboration with the Test, Research and Training Reactors (TRTR) group to review cyber security programs at US nuclear non-power reactor (NPR) facilities. Following their review of cyber security at four different university NPR (i.e. university research reactor (URR)) facilities, the NRC staff made recommendations for improvements at URR including 1) augmenting the URR licensees' understanding of the protective features provided with their physical security systems, 2) educating URR facility staff on cyber security issues, and 3) developing guidance to help the URR facilities maintain adequate cyber security going forward. [1]

This three-year project to develop and implement a cyber-security risk assessment methodology and defense-in-depth mitigation strategy for application at URR facilities provides solutions effectively addressing each of the recommendations given in the NRC review referenced above. In support of this project, cyber security documentation and guidance from the NRC [2][3], Department of Homeland Security (DHS) Industrial Control Systems (ICS) Cyber Emergency Response Team (CERT) [4], National Institute of Standards and Technology (NIST) [5], and the International Atomic Energy Agency (IAEA) [6][7], were reviewed. Most of this documentation did not take the unique resources, configuration, and infrastructure associated with URR facilities into account. The NRC-TRTR effective practices document [2] provides useful guidance for implementing cyber security protections at URR, but lacks a structured framework for systematically auditing facility digital control assets (DCA) and evaluating associated cyber threats, vulnerabilities, and risk. The outcomes from this project, therefore, seek to build on the general resources above by providing a straightforward DCA auditing and risk assessment methodology, as well as mitigation strategies, that may be implemented to address the risk of cyber-attack at URR facilities.

Introduction:

This final project report details the outcomes from a three-year research project to develop and implement a cyber-security risk assessment methodology and defense-in-depth mitigation strategy for application at URR facilities. The primary objectives of the project were to 1) develop a cyber-security and vulnerability assessment methodology and mitigation strategies for URR that can be shared with other research reactor owners, 2) hypothesize a credible vulnerability for a URR and resolve the potential impact and/or consequences of an attack against the vulnerability through application of theoretical, modeling and simulation, and an experimental proof-of-principle exercise, and 3) use the developed methodology and results to enhance the university training in cyber-security for reactor operators, and engineering students including nuclear engineers. Section 1 of this report provides a narrative summary of how these objectives were accomplished over the three-year project period. Section 2 discusses the iterative development of the risk assessment methodology, which is appended. Section 3 discusses the outcomes from the application of the risk assessment methodology at the PULSTAR reactor facility as a representative test case. Section 4 details the defense-in-depth mitigation strategies that were developed taking the unique facilities and resources associated with URR into account. Additional appendices to this report include a cyber-security course module outline, and publications disseminating the outcomes from this project to the URR community.

Section 1: Summary of Project Objectives and Year 1, 2 & 3 Activities

The following objectives were accomplished during Year 1 of the project.

1. **Train the assessment team to think more like attackers.** The lead assessment team member reviewed the documentation and ICS-CERT training content listed below, in addition to significant additional ICS cyber security documentation available from NIST and the IAEA: 1) NRC Regulatory Guide 5.71 – "Cyber Security Programs for Nuclear Facilities"[3]; 2) TRTR-NRC "Cyber Security; Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities"[2]; and 3) the Department of Homeland Security (DHS) Industrial Control System (ICS) Cyber Emergency Response Team (CERT) Web-Based Training Modules[4]. Subsequently, additional team members including student reactor operators reviewed these materials prior to performing research contributing to the project.

2. **Develop an assessment methodology by looking at the university reactor as a representative research reactor facility from an attacker's point of view.** Consulting the materials reviewed above, a risk assessment methodology was developed by looking at the university reactor from an attacker's point of view and applying the principles of "Operational Security" (OPSEC).

   The initial methodology incorporated the following basic steps:

   a. Perform a facility cyber-security baseline evaluation through a) identifying critical reactor systems, b) creating an inventory of Digital Control Assets (DCA) comprising each of these systems, c) performing an audit of the DCA, identifying asset location, hardware/software configuration and vulnerabilities, connectivity and network connection points, and for those DCA connected to local data networks, generating a network map detailing network configuration, firewalls and security layers; and d) evaluating existing institutional cyber-security infrastructure, culture, hygiene, procedures and training to determine whether they are adequate to protecting the research reactor facility DCA and SGI.

b. Perform a risk assessment for each DCA system or sub-system by evaluating potential threats from the point of view of an attacker (assessing attacker capability, intent and opportunity), assessing the vulnerability of each DCA to attack, and determining the consequences of cyber-attack on the DCA. Risk was determined as a function of the threat, vulnerability and consequence metrics as suggested by OPSEC practices.
c. Rank the risk associated with a cyber-attack on each DCA or system, and prioritize the mitigation of vulnerabilities found in the hardware, software, and/or network components of the DCA systems by ranking relative risk level.
d. Perform a separate reactor physical security system assessment following methodology developed in partnership with the INL site team and the Security Applications Technology (SAT) team at NC State.

3. **Perform an assessment of the specific university research reactor facility that is partnering in this project.** An initial assessment of cyber-security at the PULSTAR reactor facility was performed following the developed assessment methodology.

   a. An inventory of critical systems and digital equipment was performed and a list of 'Digital Control Assets' created. Extensive interviews and walk-downs were performed with facility operations and experimental staff to obtain a full understanding of how Digital Control Assets are deployed and utilized. An audit of identified DCA was performed as discussed under objective 2 above. DCA operating software, applications software, and firmware were checked for Common Vulnerability Exposures (CVE) utilizing ICS-CERT and NIST databases. Network maps were assembled for all DCA infrastructure with network connectivity. Facility procedures were reviewed.
   b. An initial risk assessment was performed for all DCA, evaluating attacker capability, intent, and opportunity, DCA vulnerabilities, and the potential consequences of a successful attack.
   c. An initial ranking of risk for each DCA was obtained, allowing an assessment of the effectiveness of the methodology.

The following objectives were accomplished during Year 2 of the project.

4. **Develop a risk assessment strategy/process from the collected data along with the objectives and purposes of a research reactor.** The assessment methodology developed in year 1 was revised and finalized, incorporating the lessons learned from the initial assessment and recommendations of the project team. The revised final risk assessment methodology is given in Appendix 1 to this report and discussed in Section 2 below.

5. **Perform a risk assessment of the specific university research reactor facility that is partnering in this project.** The risk assessment methodology was implemented by the research team to perform the full cyber security risk assessment of the PULSTAR Reactor facility. Five undergraduate student licensed reactor facility operators worked as part of the research team to assist with performing the full facility assessment. The undergraduates all completed the training as suggested by the methodology. A meeting was held between the project team and university staff from the NC State Office of

Information and Technology (OIT), Information and Security Services (ISS), and the Office of Security and Compliance. Vulnerabilities associated with the current reactor ICS network configuration as determined during the audit and risk evaluation were discussed along with strategies for mitigation. Mitigations involving reconfiguration of the local area network zones were discussed.

A set of initial questions developed by the INL project team were utilized to perform a risk assessment of the PULSTAR physical security system. The INL project team visited the facility in September 2017 to walk down and review the reactor physical security systems with the campus Security Applications and Technologies (SAT) group responsible for its operation and maintenance. The INL project team worked with the SAT staff to evaluate the cyber vulnerabilities associated with the facility physical security system. Extensive technical discussion of potential vulnerabilities provided additional training to the NC State SAT staff and reactor operations team.

The final risk assessment results are discussed in Section 3 below.

The following objectives were accomplished during Year 3 of the project.

6. **Develop and implement mitigations for the university research reactor facility.** The following defense-in-depth mitigation strategies were investigated to address the cyber-vulnerabilities identified during the facility risk assessment completed in Year 2.

   Strategy #1: Implement cyber security policies and procedures covering reactor ICS and train the reactor facility operations and research staff in effective cyber hygiene practices.

   Strategy #2: Harden reactor ICS networks though integrating under the university supported secure network infrastructure, employing software hardening tools such as whitelisting and anti-virus, and installing effective air gapping infrastructure.

   Strategy #3: Identify DCA hardware and software updates and patches that will a) allow any unsupported/outdated OS to be upgraded to current supported OS, and b) mitigate the CVEs identified for application and firmware without compromising the operation of the ICS networks.

   The mitigation strategies and the status of their implementation are discussed in Section 4 below.

7. **Integrate the findings into the engineering and training curriculum.** A cyber security course module for the NC State NE235 ‘Reactor Operations Training’ course was finalized and presented to enrolled students in both the Fall 2017 and Fall 2018 semesters, impacting a total of 37 students. The course module consists of a lecture and a lab session introducing cyber security concepts as applied to nuclear plant ICS, and includes content such as: operations security (OPSEC) concepts; good cyber-hygiene practices; identifying and auditing CDA supporting SSEP functions; the use of the ICS-CERT and NIST-NVD online databases for identifying and evaluating common vulnerability exposures (CVE); performing threat, vulnerability and risk assessments; identifying attack vectors and disrupting the cyber kill chain through defense-in-depth mitigation strategies; and reviewing the cyber assessment outcomes of the PULSTAR plant ICS as a case study. The students are also familiarized with resources such as the DHS ICS-CERT online training modules. The NE235 “Cyber Security of Nuclear Plant Industrial Control Systems” course module outline is provided in Appendix 2. Reactor operations staff, including student reactor operators, received cyber security hygiene training and reviewed reactor ICS cyber security procedural content.

8: **Share the newly developed cyber security assessment methodology with other research reactor owners.** A paper entitled "Methodology Development for Cybersecurity Vulnerability Assessment of University Research Reactors" was submitted and presented at the annual meeting of the American Nuclear Society in June 2018 (see Appendix 3). A presentation entitled "Cybersecurity Vulnerability Assessment and Defense-in-Depth Strategy for University Research Reactors" was given at the Test, Research and Training Reactors (TRTR) annual meeting in October 2018 (see Appendix 4).

Section 2 – Risk Assessment Methodology

The objective of the developed methodology is to present a comprehensive yet straightforward approach for URR staff to utilize in assessing the cyber security risks associated with reactor facility ICS and DCA. It was developed utilizing NRC guidance and general ICS assessment guidance available through DHS ICS-CERT. In developing the methodology, all process control systems and subsystems of the PULSTAR research reactor were reviewed and considered, searching for targets of opportunity. Systems reviewed included reactor operations and control, cooling loop infrastructure, radiation monitoring and safety, physical security, auxiliary and emergency systems, critical infrastructure including building utilities (electric, water, natural gas, HVAC), data acquisition, and educational and research systems. The methodology is tailored to take into account the resources and risks associated with URR facilities. Given the volumes of information available, effort was made to focus the audit and assessment activities in key areas that will provide facility owners and operators with a detailed overview of their deployed ICS architecture and associated threats and vulnerabilities. The specific information compiled will be useful in developing a comprehensive understanding of the configuration of the facility ICS DCA, and what steps may be taken to mitigate identified vulnerabilities and reduce risk. While NRC guidance was considered in its development, the methodology does not facilitate compliance with the NRC regulatory requirements as developed for nuclear power facilities.

The assessment methodology went through several iterations, as lessons learned from its implementation were incorporated. The audit procedure was modified and streamlined to require that only relevant and select information needed for evaluating the defined threat, vulnerability and consequence metrics is compiled. For example, in the original audit procedure, all of the CVE associated with PC based DCA operating systems were to be reviewed, numbering in the thousands. In the final version, this requirement was modified to only log whether a current and supported OS is installed and whether automatic updates are enabled. This was determined to be more valuable in assessing vulnerability and provide key and useful information to be utilized in mitigation activities. The Attacker Capability and Intent Index metrics were both modified to utilize content derived from searching the ICS-CERT Alert database to inform their settings, providing a more quantitative basis for evaluating these indices. The Network Protection index was modified to evaluate basic DCA digital connectivity and network protection parameters that represent key vectors for cyber-attack. The Vulnerability Scoring index was updated to incorporate parallel metrics for evaluating vulnerabilities in both the operating system software and in application software or firmware. An Interdependency Vulnerability metric was added to allow facilities to evaluate and review their potential vulnerabilities to dependencies on externally provided services such as building utilities and communications. The assessment methodology for the physical security system was developed in parallel in partnership with an assessment team from Idaho National Laboratory.

Lessons learned from a site walk-down of the reactor physical protection system by INL personnel at the PULSTAR facility were incorporated, with university personnel providing valuable feedback concerning the implementation of the methodology. Finally, cyber security procedural guidance derived from nuclear utility cyber security procedures was added as an attachment to the methodology for use by URR facilities in developing reactor ICS specific cyber security procedures and programs.

All of the audit and assessment metrics are designed to focus attention on key areas vital to assessing risk for cyber-attack. The full "Cyber-Security Risk Assessment Methodology for University Research Reactors" is given in Appendix 1 to this report.

Section 3 – Results from Risk Assessment of PULSTAR Facility

Reactor ICS Assessment Results:

The assessment methodology above was applied to review the PULSTAR reactor facility SSEP and experimental facility functions. 84 separate digital control assets (DCA) comprising these systems and functions were identified and audited. The majority of these DCA were located inside the physically protected area of the facility, and most of the reactor control and radiation safety related DCA either had no digital connectivity or were functionally air gapped. Most password protected DCA did not use default passwords, and most had a single administrator account without a least permissions architecture. Whitelisting was not utilized on any DCA, and antivirus software was only active on certain Windows 7 or 10 based systems. Most DCA had unused communication ports without physical port locks, and Wi-fi was not enabled for most DCA. A significant amount of information about facility experimental systems is available online on the facility website and in publications, but with limited details about the make, model and configuration of DCA. Interdependencies of DCA on externally supported infrastructure were evaluated, but most DCA either had redundant backup or defaulted to a fail-safe condition relative to their associated consequence metric. For networked DCA, limited network zones were utilized but associated firewalls were not maintained and used permissive default settings. Most networked DCA were connected directly to the campus network. Certain experimental system LAN utilized VPN protections, but no robust network protections were in place.

A search of the NIST NVD and ICS-CERT Advisories databases yielded more than 17,000 common vulnerability and exposures (CVE) related to the DCA operating systems and application software and firmware in use. Several experimental facility DCA utilized either outdated and unsupported operating systems, or current operating systems with automatic updates disabled. The CVE associated with these operating systems numbered in the thousands. CVE associated with DCA firmware and application software were limited in number and tabulated for evaluation during mitigation. A search of the ICS-CERT Alert database yielded information about general threats to ICS, and specific threats to programmable logic controllers (PLC).

No formal cyber security policies, procedures or training were in place for reactor ICS, including for maintaining air gaps and firewalls. Facility staff had general cyber awareness and maintained functional air gaps around critical equipment, but overall good cyber hygiene practices were lacking.

Following the audit of DCA, the metrics associated with the risk assessment were evaluated. Figure 1 below indicates the distribution of the Consequence Index metric associated with the facility DCA. The

DCA with CI values of 3 and 4 are primarily reactor control and radiation safety equipment. The lower CI values are primarily for auxiliary and experimental equipment.

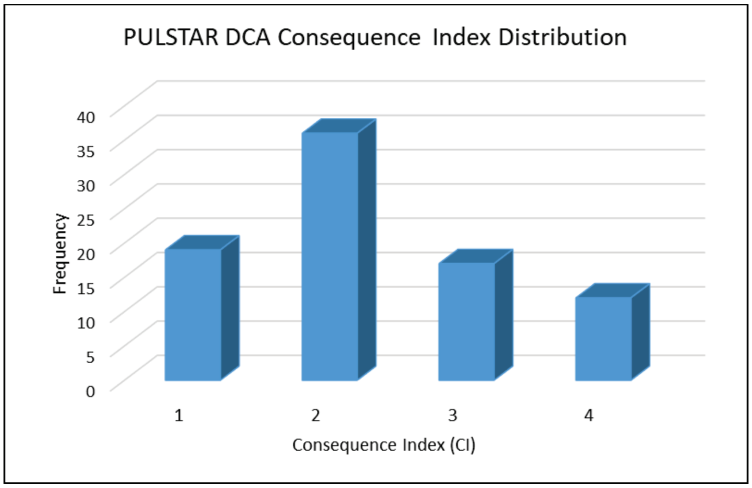


Figure 1 – Consequence Index Distribution

The distributions for the Vulnerability and Threat Indexes are given in Figure 2 below. The vulnerability index distribution is highly variable due to the independent nature of the metric variables for setting the Network Protection and Vulnerability Scoring indices. The higher vulnerabilities indicated are for certain networked experimental facilities. The Threat Index distribution is smoother, possibly due to a certain amount of correlation between the Attacker Capability and Intent Indices, as they are both set through reviewing the content of the ICS-CERT Alert database. The higher threat indices indicated are also primarily for certain networked experimental facilities.

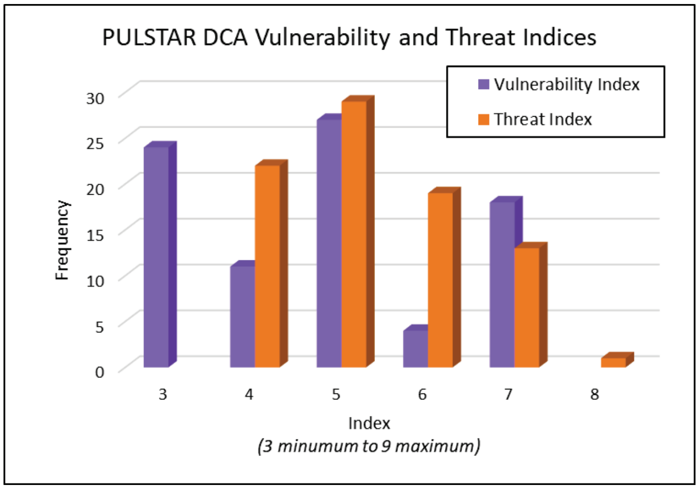


Figure 2 – Distribution of Vulnerability and Threat Indices

Utilizing the analyzed consequence, threat and vulnerability metrics to calculate the relative Risk Index (RI) values for each DCA results in the distribution shown in Figure 3 below. According to the methodology, any DCA with RI values ≥0.5 are accorded the highest priority for mitigation, 0.5 > RI ≥ 0.25 are of medium priority, and RI < 0.25 are the lowest priority. The RI values above 0.3 as shown in Figure 3 are all for networked experimental DCA equipment with limited network protections and higher amounts of published system information available. Certain process data recorders had RI values of between 0.25 to 0.3, due primarily to higher consequence indices and functional air gapping without procedural controls. All reactor control and radiation safety equipment had RI values of less than 0.25, being functionally air gapped with limited or no digital connectivity. The lowest RI values (i.e. <0.10) were for auxiliary support equipment, and certain experimental equipment with low consequence indexes.

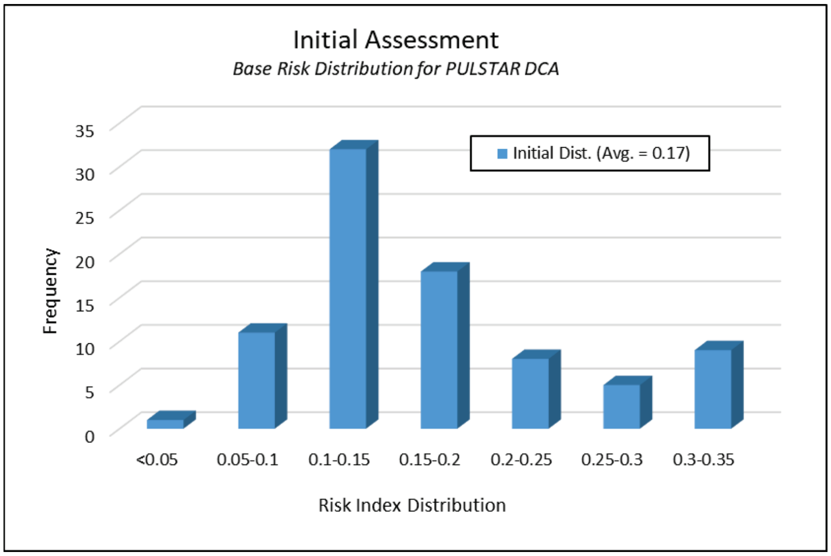


Figure 3 – Risk Index Distribution for Initial Assessment of PULSTAR DCA

Physical Security System Assessment Results

The scope of the reactor facility physical security system assessment by the INL project team included evaluating the hardware, software, network infrastructure, and implementation procedures provided by the Security Applications Technologies (SAT) group on campus. A secondary goal of the assessment was to test an approach that could be applied to evaluate physical security systems at other research reactor facilities. The INL project team provided SAT personnel with a preliminary list of questions about the configuration of the physical security system which were reviewed and answered. The INL team members performed a walk down of the system equipment and were given hands on access to test equipment at the SAT office.

Following their review, the INL team identified concerns with 1) the configuration of the multifactor identification readers, 2) publicly addressable IP for certain networked equipment, 3) virtualized authentication servers residing on the same hardware as non-security virtual machines, and 4) the potential for email spoofing to circumvent access authorization procedures. SAT personnel provided feedback and assisted with refining the questions to be used in assisting with the review and evaluation of physical security systems at other facilities. The updated and finalized physical security system assessment methodology is included in Appendix 1. The items of concern involving publicly addressable IP's and email spoofing have been addressed. The items of concern identified involving upgrades to the networked access control hardware and authentication servers are under review by SAT and will be implemented as resources permit.

Section 4 – Mitigation Strategy Development & Implementation

A standard defense-in-depth approach to mitigating the threats and vulnerabilities identified as driving elevated risks to the reactor ICS DCA has been formulated. The approach is tailored to take into account the unique resources and risks associated with URR facilities. The primary objective of the approach is to apply limited URR facility resources strategically and efficiently towards mitigating the identified threats and vulnerabilities that lead to the increased risk of cyber-attack on ICS DCA.

The approach employs three main strategies:

1) Implement cyber security policies and procedures covering reactor ICS and train the reactor facility operations and research staff in effective cyber hygiene practices.
2) Harden reactor ICS networks though integrating under the university supported secure network infrastructure, employing software hardening tools such as whitelisting and anti-virus, and installing effective air gapping infrastructure.
3) Identify DCA hardware and software updates and patches that will a) allow any unsupported/outdated OS to be upgraded to current supported OS, and b) mitigate the CVEs identified for application and firmware without compromising the operation of the ICS networks.

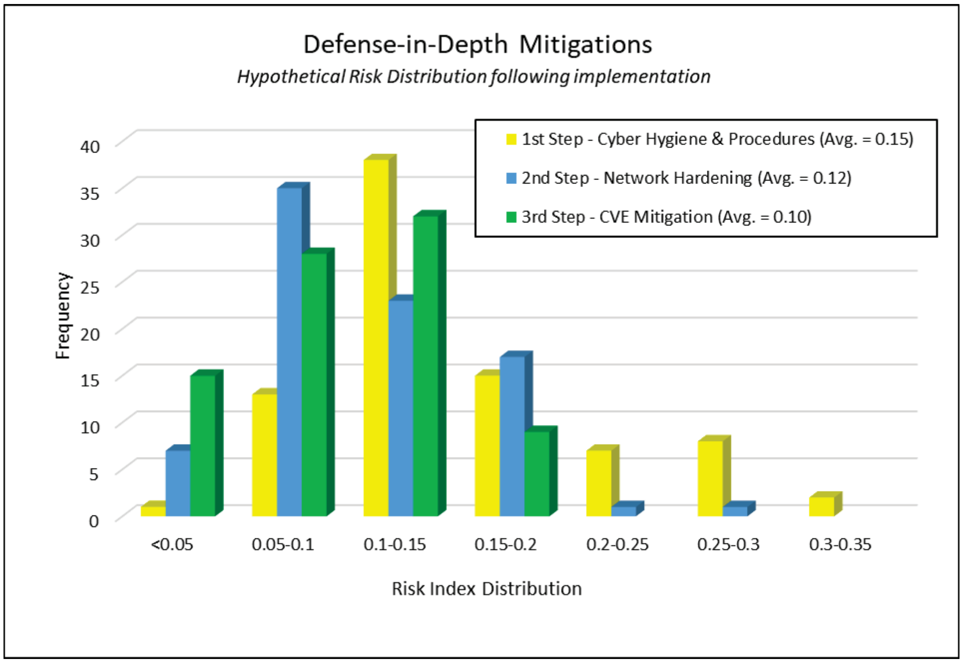


Figure 4 – Risk Index Distribution following three successive stages of mitigation

Taken in order, the strategies require a progressively increasing commitment of resources to achieve risk mitigation. The time and money required to implement policies, procedures and training is small compared to that required to upgrade hardware and software, so it is appropriate to undertake strategy number one first, followed by the second and third. The risk index values obtained as a result of the assessment may also be utilized to prioritize mitigation, which may be approached serially or on a case-by-case basis. In the serial approach, DCA with high RI values would have their vulnerabilities and threats addressed first, with mitigations for those with lower RI values following as resources permitted. Alternately, risks identified for high consequence index DCA may be elected for priority mitigation, even if their RI values are less than those for other DCA.

Given that there are commonalities between the vulnerabilities and threats affecting the various facility DCA, it is suggested to implement the first two strategies above thus mitigating significant risk for all DCA, and then selectively implement the third strategy as resources permit. Figure 4 presents the hypothetical shift in the risk index distribution following the implementation of each of the three strategies. Figure 5 below details how the average value of the risk distribution decreases following the hypothetical implementation of each strategy. It is clear that implementing strategies one and two yield a significant reduction in overall risk, with a slightly diminishing return for the implementation of strategy number three. Assuming full mitigation measures are taken, the residual risk yields RI values in the range of 0.03 – 0.11 depending on the consequence index. Given the resources require to implement the third strategy as discussed below, it is evident that it should only be applied selectively to mitigate residual level risk for high consequence index DCA.

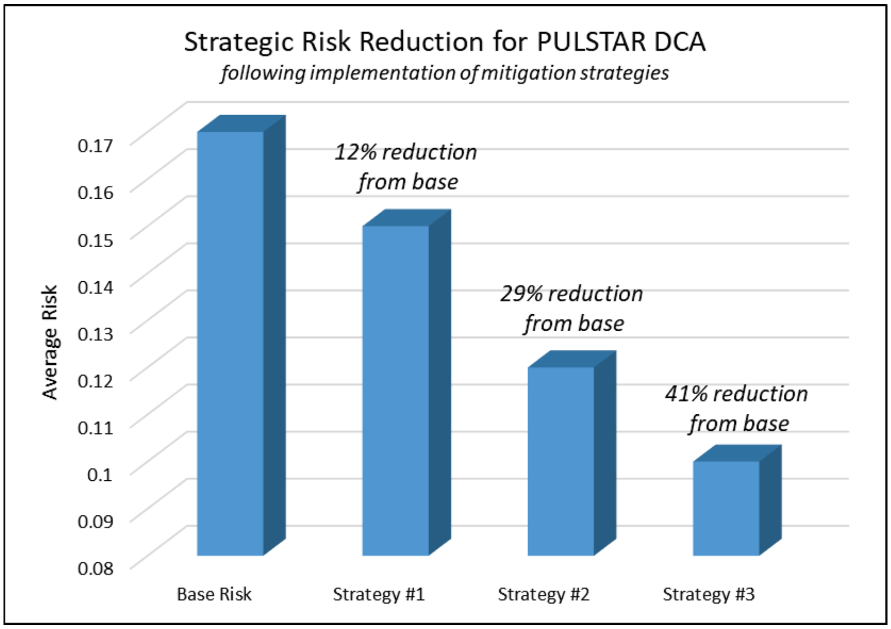


Figure 5 – Average Risk Index reduction following mitigation stages

Strategy Development & Implementation

The mitigation strategies as introduced above were developed for implementation at the NC State PULSTAR Reactor Facility. As a representative URR with plant systems similar to those of other university reactors, these strategies will be generally applicable to reducing cyber risk at all URR facilities.

Strategy #1 - *Implement cyber security policies and procedures covering reactor ICS and train the reactor facility operations and research staff in effective cyber hygiene practices.*

Procedural content relevant to research reactor facilities was extracted from procedures obtained from a nuclear utility and URR cyber security procedural guidance has been generated. This guidance is attached in Appendix 1 and may be utilized as source material for generating facility specific ICS cyber security programs. Initial cyber security training of reactor operations and experimental staff at NC State has been performed. Implementation of procedures and additional cyber security hygiene training of operations staff and users is in process.

Strategy #2 - *Harden reactor ICS networks though integrating under the university supported secure network infrastructure, employing software hardening tools such as whitelisting and anti-virus, and installing effective air gapping infrastructure.*

Local Area Network Hardening Strategy for URR DCAs

Local Area Networks (LAN) connecting reactor ICS DCA must be protected and segmented from the university LAN and the internet. It is recommended to utilize properly maintained and configured network protection to isolate and protect ICS network segments. DCA with a High Consequence Index per the DCA audit procedure (e.g. a CI value of ≥3) should either be air gapped or protected behind at least two layers of network protection (e.g. in Segment 2 or 3 as detailed in Figure 6 below) utilizing firewalls and/or data diodes. Additional protective measures include utilizing VPN, intrusion detection and prevention systems (IDS/IPS), and a host-based intrusion detection system (HIDS). Designing and installing zoned network protection should be performed by network professionals, and the campus information technology department may be a useful resource. Useful resources detailing network hardening methodology are listed below.

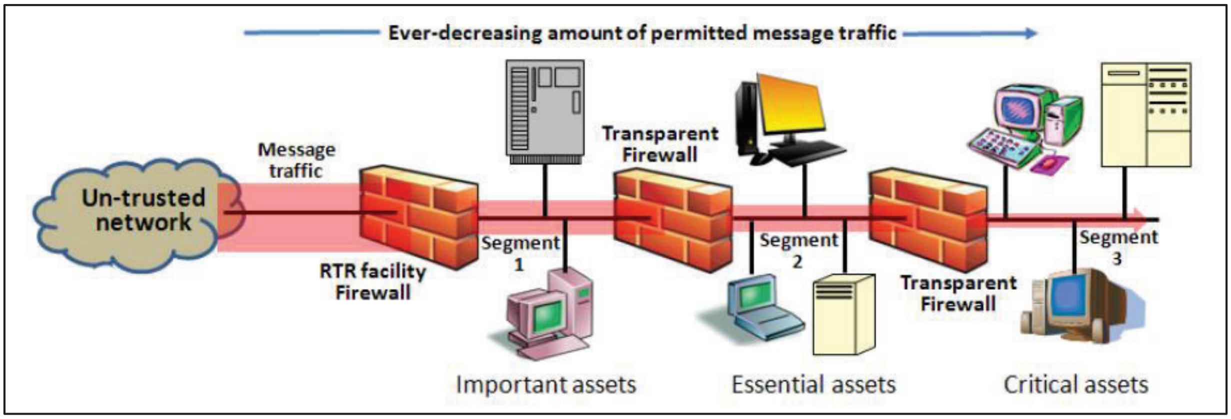


Figure 6 - NRC-TRTR Effective Practices Document; Creating defense-in-depth with LAN segmentation

Network Infrastructure Hardening Guidance and Resources:

- *TRTR-NRC "Cyber Security; Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities" – Section 6: "Network Architectural (and) Interconnectivity Issues"*
- *ICS-CERT Training Module 210W-03: Cybersecurity for Industrial Control Systems – Common Industrial Control System Components*

- *ICS-CERT Training Module 210W-10: Cybersecurity for Industrial Control Systems – Mapping IT Defense-in-Depth Solutions – "3rd Layer – Network Security" section.*
- *ICS-CERT Secure Architecture Design at* https://ics-cert.us-cert.gov/Secure-Architecture-Design

Network Hardening Implementation at the PULSTAR Reactor

The NCSU Office of Information Security (OIS) proposes to establish three subnet zones to protect the reactor facility CDA. These subnets will be included under the firewalled 'Research-1' university network, which incorporates an intrusion detection system. Zone 1 will be for DCA that must be connected to reactor systems and do not need to be accessed from machines external to the reactor facility. Zone 2 will be for DCA that must be connected to reactor systems and do need to be accessed from machines external to the reactor facility. Zone 3 will be for DCA that need to receive data from machines in Zone 1 or Zone 2 or from machines external to the facility, but do not need to send data to Zones 1 and 2. The zones will be separated from each other using either firewall rules with restricted rule sets, or access control lists (ACL) allowing only authorized network traffic. Implementation and installation of network security upgrades will proceed as resources permit, however it is anticipated that this will be completed by the second quarter of 2019.

Software/Hardware Hardening for URR DCAs

The following are general recommendations for hardening the hardware and software of DCAs comprising the URR ICS. This guidance was primarily obtained from a review of nuclear utility cyber security procedures. A discussion of configuring firewalls and other network protective infrastructure, including air gapping infrastructure and procedures is given in Appendix 1.

a) Application Whitelisting (AWL): Utilize AWL on ICS workstations to restrict the software that may be enabled and utilized, thereby protecting against the installation and running of malware. Useful guidance from ICS-CERT for how to implement whitelisting on ICS entitled "Guidelines for Application Whitelisting in Industrial Control Systems" is available at: https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf

b) Anti-Virus: If possible, anti-virus software shall be installed, updated, and operational on all capable and supported devices. Update all anti-virus software with the most recent virus signature files as they are made available through 3rd party vendor processes. The following apply to anti-virus software:

   (1) Automate virus scans and updates, where possible.
   (2) Scan all software for viruses before initial installation.
   (3) Scan all files, such as e-mail file attachments or web site downloads, for viruses before the file is opened or executed.
   (4) Scan all PMMD (e.g., diskettes, compact disks, zip disks) for viruses prior to use or on-access on any digital process system.
   (5) Immediately report confirmed malware infections.

   Some digital systems and equipment cannot operate properly when installing or having installed virus protection software on the system or equipment. Examples of this type of systems or equipment include, but are not limited to, the following:

   (1) Devices that run proprietary operating systems (e.g. firmware or no operating system) and therefore don't support anti-virus software.

(2) Systems where vendor doesn't support anti-virus software because it interferes with equipment operation.

(3) Safety related systems that do not support anti-virus software.

c) Work with DCA vendors to 1) remove or disable any hardware or software feature that is not directly required for the DCA to perform its intended function and 2) maintain the most current protective features on those functions that are retained.

d) Java, JavaScript, ActiveX, Postscript, Shockwave movies, Flash animations, VBscript, and macros should not be used unless required by the DCA to perform its functions. Office software, such as Microsoft Office products, and internet browsers should not be installed and utilized on DCA unless required by the DCA to perform its functions.

e) If the DCA supports software device authentication (i.e., has the ability to restrict use of portable media and mobile devices (PMMD) to predefined devices), then it should be implemented. This feature may already be bundled into existing virus protection software. If the DCA does not support software device authentication, then perform one of the following:

(1) Logically disable ports in conjunction with a passcode-protected basic input-output system (BIOS) (preferred) or disable ports in the operating system (OS), requiring administrator access to re-enable.

(2) Implement physical controls to block unauthorized access to the ports by installing hardware port locks on any unused data ports (e.g. USB, Ethernet, serial, HDMI, etc…)

f) Disable any wireless DCA connectivity (e.g. Wi-fi, Bluetooth), unless required by the DCA to perform its functions.

Implementation of DCA Software/Hardware Hardening at the PULSTAR Reactor

Application whitelisting software such as Windows AppLocker and Symantec Advanced Threat Protection are being evaluated for installation on PULSTAR facility DCA network workstations. Air-gaping infrastructure including kiosks and flash media from OPSWAT and TRESYS have been evaluated, but have been found to be costly, with the least expensive option costing $13,000 upfront and with recurring annual fees. Alternate lower cost scanning tools for implementing air gapping need to be investigated. Other hardening methods as detailed above, including updated anti-virus protection and software device authentication, are being considered for implementation on facility DCA. Implementation and installation of DCA software and hardware hardening upgrades at the PULSTAR facilities will proceed as resources permit.

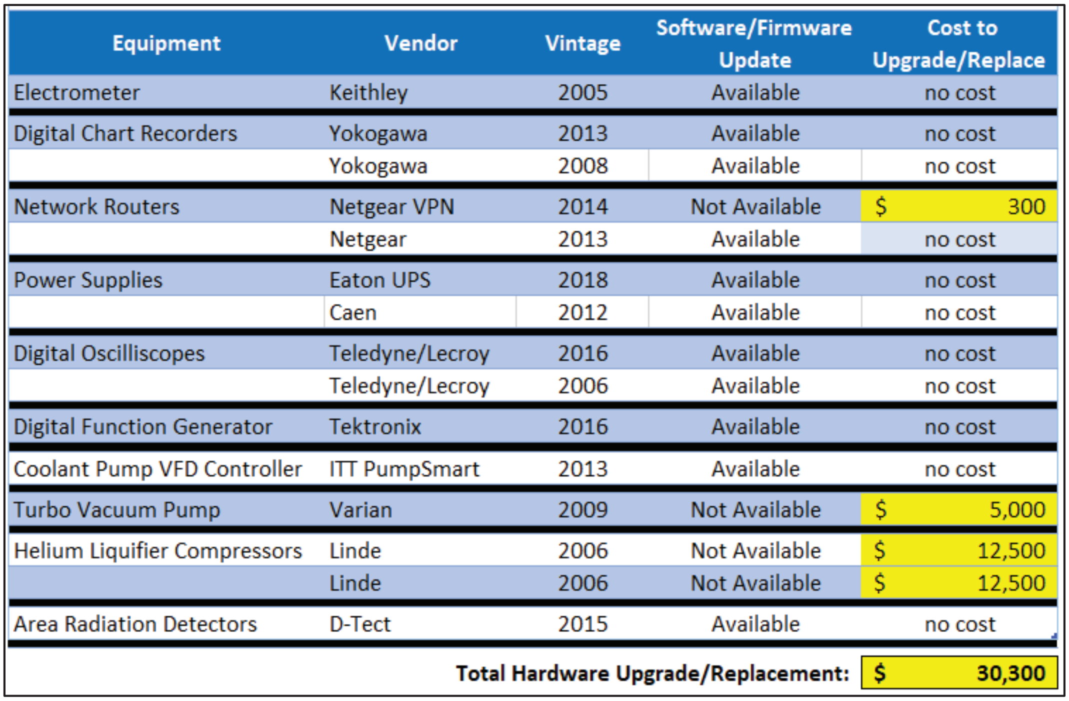
Strategy #3 - *Identify DCA hardware and software updates and patches that will a) allow any unsupported/outdated OS to be upgraded to current supported OS, and b) mitigate the CVEs identified for application and firmware without compromising the operation of the ICS networks*.

A key outcome of the assessment performed for PULSTAR DCA was the determination that outdated operating systems (OS) represent a significant vulnerability and are a key element in increasing the attack surface. Thousands of CVE were identified for the installed OS, including versions of MS Windows dating back to XP. Windows versions prior to OS 7 are no longer supported with patches or updates from the vendor and are therefore extremely vulnerable to attack. A key mitigation priority would therefore be to update all installed OS to versions supported by the vendor thereby enabling continuing protection against malware and known exploits. The issue with this strategy when applied to ICS and

SCADA networks is assuring that all installed hardware and associated drivers, applications software, and firmware are compatible with the supporting workstation OS.

Extensive reviews of specifications and datasheets obtained from DCA vendors for all 84 audited PULSTAR DCA have been performed. The majority of reactor control and experimental system DCA are still supported by vendors, with updates for associated drivers and firmware compatible with current OS versions available at little to no cost. Table 1 provides a representative sampling of the facility DCA evaluated, with their vintage, whether software drivers and firmware updates are available, and the cost. Support for only four facility DCA was discontinued, all comprising experimental facilities. The direct cost to replace the outdated hardware with new supported models would be $30,300, with significant additional costs incurred for the effort required by reactor and experimental facility staff to redesign the systems and implement the upgrades. Additionally, extensive work would remain to evaluate whether updated software may be installed without compromising the operation of the associated ICS. The PULSTAR facility does not currently have capabilities for ‘sandboxing’ to model ICS network upgrades before implementation. Therefore, for PULSTAR ICS systems running outdated OS, the interim strategy is to fully implement air gapping and application whitelisting solutions to isolate and protect the systems from malware. The replacement of unsupported experimental infrastructure will most likely be deferred until R&D funding is obtained for facility improvements and upgrades. Upgraded DCA and associated ICS infrastructure would be designed to utilize current versions of OS, firmware and application software thus effectively mitigating the identified CVE. Additional software and hardware evaluation and updates will proceed as resources permit.

Table 1 – Select Results for PULSTAR ICS DCA Hardware Evaluation



Equipment	Vendor	Vintage	Software/Firmware Update	Cost to Upgrade/Replace
Electrometer	Keithley	2005	Available	no cost
Digital Chart Recorders	Yokogawa	2013	Available	no cost
	Yokogawa	2008	Available	no cost
Network Routers	Netgear VPN	2014	Not Available	$ 300
	Netgear	2013	Available	no cost
Power Supplies	Eaton UPS	2018	Available	no cost
	Caen	2012	Available	no cost
Digital Oscilliscopes	Teledyne/Lecroy	2016	Available	no cost
	Teledyne/Lecroy	2006	Available	no cost
Digital Function Generator	Tektronix	2016	Available	no cost
Coolant Pump VFD Controller	ITT PumpSmart	2013	Available	no cost
Turbo Vacuum Pump	Varian	2009	Not Available	$ 5,000
Helium Liquifier Compressors	Linde	2006	Not Available	$ 12,500
	Linde	2006	Not Available	$ 12,500
Area Radiation Detectors	D-Tect	2015	Available	no cost
			Total Hardware Upgrade/Replacement:	**$ 30,300**

Firmware and application software for PULSTAR DCA were checked for CVEs as part of the audit using the ICS-CERT Advisories database and NIST National Vulnerability Database (NVD). 33 separate CVE were identified, with associated Common Vulnerability Scoring System (CVSS) base scores ranging up to the maximum value of 10. The CVE identified impacted experimental research infrastructure and educational systems, with none being identified for reactor control, auxiliary or safety system related DCA. Additional work is needed to evaluate whether CVE patches and software updates may be installed without compromising the operation of the associated experimental ICS.

An excellent resource for additional ICS network hardening strategies is given by the *TRTR-NRC "Cyber Security; Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities" Appendix C – Effective Practices Summary*.

Conclusions

The URR ICS cyber security assessment methodology was developed from the point of view of attackers utilizing the PULSTAR Reactor as a test case. It represents a comprehensive strategy for auditing and evaluating cyber security risk for URR SSEP and experimental ICS. The methodology provides detailed guidance for identifying DCA, performing audits, performing threat and vulnerability assessments utilizing online databases, determining relative risk to facility DCA of cyber-attack, for developing ICS specific procedures, and performing assessments of the physical security system infrastructure. Defense-in-depth mitigation strategies have been presented along with an analysis of their relative effectiveness at reducing risk. Implementing procedures, training and network and software hardening tools mitigates a large fraction of the risk and may be accomplished through leveraging university resources while incurring minimal cost. Addressing outdated DCA OS and software CVE presents a more challenging problem requiring a staged solution. The interim use of air gapping and application whitelisting to protect DCA with outdated OS is recommended, deferring replacement of unsupported hardware and updating to current OS until undertaking routine funded facility upgrades. The implementation of the assessment methodology and mitigation strategy at the PULSTAR reactor has substantially reduced the risk to the facility from cyber-attack. A cyber security course module has been developed and included in the nuclear engineering curriculum at NC State and has been presented over the past two years. Training on cyber security hygiene and protection of URR ICS has been provided to senior reactor operations and experimental staff, and to student reactor operators. The outcomes from this project have been disseminated to the national research reactor community at two national meetings.

References

[1] "Cyber Security for Non-Power Reactor Facilities"; Working Group Final Report; U.S. NRC (2014).

[2] NRC-TRTR Working Group, "Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities"; ML15253A060 (2016).

[3] NRC Regulatory Guide 5.71 – Cyber Security Programs for Nuclear Facilities; ML090340159 (2010).

[4] Available at website https://ics-cert.uscert.gov/Training-Available-Through-ICSCERT

[5] Available at website https://nvd.nist.gov

[6] ST037 TECDOC - Conducting Computer Security Assessments; IAEA-TDL-006 (2016).

[7] IAEA Pub1527 – Computer Security at Nuclear Facilities, ISSN 1816–9317, no. 17 (2011).

NC STATE
UNIVERSITY

NRP
Nuclear Reactor Program

Appendix 1

Cyber-Security Risk Assessment Methodology for University Research Reactors

September 28, 2018

Nuclear Reactor Program

North Carolina State University

Introduction

This cyber security risk assessment methodology was developed for use by university research reactor (URR) facilities to assess the risks of cyber-attack on digital equipment comprising industrial control system (ICS) infrastructure. The primary objective is to provide a straightforward guide to performing cyber risk assessments taking into account the configuration and resources of the typical URR facility.

Three primary sources of information were reviewed and utilized in developing this methodology: 1) NRC Regulatory Guide 5.71 – "Cyber Security Programs for Nuclear Facilities"; 2) TRTR-NRC "Cyber Security; Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities"; and 3) the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (CERT) Web-Based Training Modules. NRC Regulatory Guide 5.71 is geared primarily towards nuclear power facilities, so guidance provided in TRTR-NRC Effective Practices document was incorporated to tailor this methodology for application at URR facilities. The ICS-CERT modules provide useful information for understanding and evaluating cyber security for ICS systems in general.

Section 1 of this methodology recommends that URR staff review the documentation referenced above for background information helpful to understanding and performing a comprehensive cyber security assessment of reactor ICS. Section 2 details a comprehensive baseline audit procedure for identifying digital control assets (DCA) and determining their configuration and associated vulnerabilities. Once the audit has been completed, Section 3 provides guidance for evaluating the results and assessing threat, vulnerability and consequence metrics for each audited DCA. Section 4 utilizes the metrics from Section 3 to determine a relative Risk Index for each DCA. The outcomes from the risk assessment completed in Section 4 may then be utilized to prioritize mitigation efforts. Section 5 details a separate procedure developed for assessing cyber vulnerabilities associated with URR physical security systems. Attachments A and B provide content related to the evaluation of the Interdependency Metric and Physical Security System. Attachment C provides draft URR Cyber Security Procedural Content and Guidance for use in reviewing and developing facility ICS cyber procedures.

Once this assessment procedure is completed, the URR facility will have a thorough understanding of the current status of their cyber security hygiene, the configuration and vulnerabilities of their ICS systems, and the risk presented to those systems for cyber-attack.

Risk Assessment Methodology

Section 1 - Industrial Control System (ICS) Cyber Security Training

All URR facility staff performing this assessment should take the following web based training modules to familiarize themselves with cyber security topics and their application to Industrial Control Systems. The following Department of Homeland Security (DHS) Industrial Control System (ICS) Cyber Emergency Response Team (CERT) Web-Based Training Modules are available at https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT:

a) Operational Security (OPSEC) for Control Systems (100W)
b) Cyber Security Industrial Control Systems (210W):
   i. 210W-01 Differences in Deployments of Industrial Control Systems
   ii. 210W-02 Influence of Common Information Technology (IT) Components on ICS
   iii. 210W-03 Common ICS Components
   iv. 210W-04 Cybersecurity within IT and ICS Domains
   v. 210W-05 Cybersecurity Risk
   vi. 210W-06 Current Trends – Threats
   vii. 210W-07 Current Trends – Vulnerabilities
   viii. 210W-08 Determining the Impact of a Cybersecurity Incident
   ix. 210W-09 Attack Methodologies in IT and ICS
   x. 210W-10 Mapping IT Defense-in-Depth Security Solutions to ICS

In addition, the documents referenced below were found to be relevant and useful in training URR staff for cyber awareness. It is recommended to read the full TRTR-NRC Effective Practices document, and to review relevant sections of the NRC Regulatory Guide.

a) TRTR-NRC "Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities"; https://www.nrc.gov/docs/ML1525/ML15253A060.pdf
b) NRC Regulatory Guide 5.71 – Cyber Security Programs for Nuclear Facilities; https://www.nrc.gov/docs/ML0903/ML090340159.pdf

Section 2 - Baseline Evaluation and Audit of URR Facility Safety, Security and Emergency Preparedness (SSEP) functions and Digital Control Assets (DCA)

In performing a baseline cyber security evaluation, it is important to properly identify the systems within the URR facility that perform Safety, Security and Emergency Preparedness (SSEP) functions as described in 10 CFR 73.54(a)(1), and discussed in NRC Regulatory Guide 5.71, section A.3.1.3. Section 4 of the TRTR-NRC effective practices document suggests that systems supporting critical URR facility functions, including SSEP functions, should be reviewed. As listed in Table 1 below, this methodology includes educational and research systems, and building management and utility systems in the review as well.

Table 1 – Critical URR Functions for Review

Physical security of the facility.*
Detection of unsafe/unauthorized conditions.
Personnel access monitoring and control.
Reactor safety.
Reactor operational control.
Emergency response/communications.
Storage and protection of Safe Guarded Information (SGI).
Accurate inventory/location of nuclear materials.
Networked educational and research systems, including experimental facilities.
Building management and utility systems, including HVAC, electrical, water, natural gas, and telecommunications.

* *Note: Physical Security System functions are audited and assessed in Section 5 of this assessment procedure, so should not be audited under this section.*

Once the critical facility systems to be reviewed have been identified, the next step is to properly identify the Digital Control Assets (DCA) that comprise each identified system or sub-system, and any interdependencies with associated externally controlled systems. This assessment procedure utilizes the term 'Digital Control Asset' as distinguished from, and not to be confused with, the regulatory term 'Critical Digital Asset' as utilized in NRC Regulatory Guide 5.71. The flow chart in Figure 1 below (as adapted from Regulatory Guide 5.71 Section C.3.1.3) may be applied to differentiate DCA from digital assets that would fall outside the scope of this assessment.

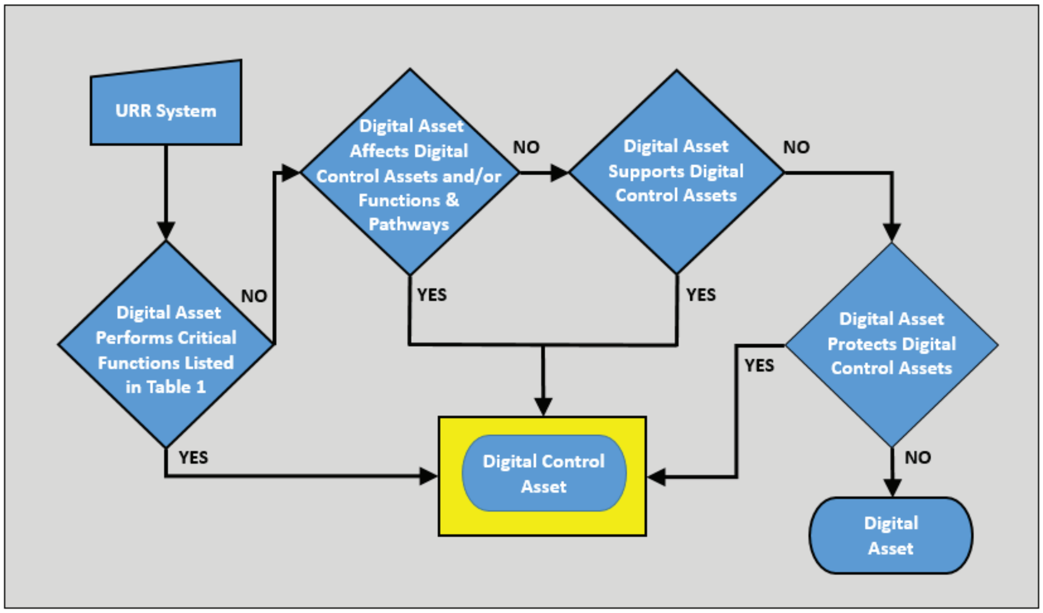

URR System
Digital Asset Performs Critical Functions Listed in Table 1
NO
YES
Digital Asset Affects Digital Control Assets and/or Functions & Pathways
NO
YES
Digital Asset Supports Digital Control Assets
NO
YES
Digital Asset Protects Digital Control Assets
YES
NO
Digital Control Asset
Digital Asset

Figure 1 – Evaluation process for identifying Digital Control Assets.

Any equipment or devices containing digital components (including Programmable Logic Controllers (PLCs) or chipsets) that are used to perform critical URR functions listed above are defined as DCA. Digital assets that affect, support, or protect the functioning of DCA are also considered digital control assets for the purpose of this assessment. Therefore, for systems connected to a local area network, the DCA for evaluation would include ICS workstations and supporting network hardware such as routers, switches, data diodes, and intrusion detection systems.

DCA Inventory and Audit

Create an inventory and perform an audit of all Digital Control Assets (DCA) identified in the process above and document the existing associated cyber-security related infrastructure and procedures. This process includes performing an inventory of all DCA hardware and software components, determining associated digital communications connectivity, and tracing the network architecture. Utilize a spreadsheet or database to list DCA and compile information concerning all parameters audited below. The information compiled will inform the setting of the threat, vulnerability, and consequence metrics discussed under section 3 below.

The inventory and audit process includes the following steps:

a) Inventory and audit all identified URR facility DCA. Determine the following functional and configuration information for each DCA:
   i. Critical reactor system or function (e.g. SSEP, experimental system) the DCA comprises, performs, affects, supports, or protects.
   ii. Configuration information for each DCA component:
      1. DCA manufacturer (vendor) and model. *NOTE: If the DCA is controlled via an integrated PLC, the make and model of the PLC should be identified and included in the audit.*
      2. A list of software installed:
         a) Operating system software and/or firmware, version, whether the version is supported by the vendor, and whether automatic updates are enabled.
         b) Application software and version.
         c) If whitelisting software is installed and enabled.
         d) If antivirus protection software is installed, enabled, and actively updated.
      3. Digital connectivity:
         a) Local – Does the DCA have USB, Ethernet, Serial/COM, or other communication ports? Are port locks installed for unused ports?
         b) Remote - Does the DCA have remote connectivity (e.g. Wifi, Bluetooth, etc…)? If so, is it enabled or disabled?
      4. A list of all personnel with accounts/user IDs on the DCA, and whether 'least permissions' restrictions are in place.
      5. A list of administrative passwords required to enable/use/operate the DCA. Note whether default system and software passwords have been changed.
   iii. The DCA component's level of physical protection. Is it inside a physically secured area, or in an un-secured area generally accessible to non-authorized personnel?
   iv. Evaluate interdependencies of DCA on externally supported infrastructure and services, such as building utilities (water, electric, gas, HVAC) and telecommunication and network services using

the guidance given in Attachment A. Provision of these services may have direct impacts on the critical functions of the facility, but the facility does not typically have direct control over these services. Interdependencies should be identified and assessed for impacts to critical functions.

v. The amount of information published or otherwise available online about the particular DCA and the configuration of the associated system. Are schematics or detailed descriptions of facility systems (e.g. experimental systems, control systems, emergency systems) available on the facility website, in publications, in educational materials, or in publicly available licensing documents?

b) Identify and quantify known threats, vulnerabilities and exploits for DCA firmware and/or application software using the DHS ICS-CERT and National Institute of Standards and Technology (NIST) vulnerability search engines. The ICS-CERT 'Alert' database provides timely notification concerning threats or activity with the potential to impact critical infrastructure computing networks, and also whether exploitation tools and/or ICS focused malware have been released. The ICS-CERT 'Advisories' database and NIST National Vulnerability Database (NVD) provide information about current security issues, and known vulnerabilities and exploits for ICS hardware and software. Common Vulnerability Exposure (CVE) entries contain extensive information concerning the nature of vulnerabilities, their potential impact and exploitability, and associated mitigation resources. CVSS base scores for each CVE are calculated based on a formula incorporating metrics that approximate the ease and impact of the exploit, allowing the severity of the CVE to be quantified. The information compiled from these reviews will inform the setting of the threat and vulnerability metrics discussed under section 3 below.

NOTE: Operating system software for workstations (e.g. MS Windows, OS-X, or Linux) are likely to have hundreds or thousands of CVE's detailing known exploits and vulnerabilities which would be onerous to evaluate under the scope of this assessment. The Vulnerability Scoring Index (VSI) metric discussed under section 3(b) below evaluates the vulnerabilities associated with PC operating systems separately.

DHS ICS-CERT Alerts and Advisories Databases

Review the Alerts and Advisories databases available at https://ics-cert.us-cert.gov/ to check for specific alerts and advisories related to DCA hardware and software. Use the 'List by Vendor' option to search for specific DCA hardware, firmware, and software by manufacturer, while being sure to review the 'Other' category.

- Alerts specific to each DCA, including installed software, should be reviewed and assessed to determine if a specific threat or activity has been identified that could impact the DCA. Log whether there are identified emerging threats or an identified increase in activities by malicious groups, including hacktivist or anarchist groups, and whether they generally target ICS infrastructure, or specific facility DCA. Determine and log whether exploitation tools and/or ICS focused malware have been released targeting specific DCA or vendors.
- Advisories specific to each DCA, including installed software, should be reviewed and a list of known CVE and associated CVSS base scores compiled. Log CVE identification numbers for use in mitigation review.

NIST National Vulnerability Database

Review the NIST NVD available at https://nvd.nist.gov to search for known vulnerabilities specific to DCA hardware, firmware, and software. Go to the "Vulnerabilities – CVE" database and perform a basic, overview keyword based search entering DCA hardware, firmware, and software manufacturers, models, and version identifiers. The search may yield a list of known CVE associated with the keywords. It will be important to verify whether each CVE result listed is applicable and relevant to the version or model of DCA utilized. Each CVE result includes a detailed description of the vulnerability and potential mitigations and patches from vendors. Perform a comprehensive search for each audited DCA, compiling a list of all identified and relevant CVE and their associated CVSS base scores.

c) Determine the digital connectivity of each DCA and the associated network architecture. The information compiled will inform the setting of the vulnerability metrics discussed under section 3 below.

   i. Determine device communication protocols & configuration and log the following information:

      1. Is the DCA connected to a local area network (LAN) via a physical or remote (e.g. Wifi) connection, or air gapped?
      2. Determine the IP and MAC addresses for all networked DCA.

   ii. Tracing Network Maps:

      1. Build a graphic map of the local network architecture detailing connection points for all DCA, including ICS hardware components, network switches and routers, hardware firewalls, data diodes, computer workstations, and any intrusion detection/prevention systems.
      2. Determine whether network zones are utilized. Network zones may employ firewalls, virtual private networks (VPN), data diodes, or other technology to segment the network and restrict communications between zones and increase security. Determine the location and configuration of firewalls and/or VPN and whether they a) are properly configured and b) are actively maintained. Guidance concerning the proper application of firewalls and other network protection may be found in the TRTR-NRC Cyber Security guide and the ICS-CERT online training modules.
      3. Review all local and remote communications connections to DCA to verify that there are not any unauthorized or 'rogue' connections.

d) URR facilities should evaluate their existing institutional cyber-security culture, policies, procedures and training to determine whether they are adequate to protecting the research reactor facility ICS DCA and SGI. Many institutions have cyber security policies in place for protecting information technology (IT) systems, but these policies may not be applied to protect reactor facility ICS DCA. Elements of comprehensive cyber-security culture, policies and procedures may be obtained by reviewing NRC Reg. Guide 5.71, Appendix B Technical Security Controls, and Appendix C Operational and Management Security Controls. Additional URR cyber security procedure guidance is provided in Attachment C - URR Cyber Security Program Procedural Guidance.

   At a minimum, an effective cyber security culture should contain the following basic elements:

   i. Cyber Security Policy Statement – A policy statement formalizing management commitment to implementing effective cyber security practices.

   ii. Procedures – Procedures covering DCA password administration, 'least permissions' access controls, documentation of configuration settings and backups, configuring and administration of firewalls and other network protective infrastructure (e.g. VPN, data diodes), physical protection requirements, disabling unneeded wireless communication functionality (Wifi, Bluetooth), effective air gapping requirements and scanning of portable media, vendor controls, encryption requirements for SGI, incident response and reporting, and performing periodic audits.

iii. Training - All URR personnel should receive a basic introductory and refresher training covering cyber security policies and established facility procedures as discussed above. Additional training topics should include good cyber-hygiene practices including phishing awareness, proper use of social media (e.g. LinkedIn, Facebook), and limiting the availability of important facility design and configuration information on the web.

Section 3 - Risk Assessment of DCA

The information obtained in the baseline DCA audit in Step 2 above may now be utilized to perform a cyber-risk assessment for each identified reactor facility critical system or sub-system. The function, configuration, threat and vulnerability search results, and digital connectivity parameters identified for each DCA may be utilized to determine associated threat, vulnerability and consequence metrics. These metrics provide the basis for quantitatively identifying and evaluating the cyber security risk for each system. Potential threats to each DCA may be evaluated from the point of view of an attacker, assessing attacker capability, intent and opportunity using defined metrics. The vulnerability of each DCA to attack may be evaluated by reviewing its connectivity, network architecture, interdependencies, and known vulnerabilities and exploits and ranking using the defined metrics. The consequences of a successful attack on each DCA may be evaluated by considering its function and the reactor system it comprises, affects, supports, or protects and ranked using the defined metric.

a) Threat Metrics:

Threat metrics include attacker capability, attacker intent, and attacker opportunity, and may be assessed through evaluating the information compiled during in the audit. It is appropriate to interpret and evaluate these metrics conservatively, given the uncertainty regarding the nature of the threat actor.

i. Attacker Capability is defined as the means or resources the attacker would require to carry out an attack, including needed skills, expertise, knowledge, money & tools. For the purpose of this assessment, the availability of certain exploitation tools or malware will be utilized to assess attacker capability. Any identified release of exploitation tools (e.g. targeting specific PLCs) or ICS focused malware obtained in the review of the ICS-CERT 'Alerts' database under step 2(b) above is applicable to setting this metric.

Evaluate the audited DCA and rate the Attacker Capability Index (ACI) for each.

Attacker Capability Index (ACI):

ACI	Parameter
1	**Low -** No exploitation tools or malware identified that could impact facility ICS or DCA.
2	**Medium -** Exploitation tools or malware identified that could generally impact facility ICS.
3	**High -** Specific exploitation tools or malware identified that could impact specific DCA.

ii. Attacker Intent, for the purposed of this assessment, is defined based on whether emerging threats, or an identified increase in activities by malicious groups, including hacktivist or anarchist groups, have been identified as targeting DCA. The data obtained in the review of the ICS-CERT 'Alerts' database is applicable to setting this metric. In the review completed in Step 2(b) above, the Alerts database was reviewed to determine if any emerging threats or activities have been identified that generally target ICS infrastructure, or that target the specific type(s) of facility DCA.

Evaluate the audited DCA and rate the Attacker Intent Index (AII) for each.

Attacker Intent Index (AII):

AII	Parameter
1	**Low –** No Emerging threats identified; no identified increase in activities by malicious groups, including hacktivist or anarchist groups, targeting ICS infrastructure or specific type of DCA.
2	**Medium -** Emerging threat(s) identified general to ICS infrastructure; identified increase in activities by malicious groups, including hacktivist or anarchist groups, generally targeting ICS infrastructure.
3	**High –** Emerging threat(s) identified specific to DCA; identified increase in activities by malicious groups, including hacktivist or anarchist groups, targeting specific type of DCA.

iii. Attacker Opportunity is the set of conditions that need to be met for an adversary to be confident their attack will be successful. Opportunities are related to the exposure and vulnerability of targets. This can be related to the level of physical access an adversary has to a DCA target, as well as access to specific knowledge about the system. Attacker opportunity is therefore increased if DCA are located outside an access controlled and physically protected area, and/or if physical communication port locks (e.g. on USB, Ethernet, and serial ports, etc…) are not installed. Attacker access to specific knowledge about DCA may be increased if the facility lacks good cyber hygiene practices or has not implemented effective cyber security policies, procedures, and training for staff and users. Good cyber hygiene practices include restricting the amount of information published about the DCA utilized in the facility, and providing awareness training for staff to reduce the threat from phishing attacks and from other attack vectors. The effective implementation of cyber security policies and procedures reduces the attack surface and an attacker's opportunity for penetrating the facility ICS. For example, a low attacker opportunity index level may be applicable if the DCA is inside the physically protected area, minimal information is publicly available about the DCA model and configuration, and effective cyber hygiene practices, policies, procedures and training are in place. A high attacker opportunity index level may be applicable if the DCA is physically accessible, extensive information is readily available about the DCA model and configuration, or the facility has poor cyber hygiene and has not implemented policies and procedures for ICS.

NOTE: The opportunity an attacker may have arising from the level of remote access to DCA targets is measured using the Network Protection Index vulnerability metric detailed in section 3(b)(i) below.

Evaluate the audited DCA and rate the Attacker Opportunity Index (AOI) for each.

Attacker Opportunity Index (AOI):

AOI	Parameter
1	**Low -** Must meet all of the following criteria: i) Physical access to the DCA is restricted (i.e. it is in a secured cabinet or room) and communication port locks are installed. ii) Specific information about DCA, including model numbers and system descriptions or schematics, are not published or available online. iii) Effective cyber hygiene practices are in place, and the facility implements official cyber security policies, procedures and training.
2	**Medium –** Must meet all of the following criteria: i) There is limited or intermittent physical access to DCA, or communication port locks are not installed. ii) Limited specific information about DCA may be published or available online. iii) "Ad hoc", unofficial, or otherwise limited cyber hygiene practices, policies, procedures, and/or training are in place.
3	**High** - Conditions that do not meet requirement given for 1 or 2 above.

b) Vulnerability Metrics:

DCA vulnerability is related to factors including 1) how well the DCA is protected by effective network security measures including network zones with properly configured and maintained firewalls, and effective cyber security administrative controls, 2) the availability to potential attackers of known exploits specific to the DCA hardware and software, and 3) the level of interdependency of the DCA on externally supported critical services. The following vulnerability metrics should be used to rate the vulnerability of each DCA audited in Step 1 above.

i. Network Protection Index (NPI): Determining whether a DCA connected to a network is well protected from unauthorized online access is a function of the network security measures that are in place. In the baseline audit, information was collected for each DCA including: local network zone architecture, IP addresses, configuration of firewalls, remote connectivity (e.g. Wifi capability), local connectivity (e.g. Ethernet, USB, serial ports), and user permissions and password protection. If DCA are not connected to a network (i.e. air-gapped) but may be accessed by portable media and mobile devices (PMMD) (e.g. flash, SD or other digital media), these media must be managed, scanned, and secured appropriately to prevent the inadvertent transfer of malware to the DCA. DCA connected to a LAN located behind properly configured firewalls in a layered network zone architecture, or on a VPN, would be less vulnerable to attack. Layered network zones employ increasing levels of firewall protection and access control restrictions to reduce the potential for unauthorized access to DCA. DCA with 'least user permissions' and robust password protection are also better protected. DCA located on an open network protected by only an enterprise firewall and using default or weak passwords would be more vulnerable to attack.

Evaluate the audited DCA and rate the Network Protection Index (NPI) for each.

Network Protection Index (NPI):

NPI	Parameter
1	Must meet all of the following criteria: i) DCA has either a) no local or remote digital connectivity, b) is effectively air gapped with commensurate procedural controls, or c) has ≥2 levels of maintained network protection (i.e. firewalled zones not including enterprise firewall, VPN, etc…).

	ii) No capability for portable media and mobile devices (PMMD) or media capability is "controlled" (scanned, secured, maintained, etc.). iii) Robust password protections are in place in accordance with the device capability and are regularly changed, maintained, or updated. Least permissions access restrictions employed where supported.
2	Must meet all of the following criteria: i) DCA is functionally air-gapped (e.g. no LAN/Wifi connection, but without PMMD scanning infrastructure) or isolated from public network via at least one maintained firewall that is not the enterprise firewall. ii) Passwords or passcodes in use, with no defaults enabled or used.
3	All other assets that do not meet requirement given for 1 or 2 above.

ii. Vulnerability Scoring Index (VSI): The hardware, firmware and application software components of DCA as audited during the baseline evaluation were checked for known vulnerabilities using the DHS ICS-CERT 'Advisories' database and NIST NVD Search Engine. These database search results yielded Common Vulnerabilities and Exposures (CVE) security issues specific to the DCA, and provided a Common Vulnerability Scoring System (CVSS) severity ranking 'Base Score' of 0 to 10 for each result, with 10 being the highest vulnerability rating. Additional information was provided for each CVE, with detailed descriptions of the vulnerability and potential mitigations and patches from vendors. For each audited DCA, review the CVE found, their CVSS base score, and potential mitigations.

In addition, for computer workstation based DCA, the operating system software and version, whether automatic updates are enabled, whether whitelisting software is utilized, and whether antivirus protection software is installed, enabled, and actively updated was determined.

Using this data, evaluate the rate the Vulnerability Scoring Index (VSI) for each audited DCA.

Vulnerability Scoring Index (VSI):

VSI	Parameter
1	**Operating System Software (For PC/workstation based DCA):** Current supported OS version installed and automatically or actively updated – OR – if automatic updates are disabled, whitelisting software is installed and maintained; antivirus software is installed, enabled, and actively updated. *- AND -* **Application Software or Firmware:** No CVE's identified for installed software versions.
2	**Operating System Software (For PC/workstation based DCA):** Current supported OS version installed but not automatically updated and whitelisting software is not installed or maintained; antivirus software is installed, enabled, and actively updated. *- AND -* **Application Software or Firmware:** ≤ 3 CVE identified for current version with maximum associated Common Vulnerability Scoring System (CVSS) Base Score(s) ≤ 6.9.
3	Conditions that do not meet the requirements given for 1 or 2 above.

iii. Interdependency Vulnerability Index (IVI): Interdependencies identified and documented under step 2(a)(iv) above using the guidance given in **Attachment A** should be reviewed to set the

Interdependency Vulnerability Index (IVI) of each DCA using the metrics below. Most DCA will be dependent on electrical power, and some may be dependent on externally controlled network services.

Interdependency Vulnerability Index (IVI):

IVI	Parameter
1	Meets one or more of the following criteria: i) The service provider can 'Fully Meet the Conditions' required in order to support the interdependent service or function under all conditions. ii) Redundant backups exist that fully mitigate any loss of service from the provider (e.g. backup generator providing electrical power, cell phone communication –vs- land line, backup parallel network connection, emergency water supply, etc…). iii) Loss of service results in DCA or SSEP system defaulting to a fail-safe condition relative to the associated consequence metric.
2	Meets one or more of the following criteria: i) The service provider can 'Partially Meet the Conditions' required in order to support the interdependent service or function, or only under limited conditions. ii) Redundant backups exist that only partially or temporarily mitigate any loss of service from the provider (e.g. backup generator providing limited electrical power, limited communication backup, etc…)
3	All other interdependencies that do not meet the requirements given for 1 or 2 above.

c) Consequence Metrics:

The consequences of a successful cyber-attack on URR DCA would vary from low to critical levels depending on the function of the related system as determined during the audit. An attack on an experimental system may corrupt data, damage equipment, or potentially lead to unsafe conditions. An attack on safety related equipment could increase the probability of radiation exposure or injury to personnel. An attack on the reactor control or emergency systems could cause an operator to take an action that could adversely impact the facility, cause damage to the reactor, or in the worst case potentially cause an uncontrolled release offsite.

Review each ICS DCA audited in step two above giving consideration to its SSEP function and/or the reactor or experimental system it comprises, affects, supports, or protects, and rate the following consequence metric if the DCA was successfully attacked:

Consequence Index (CI):

CI	Parameter
1	**Low Level Consequence** – Attack on experimental facilities or non-safety related equipment causing administrative burdens, including theft or corruption of experimental data or safeguarded documents.
2	**Medium Level Consequence** – Attack on experimental facilities or auxiliary systems resulting in potential loss of service, loss of control, or damage to equipment.
3	**High Level Consequence** – Attack on safety related equipment, instrumentation, or radiation monitoring system resulting in an increased probability of radiation exposure or injury to personnel.

4	**Critical Level Consequence** – Attack on reactor control or emergency systems resulting in an elevated probability of a loss of control, of damage to reactor systems, of potential diversion of radioactive material, or an uncontrolled release offsite.

Section 4 - Rank Risk and Prioritize Mitigation

The risk associated with a cyber-attack on each DCA or system may now be assessed utilizing the threat, vulnerability and consequence metrics evaluated in Steps 3(a), (b), and (c) above. The metrics are utilized to calculate the Threat, Vulnerability and Risk Indices as discussed below. The normalized Risk Index (RI) may then be utilized to prioritize the mitigation of vulnerabilities found in the hardware, software, and/or network components of the DCA comprising facility systems. Certain DCA may be more or less at risk for cyber-attack than previously assumed, so this ranking is useful in identifying where to focus mitigation efforts and resources.

The Risk Index (RI) may be determined as follows:

Threat Index (TI) = ACI + AII + AOI

Vulnerability Index (VI) = NPI + VSI + IVI

Risk Index (RI) = [TI x VI x CI]/C *(where C is a normalization constant set equal to 324)*

The larger the Risk Index (RI) value, the larger the associated risk of a successful cyber-attack on the DCA and systems evaluated. The resulting risk index (RI) rankings may be utilized to identify systems most at risk for cyber-attack and prioritize resources for mitigating the identified vulnerabilities.

The Risk Index may be utilized to prioritize mitigation as follows:

Risk Index (RI)	Mitigation Priority
RI ≥ 0.5	Highest Priority for mitigation.
0.5 > RI ≥ 0.25	Medium Priority for mitigation.
RI < 0.25	Lowest Priority for mitigation.

Section 5 - Physical Security System Assessment

At typical university research reactor installations, the physical security system is comprised of facility monitoring and access controls that are administered and controlled over a secure campus network. The administration, operation, and maintenance of the reactor facility physical security system (RFPSS) and related network functions are typically performed by a separate campus entity on which the reactor facility is dependent. For the purpose of this assessment, it is assumed that the personnel responsible for the RFPSS have the required competencies necessary for installing, operating and maintaining the security system and related network infrastructure. Attachment B provides an assessment methodology that may be provided to these personnel to assist them with identifying potential procedural, software, and hardware related cyber vulnerabilities in the physical security system infrastructure. The reactor facility staff should work closely with the physical security system administrators to implement the assessment procedure, identify vulnerabilities, and prioritize potential mitigations.

Attachment A: Evaluating Interdependencies

Interdependencies

Interdependencies can fall into one of four general categories which can be used as an aid in identification: physical connections, digital pathways, geographic, and other (see Figure 1, Interdependency Categories). Physical connections include the inputs and outputs of two agents, such as electrical power and analog. A digital pathway interdependency is when an asset is dependent on information transmitted through digital communication infrastructure. A geographic or proximity interdependency includes the simultaneous change of states in local infrastructure due to environmental events. Lastly, 'other' will be used for all other interdependencies such as economics, policy, or public perception. The leading literature on critical infrastructure interdependencies often refers to the 'other' category as a logical interdependency.

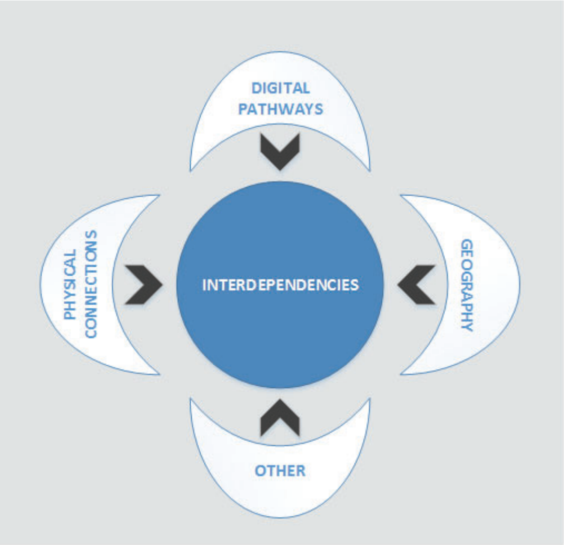


Figure 1- Interdependency Categories

Identification of Interdependencies

Identification and documentation of interdependencies is essential to a cybersecurity assessment; these interdependencies may be susceptible to a cyber-attack impacting reactor operations or providing an attack pathway to the digital systems within the research reactor facility. Identification of physical connection interdependencies should occur during the Baseline Evaluation Audit of Digital Control Assets (DCA) in Section 2 of the Assessment Methodology. Examples of external physical connection interdependencies are DCA connected to building utilities (i.e. electrical, water, HVAC), or equipment connected to a system that can only be serviced by a vendor. Identification of digital pathway interdependencies occurs under section 2(c) of this assessment methodology, auditing digital connectivity of the DCA. Systems that require digital communication will utilize a network architecture (switches, firewalls, cabling, etc.) where parts or all of that network architecture may not be controlled by the facility. Geographic interdependencies are not evaluated as part of this methodology. For the purposes of this methodology, 'other' category will be the catch-all category of interdependencies, encompassing any identified interdependencies effecting DCA that do not fit into the other categories.

Common Interdependencies for Research Reactors

The subset of critical infrastructure services that research reactors are most dependent on likely includes, at a minimum, physical security, water, electrical power, information, and telecommunications (physical security functions are evaluated separately under section 5 of the assessment methodology). The loss of any of these systems may pose a significant risk to the operations of the research reactor. A distinction should be made between interdependencies and dependencies; particularly in the context of research reactors, most of the reliance on external infrastructure is a one-way dependency. Few, if any, of the services provided with the research reactor are essential to the continued operation of the external infrastructure (see Figure 2).

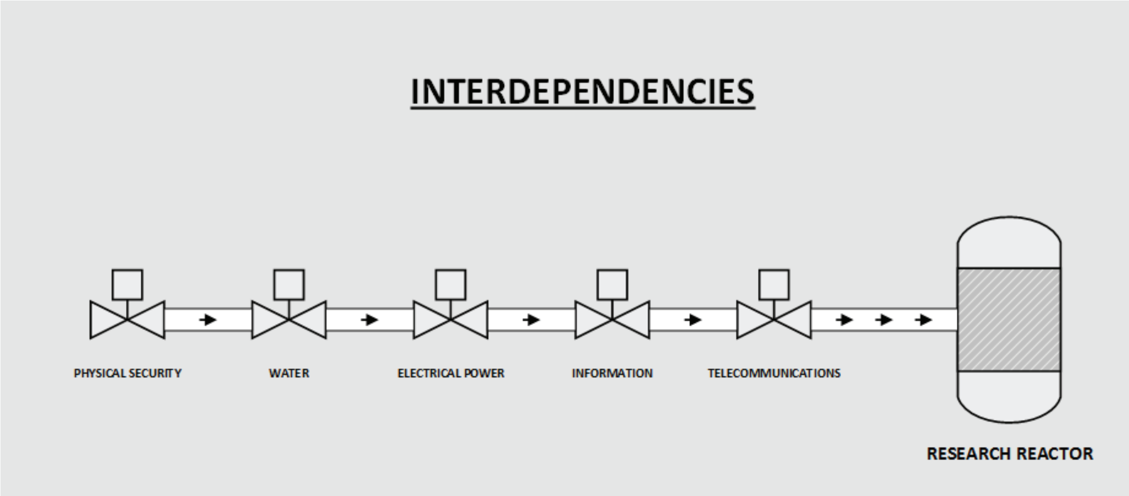


Figure 2 - Common Interdependencies for Research Reactors

Communicating with External Interdependency Service Providers

If any of the identified interdependencies require external services or sources, or is outside of the control of the research reactor facility, the service provider should be notified and understand the conditions required of their service. Important considerations are whether the service provider can partially or fully guarantee the conditions and whether a cyber-attack against the service provider could prohibit, interrupt, or delay the service. If the service provider is unable to guarantee the conditions, then the reactor facility should document manual actions to take in the event of service interruption. Form #1 below provides a structure for capturing the (inter)dependencies on external facility services.

FORM#1 - EXTERNAL INTERDEPENDENCY DOCUMENTATION

SYSTEM INFORMATION

System Name:

System Description:

System Owner:	Contact Information:

INTERDEPENDENCY INFORMATION

CATEGORY	**SERVICE PROVIDER INFORMATION**
□ Physical Connections	Company Name:
□ Digital Pathways	Address:
□ Other	Telephone Number:
	Contact Person:

Service Provider:	**REQUIRED CONDITIONS**
□ Can Fully Meet Conditions	
□ Can Partially Meet Conditions	
□ CANNOT Guarantee Conditions	
Service Provider:	Contact Individual:

IN CASE OF EMERGENCY

Required Actions:

Attachment B
Physical Security Assessment Methodology

Overview

The goal of the university's cyber security program as applied to the reactor facility physical security system (RFPSS) should be to apply and maintain defense-in-depth strategies to ensure identified digital control assets (DCA) have the capability to detect, prevent, respond to, mitigate, and recover from cyber-attacks. The protection strategies require defense-in-depth, or multiple layers of security controls. These multiple layers ensure that a failure of one security control does not result in an adverse impact to the digital control asset. For example, per NRC Regulatory Guide 5.71, "if a failure in prevention were to occur such as a violation of policy or if protection mechanisms were to be bypassed (e.g., by a new virus that is not yet identified as a cyber-attack), mechanisms would still be in place to detect and respond to an unauthorized alteration in an impacted critical digital asset (CDA), mitigate the impacts of this alteration, and recover normal operations of the impacted CDA before an adverse impact".

Security controls such as those listed in NRC Regulatory Guide 5.71, NEI 08-09, and NIST 800 can be linked to one or more of the following objectives: detect, prevent, respond to, mitigate, and recover from cyber-attacks. There may be circumstances where a security control cannot be implemented. In that situation, an acceptable alternative is to eliminate threat/attack vectors associated with the digital control asset. These vectors typically include: physical access, network connections including wireless, portable media and mobile devices, and the supply chain. For those situations, the best practice is to physically restrict access to the DCA, monitor and record physical access to the DCA to detect and respond to intrusions in a timely manner, use auditing or validation measures to detect unauthorized access and modifications to the DCAs, ensure that individuals who have access to the DCA are qualified, and ensure that those individuals are trustworthy and reliable.

Scope

The scope of this assessment should include evaluating the hardware, software, network infrastructure, and implementation procedures comprising the RFPSS. The four major components of a typical physical security system include a door access control system, a digital camera monitoring system, an intrusion detection/prevention system, and a Virtual Local Area Network (VLAN). These components are comprised of digital control assets typically installed, administered, maintained and monitored by campus administrative units separate from the reactor facility. This guidance should be utilized by those units in coordination with the reactor facility staff to review the physical security system infrastructure and identify potential vulnerabilities, or gaps in the hardware, software, network infrastructure, and implementation procedures of the reactor physical security system.

Assessment of the RFPSS

Targeted questions have been developed seeking to assist knowledgeable RFPSS administrators and technical staff with identifying potential cybersecurity vulnerabilities. The following list of questions is to be considered in the review of the RFPSS function, configuration and administration:

1. Credential Management (biometrics and RFID):
    a. Do all credentials reside in the same database?
    b. Who has the access to administer these credentials?

   c. Are multiple (multi-factor) credentials required to gain access?
   d. Are separate administrator roles broken out specifically for these credentials?
   e. What is the procedure for adding new people?
   f. Are there procedures in place to remove these credentials when people leave, or no longer need access?
   g. Is there an audit procedure for the access list? If so, how often are audits conducted?
   h. Is anyone notified by the security system when credentials are added or changed? What mechanisms are in place to audit changes to credentials?
   i. Are there policies and procedures in place to remediate lost badges and other tokens in a timely manner?
   j. Are personnel trained to promptly report a lost badge, or do people lose their badges and typically not report it for a few days?

2. Security System Architecture:
   a. What happens to the security system when a loss of power occurs?
   b. What happens during an IT failure?
   c. Is there redundancy for command and control of the security system?
   d. To what extent are the security networks hardened and physically separated from other campus networks?
   e. Who has physical access to the security console and other hardware/software involved in the security system?
   f. Who has physical access to network devices which are part of the security system?
   g. Are badging servers virtualized and residing on the same hardware as other non-security related virtual machines?
   h. Do any networked physical security DCA have publicly facing IP addresses?
   i. Are door access readers true multi-factor? Are separate wiegand strings sent to a remote secure server for dual authentication, or is authentication performed locally at the reader?
   j. Are the door access readers physically hardened to prevent tampering? Are any tamper switches enabled?
3. Video Surveillance:
   a. Is there video surveillance of all of the reactor facility physical access points?
   b. Is the video surveillance actively monitored?
   c. Do video feeds in the monitoring center automatically populate following the initiation of an alarm condition?
4. Physical Security System Alarms & Response:
   a. What are the alarm conditions?
   b. Who monitors alarming?
   c. Are there eyes the security console 24x7, or is it a pager or message based system where responders are performing other duties?
   d. What is the response procedure for alarms?
   e. How is the response escalated?
   f. What is the acceptable response time?
   g. Are procedures and training in place to help responders prioritize when multiple events take place in multiple locations?

Attachment C
URR Cyber Security Program Procedural Guidance

Following the development and implementation of the vulnerability assessment strategy at the NC State PULSTAR Reactor facility, a defense-in-depth approach to mitigating the identified threats and vulnerabilities was developed for application at URR facilities. This mitigation strategy was developed drawing from the outcomes of the risk assessment and evaluation of the PULSTAR reactor ICS, and the following documentation and training resources: 1) nuclear utility cyber security procedures; 2) the TRTR-NRC "Cyber Security; Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities" document; 3) the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (CERT) Web-Based Training Modules; and 4) NRC Reg. Guide 5.71, Appendix B Technical Security Controls, and Appendix C Operational and Management Security Controls.

This document discusses the procedural controls that should be implemented to protect URR ICS, and incorporates select content from nuclear utility cyber security procedures. URR facilities should evaluate their existing institutional cyber-security culture, policies, procedures and training to determine whether they are adequate to protecting the research reactor facility ICS DCA and SGI. Many institutions have cyber security policies in place for protecting information technology (IT) systems, but these policies may not be applied to protect reactor facility ICS DCA.

At a minimum, an effective cyber security culture should contain the following basic elements:

1. Cyber Security Policy Statement – A policy statement formalizing management commitment to implementing effective cyber security practices.
2. Procedures – Procedures covering DCA password administration, 'least permissions' access controls, documentation of configuration settings and backups, configuring and administration of firewalls and other network protective infrastructure (e.g. VPN, data diodes), physical protection requirements, disabling unneeded wireless communication functionality (Wifi, Bluetooth), effective air gapping requirements and scanning of portable media, vendor controls, encryption requirements for SGI, incident response and reporting, and performing periodic audits.
3. Training - All URR personnel should receive a basic introductory and refresher training covering cyber security policies and established facility procedures as discussed above. Additional training topics should include good cyber-hygiene practices including phishing awareness, proper use of social media (e.g. LinkedIn, Facebook), and limiting the availability of important facility design and configuration information on the web.

Guidance and draft procedural content is provided below. This content should be reviewed and considered for incorporation into facility ICS cyber security procedures.

Draft URR Cyber Security Procedural Content and Guidance

1. URR Cyber Security Program Statement

Facility management is committed to implementing effective cyber security practices to protect the reactor facility industrial control system (ICS) digital control assets (DCA). Therefore, the objective of this cyber security program is to leverage industry standards and best practices to protect facility systems and detect potential problems. Good cyber security hygiene is the responsibility of all facility staff and users, and each has a responsibility to comply with facility cyber security guidelines and procedures.

2. Passwords

Any passwords for accessing DCA and use accounts should meet the same organizational administrative requirements as those for IT systems, such as the number and type of characters required, and how often passwords should be changed.

Any default passwords or passcodes for DCA that are factory presets should be changed as soon as the DCA is deployed.

All usernames and passwords/passcodes for facility DCA should be logged and kept on file by senior facility administrators.

Configure user accounts to automatically lockout after five failed login attempts within an hour. Failed login attempts are to be logged, and the system administrator automatically notified, where capable.

Dual (multifactor) authentication methods should be utilized for access to DCA where supported and practical.

3. Authorized User Access and Least Permissions

Create a facility Authorized User List for accessing facility DCA. Authorized users may be vetted similarly to the process for granting physical access to the facility. Authorized users may be grouped into categories (e.g. system administrators, facility operations and experimental staff, and experimental users) and given DCA user accounts with only the levels of access required to perform their job functions. This is consistent with the 'Least Permissions' approach to cyber security – personnel are granted access only to the functions they require to carry out their responsibilities under the organization.

Authorized User Categories:

- System administrators are either the senior reactor facility staff or senior research staff primarily responsible for the administration of the DCA associated with reactor safety and control and experimental systems. These personnel would have the highest level of DCA access consistent with their responsibilities. The DCA administrator would be responsible for creating a list of all access permissions available to the DCA, including both physical and logical access, and documenting the individuals, organizational roles, or job functions that are allowed elevated privileged access to the device.

NOTE: Shared accounts for administrative access may be used as long as the following criterion are met:

a. Shared account access is limited to those with a valid business need.
b. Access control lists for shared accounts are maintained.
c. Passwords for shared accounts are managed.
d. Access activity for a shared account is logged.

- Facility operations or experimental staff are responsible for routine oversight and operation of certain DCA and would have more restricted access levels consistent with their responsibilities.
- Experimental users would need to access specific experimental DCA only, and would have limited access permissions consistent with their utilization requirements.

For DCAs that can support utilizing multiple accounts (e.g. workstations), configure to:

a. Terminate temporary, guest, and emergency accounts within a maximum time period of inactivity at least every 90 days.
b. Create and protect audit records for account creation, deletion, and modification.
c. Document and notify system administrators of account creation, deletion, and modification activities.

Review DCA accounts consistent with the authorized user list at least annually. Disable inactive accounts within 90 days.

4. Documentation of Configuration Settings and Backups

Documentation and backups should be kept for all DCA configuration and settings files in either hardcopy or digital form as appropriate. The documentation should be updated annually at a minimum.

Full backups should be kept of all ICS software files, including configuration settings files, to assist with recovery in the event of a system crash or successful cyber-attack. The files should be backed up annually at a minimum.

5. Configuring and administration of firewalls and other network protective infrastructure

General recommendations for the utilization and configuration of firewalls, Intrusion Detection and Prevention Systems, data diodes, and network switches are given below.

The following guidance applies to credited **firewalls**:

a. Perform a stateful inspection.
b. Firewalls are configured for 'deny all' by default or end in a 'deny all' rule.
c. Rules prevent direct connection from lower to higher security layers.
   (1) No data, including handshaking signals may go directly from a lower security level to a higher level.
   (2) The higher layer must initiate the connection.
d. Rules are specific in nature allowing specific source and destination addresses or ranges, and specific protocols, where possible.
e. All DCA firewalls record and forward logs to a centralized logging server (if applicable):
   (1) Firewalls log 'Allowed' and 'Denied' connections.

(2) Firewalls record information flow for traffic monitoring, analysis, and intrusion detection.
(3) Firewalls log administrative access, rule set changes, and configuration changes.

f. Firewalls receive time synchronization from an internal source and are synchronized with the protected DCAs (as applicable).

The following guidance applies to **Data diodes**:

a. Data diodes are Physically Deterministic.
(1) Data diodes rely on physical limitations to ensure they are unidirectional.
(2) Data diodes do not rely on firmware or software to limit their data flow direction.

b. No connections with the potential to transmit data bypassing the data diode are allowed.

The following guidance applies to **Intrusion Detection and Prevention Systems** (IDS/IPS), including those embedded in firewalls:

a. IDS is deployed on each side of each boundary device (i.e. firewall, data diode) or as part of the boundary device.
b. For firewall boundaries where the firewall contains IDS, no additional IDS is required.
c. IDS/IPS records and forwards logs to a centralized logging server (as applicable).

The following guidance applies to **Switches**:

a. Where technically capable and not restricted by the equipment vendor, Media Access Control (MAC) address locking is implemented on the switch to restrict access to approved devices.
b. Where technically capable and supported by the equipment vendor, unused ports are disabled or grouped into an unused VLAN. When grouped into an unused VLAN, ports are monitored and alerted on connection changes.
c. Unused ports are blocked with locking devices (port blocks requiring keys or special tools to remove).

6. Physical Protection Requirements

All URR ICS DCA should have physical access restrictions in place. Access controls include locating inside the physically protected area of the URR facility (e.g. reactor bay or control room) and installation in locked enclosures. Following the facility DCA audit, any ICS DCA that are determined to perform or support functions that have a consequence index (CI) of 3 or 4 should be verified to be located inside the physically protected area of the facility. DCA with a consequence index of 2 or below should at a minimum be contained in locked laboratories or cabinets.

7. Air Gapping Infrastructure

Kiosks: Malware scanning stations or Kiosks should be made available for scanning authorized PMMD. Malware scanning stations or Kiosks must employ more than one Virus scanning engine, one of which includes heuristic scanning with Virus definitions updated at a frequency not to exceed 2 weeks. To mitigate attack vectors to DCAs introduced by the station, harden the PMMD and maintain per vendor recommendations. In order to maintain the Kiosk, only portable media designated for use on a DCA are to be scanned on these scanning stations.

Portable Media and Mobile Devices (PMMD): NIST defines PMMD as any portable cartridge/disk-based, removable storage media (e.g. floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives/devices that contain nonvolatile memory) and portable computing and communications devices with information storage capability (e.g. notebook/laptop computers, test equipment, tablets, personal digital assistants, cellular telephones, digital cameras, audio recording devices).

Such PMMDs are typically used to manage, configure, test, troubleshoot, or calibrate digital devices. Any PMMD digitally connected to any DCA must be compliant with all requirements below:

a. All PMMD shall be analyzed and hardened, employing a virus protection kiosk and/or whitelisting, prior to placing in the PMMD program and use on DCAs.
b. Authorized PMMD shall be identifiable by visibly Marking the devices using techniques, such as highly visible labels, or body of device, color coded devices, tags.
c. If configurable, then wireless capability shall be turned off or disabled on all PMMDs.
d. Turn off or disable webcam and microphones where their use is not required for maintenance, support, operation, or configuration.
e. USB PMMD devices are selected to minimize the threat of boot sector and firmware based threats such as 'BAD USB'.
f. Scan software updates provided by vendors prior to manually updating PMMD devices.

Passive media (CD-R, DVD-R, or CD/DVD ROM) should be used where possible and practical, however 1) size limitations of the media may make it impractical to use, and 2) many devices do not support passive media.
Prior to use of passive media, the media shall be scanned on the scanning kiosk before introduction into a DCA. Blank media cannot be scanned. If blank media is to be written to by a DCA, then scan the media after writing.

8. Vendor Access and Controls

The individual escorting the vendor is responsible for ensuring vendor activities using laptops or PMMDs are in compliance with scanning and air gapping procedures.

Vendors shall only be authorized to access the specific resources needed to achieve the business requirements of their connection.

Scan vendor PMMD or laptops using the scanning kiosk prior to and after use on plant digital equipment. Vendors shall use scanned and authorized PMMDs performing work on DAs and DCAs.

Vendor support device requirements:

a. Vendors shall access systems only from university-owned or vendor-owned computers.
   (1) No personal or 'home' computers are allowed access.
   (2) All activities performed from this connection are subject to monitoring and logging.
b. Active and current virus protection shall be present on the computer the vendor is using for access.
c. The computer shall utilize a current supported and actively updated operating system.
d. Do not allow connections to other networks, including the Internet and outbound VPN connections, while also connected to ICS networks.

9. Cyber Security Incident Response and Recovery

Incident Verification

The following are examples of suspicious cyber activities that could indicate the potential for a Cyber-attack. These situations require further investigation and should be reviewed by facility staff:

a) The discovery of individuals with uncommon interests or inquiries related to the facility's cyber security measures, personnel, or security controls.

b) The discovery of individuals eliciting or attempting to elicit information from security or other facility personnel regarding Digital Control Assets (DCAs), security measures, or vulnerabilities for Safety, Security or Emergency Preparedness (SSEP) functions.

c) The discovery of unsubstantiated cyber-attack threats that are considered to be related to harassment, including threats that could also represent tests of response capabilities or intelligence-gathering activities, or an attempt to disrupt facility operations.

d) The discovery of the degradation or failure of a DCA that is of suspicious or unknown origin.

e) The discovery of unauthorized personnel at or near the facility performing wireless reconnaissance of the licensee's wireless networks and communications systems.

f) The discovery of the theft or suspicious loss of authentication information necessary for accessing DCAs.

g) The discovery of the use of forged or stolen authentication devices used to support access control to DCAs or authorization activities.

h) The discovery of falsified identification badges, key cards, or other access-control devices that could allow unauthorized individuals access to DCAs.

i) The discovery of an active attack, virus, worm, logic bomb, etc., on a network containing DCAs that, if security controls were not in place, could adversely affect DCAs or SSEP functions.

j) The discovery of malware, unauthorized software, or firmware installed on a DCA.

k) Failures, degradations, or discovered vulnerabilities of DCAs or security controls that protect DCAs that would be likely to allow unauthorized or undetected access to those DCAS or that could result in compromising the DCA or an SSEP function.

l) The successful penetration or compromise of a DCA by unauthorized personnel.

m) The theft of sensitive cyber security data.

n) The loss of cyber intrusion detection capability in networks that contain DCAs.

Examples of potential tampering with plant equipment include:

a. Unlabeled or non-standard (wrong color) Universal Serial Bus (USB) devices.

b. Unauthorized mobile devices (e.g., cell phones) connected to plant equipment.

c. PMMD connected to plant equipment without Labeling to indicate it is authorized.

d. Unexpected cables or wiring hanging from electronic equipment.

e. Unexpected personnel connecting PMMD to plant equipment.

Incident Handling

Notifications – Notify senior facility staff that a cyber-security incident has been detected or has occurred. Notify a cyber-security expert at the institutional IT department, and obtain their technical support.

Incident Tracking – Create an entry in an Incident Log, detailing what is known about the incident and the timeline. During the incident response process, document system responses and observed changes in files to support analysis and understanding of the incident, and systematic elimination of the problem during the remediation phase.

Containment - The containment actions least disruptive to safety, security, and emergency preparedness functions are taken. Cyber security attack containment activities should include, but are not limited to:

a. Isolate the affected CDA using standard plant maintenance processes and approvals.
b. Assist in determining the CDA's operability or functionality.
c. Verify surrounding networks and support systems are not infected.
d. Ensure plant system operation and functionality.
e. Prevent or limit damage to and theft of company resources.
f. Evidence preservation.
g. Maintain service availability (e.g., network connectivity, data provided to other systems) if possible.

Incident Response Plan - The Incident Response Plan should detail items such as:

a. The likely evidence needed to analyze the situation.
b. The need to consult HR or Legal departments if disciplinary or legal action is to be taken, and any other external organizations that need to participate or be notified.
c. Level of analysis required.
d. Containment, eradication, and recovery strategies and steps identified and decisions made for proceeding.
e. Any special considerations.
f. Ensure all information is documented in the IR Log.
g. Obtain any work authorization required (Work Orders, Work Requests, Clearances) before making alterations to plant systems.

Collect Evidence - A detailed log should be kept for all Evidence including, but not limited to, the following:

a. Identifying information (e.g., the location, serial number, model number, hostname, equipment tag, media access control (MAC) address and original Internet Protocol (IP) address of device, if so equipped).
b. Name, title, and phone number of each person who collected or handled the Evidence.
c. Time and date of each occurrence of Evidence gathering, handling, or transfer.
d. Work Order or Work Request associated with all actions to resolve the incident.
e. If hard copies of device logs, configuration, or other files need to be collected as Evidence, then the documentation shall include a date and time stamp, and the name of the individual performing the collection.

Potential items to be collected include (but are not limited to):

a. Recovered file fragments and hidden and deleted files and directories from any location (e.g., identifying used space, free space, slack space).
b. File structures, headers, and other characteristics to determine what type of data each file contains rather than relying on file extensions.
c. Contents of any graphic files.
d. Graphically displayed directory structure.
e. Generated new checksums for core files and comparing to previous values.
f. Generated reports.

Incident Analysis - The facility technical staff, with assistance from institutional IT and other resources, shall perform a detailed analysis to determine:

a. The incident's scope (such as which networks, systems, or applications are affected).
b. Who or what initiated the incident and when it was identified.
c. How the incident has occurred (e.g., what tools or attack methods were used, what vulnerabilities were exploited).

Document results of the analysis in the Incident Log.

The incident response lead should determine the priorities and flow of the analysis, considering the following as needed:

a. Comparison of current behaviors to normal behaviors.
b. Content of the logging systems.
c. Correlation of incident data.
d. Variances of time between relevant clocks.
e. Content available from knowledge bases and industry OE.
f. System baselines.
g. Commonly used ports.
h. Links to malicious code and hoax information anti-virus vendor websites.
i. Links to lists of domains that have been blacklisted for spam and phishing attacks.

10. URR ICS Personnel Cyber Security Training

Generic Cyber Security Awareness Training

Personnel with access to any DCA (including outside the Protected Area) should have Generic Cyber Security Awareness training. Generic Cyber Security Awareness training is required for all staff and users badged for unescorted access.

Initial training and refresher training is accomplished annually with training topics as follows:

a. Site-specific objectives, management expectations, roles and responsibilities, procedures, guidelines and potential consequences for non-compliance.
b. General attack methodologies, including social engineering techniques, and appropriate and inappropriate cyber security practices.
c. Attack Indicators such as:
   (1) Unusual equipment in secure areas.
   (2) Unusual requests for information about or access to the system (Social Engineering attempts).
   (3) Workstation and server attacks including log files, lockouts, and bypassing a data diode.

(4) Unexpected system unavailability.
(5) Unusually heavy network traffic.
(6) Out of disk space or significantly reduced free disk space.
(7) Unusually high CPU usage.
(8) Creation of new user accounts.
(9) Attempted or actual use of administrator-level accounts.
(10) Locked-out accounts.
(11) Account in-use when the user is not at work.
(12) Cleared log files.
(13) Full log files with unusually large number of events.
(14) Antivirus or Intrusion Detection System (IDS) alerts.
(15) Disabled antivirus software and other security controls.
(16) Unexpected patch changes.
(17) Machines connecting to outside Internet Protocol (IP) addresses.
(18) Unexpected changes in configuration settings.
(19) Unusual activity from control devices.
(20) Loss of signal from control devices.

d. Organizational contacts for reporting of suspicious activity, incidents and violations of cyber security policies, procedures, and guidelines.
e. Why access and control methods are required.
f. Measures users can employ to reduce risks.
g. Organizational impact of the failure of the cyber security policy, procedures, and guidelines.

Technical Cyber Security Training

1. Technical training ensures suitable proficiency is achieved and maintained by the following individuals:
    a. Those with cyber security responsibilities
    b. Those with design, modification, or maintenance control of DCAs
    c. System Manager and Owners
2. Technical training is required:
    a. Prior to authorizing access to DCAs.
    b. As required by procedure changes and plant modifications.
    c. Every 12 months to mitigate risk and ensure proficiency.
3. Training topics include the following:
    a. Applicable cyber security concepts and practices to job responsibilities.
    b. Knowledge of specific cyber security and engineering practices, procedures, and technologies which may be encountered.
    c. General information on cyber security vulnerabilities, potential consequences, and cyber security risk reduction methods.

Useful Training References & Resources:

- *TRTR-NRC "Cyber Security; Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities", Section 8 "Personnel cyber security training issues"*
- *Avoiding Social Engineering and Phishing Attacks - https://www.us-cert.gov/ncas/tips/ST04-014*
- *Securing Your Web Browser - https://www.us-cert.gov/publications/securing-your-web-browser*

11. Requirements for Safeguarded Information (SGI)

Digital SGI should be encrypted, stored on PMMD that has been scanned, is air gapped, and is physically secured per facility requirements.

Per NRC U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD) "MD12.5 – NRC Cyber Security Program", digital encryption used for SGI should use FIPS 140-2 validated cryptographic modules operated in FIPS mode. Cryptographic modules used for SGI should be FIPS 140-2 validated to at least an overall level 2 with the validation subcategories of Roles, Services, and Authentication; electromagnetic interference/electromagnetic compatibility; and Design Assurance validated to at least level 3.

12. Audits

Initial: An initial URR ICS DCA audit and risk assessment should be performed as detailed in the "Cyber-Security Risk Assessment Methodology for University Research Reactors" procedure.
Periodic: Perform an updated audit of DCAs every 12 months per the assessment procedure, or minimally upon major changes in ICS or DCA configurations or functionality.

Appendix 2 - NE235 Cyber Security Course Module

Lecture Topic - "Cyber Security of Nuclear Plant Industrial Control Systems" (1.5 contact hours)

Lecture Contents:

1. Aurora Test – A case study in what can happen.
2. ICS / SCADA Network Architecture:
   a. Network Segmentation & Firewalls
   b. Control System LAN
   c. ICS Field Devices and PLCs
3. Common ICS Attack Vectors:
   a. Attack Delivery Methods
   b. Cyber "Kill Chain"
4. Cyber Security Defense in Depth:
   a. Cyber Security Culture, Hygiene & Procedures
   b. Network Zones and Hardening – Firewalls, Data Diodes, IDS/IPS, VPN, Air Gapping
   c. Software Solutions – OS Updates, Antivirus, Whitelisting
5. SSEP Functions & CDA Audit:
   a. SSEP Plant Systems and Components
   b. Critical Digital Assets (CDA) –vs- Digital Assets (DA)
   c. CDA Audit Methodology – CDA Configuration, Network Mapping, Physical Protection
6. Threat, Vulnerability & Risk Assessment:
   a. Threat Metrics – Attacker Intent, Capability & Opportunity
   b. Vulnerability Metrics – Network Protection, Common Vulnerability Exposures (CVE), Interdependencies
   c. Consequence Metric – Low, Medium, High, and Critical Impacts
7. PULSTAR Facility ICS Risk Assessment - Case Review
8. History of Cyber Attacks at NPP's and Industry Vulnerability Trends:
   a. Cyber Attacks - Davis Besse, Hatch Plant, Stuxnet, KHNP, Virus at NPP, Nuclear 17
   b. Continuously Evolving Cyber Threat Landscape

Lab Module – "Cyber Security & OPSEC for ICS" (2.5 contact hours)

Lab Contents

1. Introduction to ICS CERT Website Resources:
   a. Virtual Learning Portal - Web Based ICS Training Modules
      i. Access & Review Module 100W – "Operations Security (OPSEC) for Control Systems"
      ii. Multifactor Authentication Methods
   b. Alerts and Advisories Databases for ICS Hardware and Software
2. NIST National Vulnerability Database:
   a. Review of OS, Application Software & Firmware
   b. CVE and CVSS Base Scores

Methodology Development for Cybersecurity Vulnerability Assessment of University Research Reactors

S. A. Lassell[1], A. I. Hawari[1], J. S. Benjamin[2], K. T. Barnes[2], V. L. Wright[2]

[1]Nuclear Reactor Program, Nuclear Engineering, North Carolina State University, Raleigh, NC, USA
[2]National and Homeland Security Division, Idaho National Lab, Idaho Falls, ID, USA
ayman.hawari@ncsu.edu

INTRODUCTION

A methodology for assessing the cybersecurity robustness and vulnerability of university research reactors has been developed using the PULSTAR reactor as a test case. The PULSTAR is the latest of four research reactors built at North Carolina State University by the nation's first academic nuclear engineering program established in 1950. The 1-MW PULSTAR (see Figure 1), which went critical in 1972, represents an active research reactor facility with a history rooted in education, scientific research and national outreach.

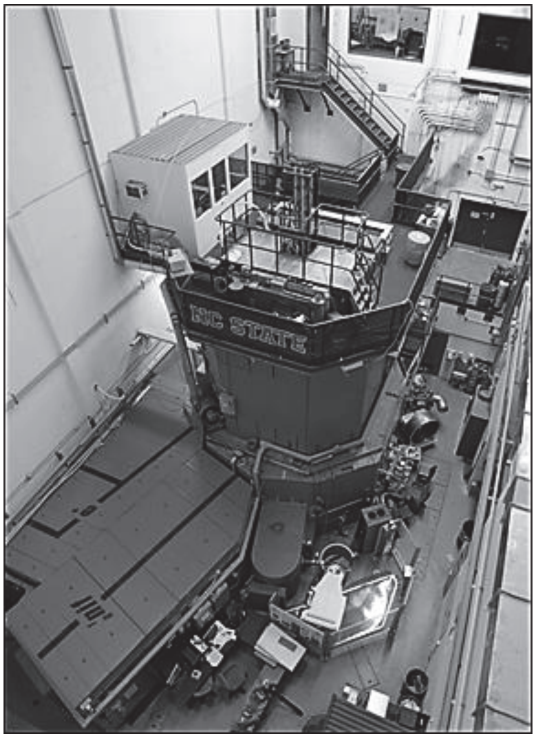


Fig. 1. PULSTAR Reactor and bay area showing various facilities.

Over the past 15 years, the PULSTAR has undergone significant developments in its operational, educational, and scientific infrastructure that have resulted in quadrupling its utilization by national and international users. Among the installed systems are state-of-the-art and internet-based educational capabilities, modern safety and security systems, and unique experimental capabilities supporting irradiation testing and pre- and post-irradiation examination. Current experimental facilities include a Neutron Powder Diffractometer, an Intense Positron Beam facility with associated Positron Annihilation Lifetime Spectrometers (PALS), a Neutron Imaging facility, and an Ultracold Neutron Source [1].

The developed cybersecurity assessment methodology provides guidance for identifying and auditing critical digital assets (CDA) comprising facility Safety, Security and Emergency Preparedness (SSEP) related systems, as well as experimental apparatus and other research and educational infrastructure typical of a university reactor. Metrics are provided for identifying, assessing and quantifying potential cybersecurity threats and vulnerabilities, and the consequences associated with a successful cyber-attack. The threat, vulnerability and consequence metrics may be utilized to calculate the relative risk of cyber-attack on each system, providing a ranking useful in identifying higher risk systems and establishing priorities for mitigation. While the developed methodology has been tested and applied using the PULSTAR reactor facility, it has been formulated as a general blueprint to be used for the cyber-assessment of university research reactors nationally and internationally.

METHODOLOGY DEVELOPMENT

To support the cybersecurity methodology development, an assessment team was formed that is comprised of reactor staff and operators (including student operators) and cyber security professionals from Idaho National Laboratory (INL). The university team received cyber-security training including Department of Homeland Security (DHS) Industrial Control System (ICS) Cyber Emergency Response Training (CERT) Web Based training modules [2]. The training also included the ICS Cybersecurity Workshop with a Red Team/Blue Team exercise hosted on site at INL.

In addition, key cyber-security related documents were reviewed by the team and utilized in developing the assessment methodology [3,4,5,6].

The methodology developed by the team is comprised of the following basic elements:

a. *Baseline Evaluation and Audit of University Reactor Facility SSEP Functions and CDA*. A facility cyber-security baseline evaluation is performed through i) identifying SSEP related reactor systems, ii) creating an inventory of CDA comprising each of these systems (see Figure 2 below, for CDA identification flowchart), iii) performing a comprehensive cyber audit of the identified CDA, including generating network diagrams, identifying known vulnerabilities and exploits associated with ICS operating system and application software, and evaluating interdependencies on externally supported SSEP related infrastructure, and iv) evaluating existing institutional cyber-security infrastructure, culture, policies, procedures and training to determine whether they are adequate to protecting the research reactor facility CDA.

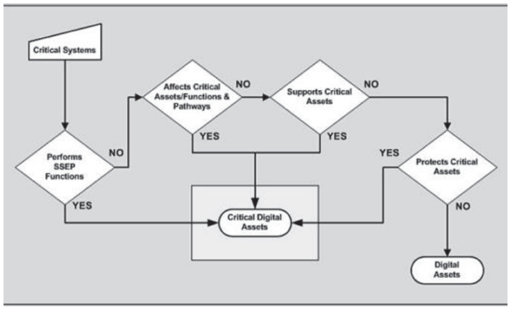


Fig.2. Flow Chart for Identifying Critical Digital Assets.

b. *Risk Assessment of CDA***.** Utilizing the data generated from the baseline audit and the guidance provided, an evaluation is performed of the given threat metrics (attacker capability index (ACI), attacker intent index (AII), and attacker opportunity index (AOI)), vulnerability metrics (network protection index (NPI), vulnerability scoring index (VSI), and interdependency vulnerability index (IVI)), and consequence metrics (consequence index (CI)) for each CDA. Values are assigned for each metric and the relative risk index (RI) for cyber-attack is calculated using

$$RI = \frac{[(ACI+AII+AOI)\times(NPI+VSI+IVI)\times(CI)]}{C}, \qquad (1)$$

where C is a normalization constant. A RI value of 100% represents the highest relative risk of cyber-attack.

c. *Rank Risk and Prioritize Mitigation***.** Prioritize the mitigation of vulnerabilities found in the hardware, software, and/or network components of the CDA systems by ranking relative risk levels as calculated in part (b) above.

d. *Physical Security System Assessment***.** Using the guidance and assessment metrics provided, work with the campus entity responsible for administering physical security functions to identify and mitigate potential procedural, hardware and software related cyber vulnerabilities in the physical security system infrastructure.

METHODOLOGY IMPLEMENTATION

Steps (a), (b), and (c) of the methodology detailed above were implemented and a risk assessment of the research reactor facility systems was completed. Seventy nine separate CDA comprising the SSEP related systems and experimental infrastructure were identified and audited. A search of the NIST National Vulnerability Database and ICS-CERT databases yielded more than 17,000 CVE related to the CDA operating system and application software in use. Threat, vulnerability, and consequence metrics were evaluated for each CDA and utilized to calculate relative cyber risk indices. It was found that all reactor control system CDA were at a relatively lower risk of cyber-attack with RI values of $\leq 25\%$. Certain networked experimental systems had higher RI values of up to 30%.

For the physical security system, an assessment was performed per step (d) of the methodology described above. The scope of the security system assessment included evaluating the hardware, software, network infrastructure, and implementation procedures. The project team provided the Security Applications and Technologies (SAT) division at NCSU with a list of questions concerning the configuration and administration of the physical security system which were reviewed and discussed. The team members performed a walk down of the reactor security system equipment and were given hands on access to test security equipment and access control. Following the review, recommendations were made for enhancing the physical security system.

To address any cyber-vulnerabilities identified during the facility risk assessment, a defense-in depth-approach is currently being developed and implemented. The corresponding mitigation strategy includes implementation of effective cyber security policies and procedures covering the reactor ICS, training the reactor facility operations and research staff in aspects of cyber hygiene, integrating networked reactor ICS under the university supported network security infrastructure, and working with facility ICS hardware and software vendors to identify software updates and patches that will mitigate CVEs without compromising operation of the ICS networks.

CONCLUSION

A cybersecurity assessment methodology has been developed at the PULSTAR reactor. The developed methodology guides university research reactor operators through a comprehensive and straightforward process to identify cyber vulnerabilities at their facilities. Assessment results allow understanding cyber risk exposure, and how best to allocate resources towards mitigating those risks. The outcomes from the risk assessment completed at the PULSTAR reactor facility have been utilized to prioritize mitigation steps. A mitigation strategy is currently being developed and implemented. The lessons learned have been utilized to develop cyber informed engineering content which is being incorporated into the nuclear engineering and reactor operator training curriculum at North Carolina State University.

ACKNOWLEDGMENT

This work is supported by the US Department of Energy Nuclear Energy University Program (NEUP).

REFERENCES

1. A. I. Hawari, “Multidisciplinary Engagement at Research Reactors: The NCSU PULSTAR,” IGORR 2017, Sydney, Australia (2017).

2. Available at website https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

3. NRC-TRTR Working Group, “Effective Practices for the Establishment and Maintenance of Adequate Cyber Security at Non-Power (Research and Test) Reactor Facilities”; ML15253A060 (2016).

4. NRC Regulatory Guide 5.71 – Cyber Security Programs for Nuclear Facilities; ML090340159 (2010).

5. NST037 TECDOC - Conducting Computer Security Assessments; IAEA-TDL-006 (2016).

6. IAEA Pub1527 – Computer Security at Nuclear Facilities, ISSN 1816–9317, no. 17 (2011).

Appendix 4

TRTR 2018 Meeting

CYBERSECURITY VULNERABILITY ASSESSMENT AND DEFENSE-IN-DEPTH STRATEGY FOR UNIVERSITY RESEARCH REACTORS

S. A. Lassell, A. I. Hawari
Nuclear Reactor Program, Dept. of Nuclear Engineering, North Carolina State University, Raleigh, NC, USA

J. S. Benjamin, K. T. Barnes, V. L. Wright
National and Homeland Security Division, Idaho National Lab, Idaho Falls, ID, USA

ABSTRACT

A methodology for identifying, assessing and mitigating the cybersecurity vulnerabilities of university research reactor (URR) industrial control systems (ICS) has been developed using the PULSTAR reactor as a test case. The PULSTAR is the latest of four research reactors built at North Carolina State University by the nation's first academic nuclear engineering program established in 1950. The 1-MW PULSTAR, which went critical in 1972, represents an active research reactor facility with a history rooted in education, scientific research and national outreach. The assessment methodology developed provides guidance for identifying and auditing critical digital assets (CDA) comprising facility Safety, Security and Emergency Preparedness (SSEP) related systems, as well as experimental apparatus and other research and educational infrastructure typical of a URR. Metrics are provided for identifying, assessing and quantifying potential cybersecurity threats and vulnerabilities for each CDA, and the consequences associated with a successful cyber-attack. These threat, vulnerability and consequence metrics may then be utilized to determine the relative risk of cyber-attack for each system, providing a ranking useful in identifying higher risk systems and establishing priorities for mitigation. A parallel assessment process for URR physical security systems (PSS) has also been developed, leveraging partnerships with campus security and IT personnel to evaluate system robustness to cyberattack. Following the implementation of the developed assessment methodology at the PULSTAR, defense-in-depth mitigation strategies were developed for application at URRs, taking into account the resources typical of university facilities. Strategies for mitigation include: 1) resolution of key common vulnerability exposures (CVE) identified for each CDA; 2) implementation of effective network security and air gapping hardware and protocols; 3) incorporating URR specific cyber security policies, procedures and training; and 4) engaging with the campus physical security system administrator to address vulnerabilities identified in the PSS. Experience with implementing the developed assessment and mitigation strategies at the PULSTAR reactor facility and an assessment of the resulting improvements in cyber security robustness will be presented.