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.

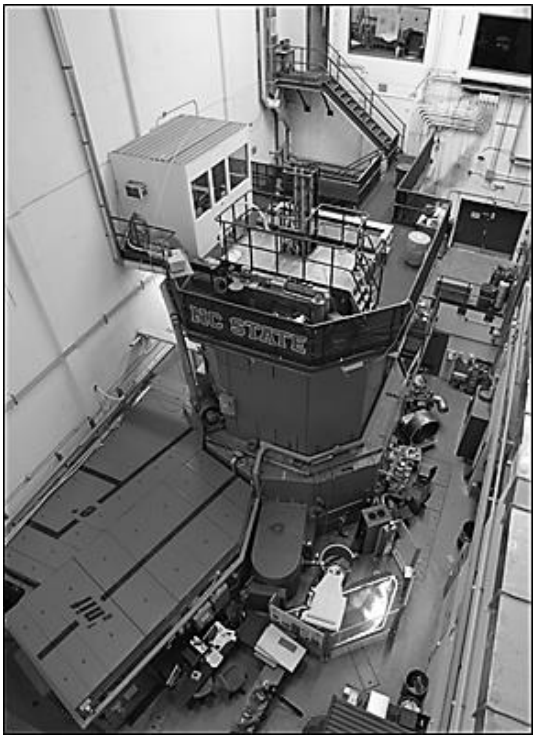

Fig. 1. PULSTAR Reactor and bay area showing various facilities.

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.

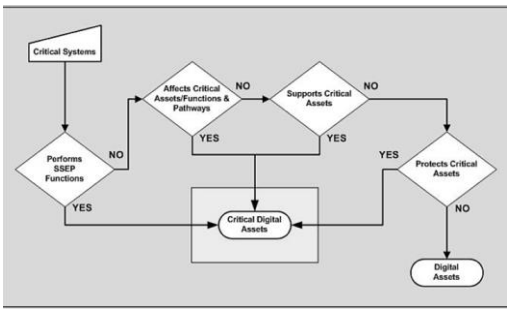

Fig.2. Flow Chart for Identifying Critical Digital Assets.

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).