Risk Informed Cyber Security for Nuclear Power Plants

Phillip L. Turner, Timothy A. Wheeler, Matt Gibson

Sandia National Laboratories | Electric Power Research Institute
Albuquerque, NM USA | Charlotte, NC USA
pturner@sandia.gov, tawheel@sandia.gov, mgibson@epri.com

ABSTRACT

Nuclear power plants are increasingly adding digital components for plant operation, safety, and security. These digital components fill a gap with legacy equipment where replacement components no longer exist. They also benefit operation of the plant by increasing efficiency in power generation, monitoring of equipment and plant parameters, as well as aiding operator control. However, the addition of digital components and systems also adds cyber risks with previously unanalyzed failure modes and attack vectors are introduced with these new systems. These risks are difficult to identify, analyze, and mitigate due to the increasingly complex nature of the digital components and the integration of these components with additional plant processes and communication networks. The research presented in this paper develops a new method that addresses the cyber risk to inform appropriate levels of protection.

EPRI and Sandia are working under a Cooperative Research and Development Agreement to develop an effective method of evaluating the cyber risk in production nuclear power facilities. The Cyber Hazards Analysis Risk Methodology (CHARM) focuses on ensuring adequate controls are in place for appropriate cyber protection of the plant from radiological release or generation risk. Existing plant hazards analyses (e.g., PRA, FTA) do not account for software deficiencies or adversarial intent. This method leverages existing plant analyses and MIT's Systems Theoretic Process Analysis (STPA) to create cyber informed fault trees. These new fault trees will provide the basis for comprehensive cyber risk analysis and help ensure potential gaps in cyber security controls are identified and corrected.

Key Words: cyber security, cybersecurity, industrial control systems, hazards analysis, nuclear power plants.

1 INTRODUCTION

Digital control systems are becoming more and more prevalent in nuclear power generating plants. In older plants, these digital systems fill a gap with legacy equipment where replacement components no longer exist. Newer plants being built today are coming with fully digital systems to control the reactor and power generation. The digital systems benefit operation of the plant by increasing efficiency in power generation, monitoring of equipment and plant parameters, as well as aiding operator control. However, the addition of digital components and systems brings cyber risks with previously unanalyzed failure modes. New attack vectors are introduced with these new systems as a result of the new *interconnected processes* [1] that are being introduced to the plants. These risks are difficult to identify, analyze, and mitigate due to the increasingly complex nature of the digital components and the integration of these components with additional plant processes and communication networks. The research presented in this paper develops a new method to understand the cyber risks and inform appropriate levels of protection.

> An *interconnected process* is any process that allows data, software, or hardware to move into, out of, or change the system of concern. In this context, the most obvious example of an interconnected process is a system or systems that are attached to the internet or on a local area network serving as the communications path for those systems. An isolated ICS network would be its own process with connections to those systems residing within that collision domain…

> [Other processes could be] a vendor laptop that is occasionally connected to a component for maintenance, a firmware update that was obtained from the manufacturer and is applied to a controller, or a person making configuration changes manually at the component through an interface. The main difference in these processes is the latency involved in the connections because the processes don't always have a digital connection to various components within the process as a computer network would. [1]

The Electric Power Research Institute (EPRI) and Sandia National Laboratories are working under a Cooperative Research and Development Agreement (CRADA) to develop an effective method of evaluating the cyber risk in production nuclear power facilities. The Cyber Hazards Analysis Risk Methodology (CHARM) being developed focuses on ensuring adequate controls are in place for appropriate cyber protection of the plant from radiological release or generation risk. Existing plant hazards analyses (e.g., PRA, FTA) do not account for software deficiencies or adversarial intent.

2 RESEARCH PHASES

This research has been ongoing for several years and has been performed in phases. Phases one and two evaluated various hazard analysis methods for efficacy and developed an initial methodology for risk analysis in nuclear power plants. This research effort is currently in the third phase to evaluate and refine the method. Pilot runs of the method are being performed on existing plants to ensure appropriate sensitivity and alignment of vulnerability identification and mitigation.

2.1 Phase 1

Phase 1 of the research started with evaluation of different hazards analysis methods for their efficacy in identifying and prioritizing cyber risks [2, 3]. It was determined that MIT's Systems Theoretic Process Analysis (STPA) and Fault Tree Analysis (FTA) methods were the most suitable for identifying risks within the plant. Combining these two methods allows for the creation of cyber informed fault trees that provide the basis for comprehensive cyber risk analysis within CHARM.

2.2 Phase 2

Phase 2 focused on developing the framework for an integrated method. The method takes the insights from STPA and FTA to provide attacker goals in the attack graph. The attack graph combines those with a means of identifying vulnerabilities within the plant's digital architecture and processes. The cyber security controls are included to prioritize their importance based upon the identified architecture vulnerabilities and risks [4].

The Cyber Informed Fault Trees (CIFT) show where top level events can be achieved by digital components. Whereas traditional Probabilistic Reliability Analyses (PRA) focuses on the probability of a component failure, random failures aren't considered in this analysis. Therefore, if a nondigital component is part of the resulting cut-set for that chain, that cut-set is removed from the CIFT. The CIFT cut-sets will become the goal-sets for the attack graphs.

To help identify vulnerabilities, the team leveraged previous work with Sandia's Information Design Assurance Red Team (IDART) methodology [5] and Sandia's Cyber Informed Risk Analysis (CIRA) method. This is a Subject Matter Expert (SME) based method where a system is analyzed and weaknesses or vulnerabilities identified that could allow an adversary to accomplish attack goals. Elements of this method have been used extensively in vulnerability assessments of highly critical and complex systems with a high level of success in identifying architectural level vulnerabilities. This leads to the ability to mitigate system weaknesses and increase the difficulty for an attacker to successfully accomplish their goals. CIRA takes the resulting attack graph and prioritizes nodes and paths.

Cyber security controls are identified and given an importance to each of the nodes and attack vectors for the system. This provides a means for prioritizing the cyber security controls based on their relative importance within the system analysis. The system can then be evaluated to determine where gaps in protection of the system might exist. Prioritizing the controls helps focus cyber security resources where they are needed most within the plant.

In combining aspects of these methods, the team developed the steps outlined below to evaluate the system for cyber risks, prioritize cyber security controls, and identify potential gaps in the cyber security controls:

1. Gather plant data.
2. Identify the digital instrumentation and control (I&C) relationships to the plant system.
3. Perform STPA on the plant system.
4. Modify and solve existing fault trees to include new cyber-induced faults.
5. Develop cyber attack graphs.
6. Rank cyber risks.
7. Identify cyber security controls relevant to ranked components and attack graphs.
8. Identify gaps in cyber security controls for risks.

2.3 Phase 3

Phase 3 of the research is intended to refine and validate the methodology and is the current phase. A new method was also introduced during this phase, EPRI's Technical Assessment Methodology (TAM) [6] that defines assessments of digital components and the creation of Cyber Security Data Sheets (CSDS). Elements of the TAM are being incorporated into CHARM, resulting in a significant shift in the method in terms of how the attack graph is created and analyzed. Incorporation of the CSDS allows for a means of automating creation of process topologies, e.g., network topologies, when the interfacing connections are identified within the plant architecture for the components. These topologies also allow for automating attack graph creation by defining these interfaces as potential attack vectors for the system. Any component and process vulnerabilities or cyber security controls identified from the TAM can also be brought into the attack graph. Automating this process removes the need for SME input in the creation of the graph and allows for repeatable results.

This research has identified the need to also include other processes and their elements and interfaces that exist outside of the communications networks. For example, take the process to update firmware on a digital component. This process might start with downloading the firmware from the vendor through the web, moving it from the engineering network to a USB drive and then to a maintenance laptop. The laptop would then be connected to the device and update the firmware. The elements used within this process, manufacturer website, Engineering workstation, USB drive, and maintenance laptop are now additional elements that are important in determining access vectors into the plant system. Evaluation of this process identifies these additional digital elements that should be included in the assessment of the system. Perhaps they don't require the same level of rigor used in evaluating the plant digital components, but at a minimum, their interfaces and other processes they are used in should be identified. These other *interconnected processes* then become important to the overall analysis by identifying potential attack paths into the system and the resulting cyber security controls. With this added information, a comprehensive attack graph can be developed, and it is expected that it will grow quite large. The team will evaluate means of appropriately analyzing the graph as it expands.

At the time of writing, the team is working on a means of analyzing the attack graph by scoring metrics for each node and edge and the importance of each goal. These metrics determine the difficulty of exploiting a node and how the cyber security controls affect that. Each path within the graph will also be scored based upon scores of nodes and edges along the path. This will allow for prioritizing the paths, identifying high-importance nodes, and evaluating the effects of cyber-security controls on the system. The goal is to ensure adequate protections exist and there are no gaps in coverage for a potential exploitation path.

Pilot runs of the method are being performed on existing plants to ensure appropriate sensitivity and alignment of vulnerability identification and mitigation. Four plants are currently slated to pilot the method. One is a new fully digital plant in licensing and another is an existing plant currently in operation. Two others are in discussions and are solidifying their participation, another currently operating plant and a new plant under construction. Having the ability to focus on different types of plants with varying degrees of digital implementation will be very helpful in understanding limitations on the method and where improvements to the method can be made.

2.4 Phase 4

At the completion of the current phase, EPRI will begin work to develop a tool that incorporates the CHARM method. This will incorporate inputs for FTA, STPA, TAM, and CHARM. Some degree of input in the process will be needed, e.g., STPA and FTA development of CIFT. The goal is to automate as many elements of the method as possible to ensure a repeatable process exists and reduce the reliance on SME input for a comprehensive analysis. This will allow for less subjectivity in the process and should enable the resulting evaluations to be credible and standup to scrutiny.

3 CONCLUSION

When this research is completed, the nuclear power industry will have a risk-based methodology that can leverage existing work in hazards analyses to understand how cyber attacks could affect the plants. This will provide a basis for analysis of plant risks from potential cyber attacks and prioritization of cyber security controls put in place to mitigate these risks. Key industry benefits of this research are reducing cyber vulnerability mitigation costs, limiting cyber mitigation to a sustainable but effective scope, providing consistent cyber risk determinations, aligning resources with actual risk, and generally improving digital risk insights and plant protection. Ultimately, this method will provide the nuclear power industry with a validated risk-based analytic approach for ensuring appropriate levels of cyber protection for the safe operation of nuclear power plants.

4 ACKNOWLEDGMENTS

Funding for this research has been provided by EPRI and the Department of Energy Office of Nuclear Energy.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2017-3970 C.

5 REFERENCES

1. Turner, P. L., Adams, S. S., Hendrickson, S. M. Enhancing Power Plant Safety through Simulated Cyber Events. Submitted to the American Nuclear Society's 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies. (2017).
2. Turner, P. L., Wheeler, T. A., Dawson, L. A., Muna, A. Assessment of Hazard Analysis Methods for Nuclear Power Cyber Security. American Nuclear Society's 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, Volume 3. (2015).
3. Analysis of Hazard Models for Cybersecurity: Phase I. 3002004995. EPRI, Palo Alto, CA. (2015).
4. Program on Technology Innovation: Cyber Hazards Analysis Risk Methodology, Phase II: A Risk Informed Approach. 3002004997. EPRI, Palo Alto, CA. (2015).

5. Duggan, D. P., Thomas, S. R., Veitch, C. K., Woodward, L. Categorizing Threat: Building and Using a Generic Threat Matrix. Sandia Report: SAND2007-5791. http://www.idart.sandia.gov. Sandia National Laboratories. (2007).
6. Cyber Security Technical Assessment Methodology: Vulnerability Identification and Mitigation: Vulnerability Identification and Mitigation. 3002008023. EPRI, Palo Alto, CA. (2016).