Enhancing Power Plant Safety Through Simulated Cyber Events

Phillip L. Turner[1], Susan S. Adams[1], Stacey M. Hendrickson[1]

[1]Sandia National Laboratories
Albuquerque, NM USA
{pturner, smsteve, smhendr}@sandia.gov

ABSTRACT

There are gaps in understanding how a cyber-attack would manifest itself within power plants and what these events would look like within the control room from an operator's perspective. This is especially true for nuclear power plants where safety has much broader consequences than nonnuclear plants. The operating and emergency procedures that operators currently use are likely inadequate for targeted cyber-attacks. This research focuses on understanding how a cyber event would affect the operation of the plant, how an operator would perceive the event, and if the operator's actions would keep the plant in a safe condition.

This research is part of Sandia's Laboratory Directed Research and Development program where a nuclear power plant cyber model of the control system digital architecture is coupled with a generic pressurized water reactor plant training simulator. Cyber event scenarios will be performed on the coupled system with plant operators. The scenarios simulate plant conditions that may exist during a cyber-attack, component failure, or insider sabotage, and provide an understanding of the displayed information and the actual plant conditions. These scenarios will determine if plant operators can 1) recognize that they are under cyber-attack and 2) take appropriate actions to keep the plant safe. This will also provide the opportunity to assess the operator cognitive workload during such events and identify where improvements might be made. Experiments with nuclear power plant operators will be carried out over FY 2018 and results of the research are expected by the end of FY 2018.

Key Words: cyber security, industrial control systems, human factors, decision making, nuclear power plants.

1 INTRODUCTION

Industrial control systems (ICS) generally lack the security controls necessary to protect them from cyber events. In the early implementation, digital control systems were put in place solely to provide a function, to control a process through an automated means instead of using an analog process. As such, these early systems were designed with no security measures in place that would protect them from modern day cyber threats. If security is needed, it must be layered around the system. The vast majority of cyber-attacks focused on enterprise systems, PCs, and network devices. Over time the world started seeing the effects of malware that would get into control systems. At first it would cause unpredictable behaviors because the programmable logic controllers (PLCs) and such didn't know how to predict the unusual format that it would natively use. Something as benign as a ping would cause the equipment to go haywire [1]. Then the world started seeing attacks targeting those systems and taking control of them [2]. Depending on the process being controlled, the effect could be disastrous or, at the least, very costly.

The need for securing these systems is continually increasing as cyber actors become more advanced in their capabilities. Since adequate security is not built in today, it must be placed around the devices, communications networks, and interconnected processes for these systems. Adding layers of security can have a good impact in terms of increasing the difficulty of attacks against the system (raising the bar); however, there still may be weaknesses that don't defend some access vectors well enough to keep adversaries completely out. Even if the systems are air-gapped, there are still interconnected processes that provide opportunities that adversaries could leverage.

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. The main reason for calling these *interconnected processes* instead of *interconnected networks* is to show the similarity to processes that are usually not associated as being interconnected, such as 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.

In the example of updating firmware, an *interconnected process* starts at the manufacturer's software development network, carries through delivery to the plant, and continues until it is installed on a device that is operating within the plant. These processes are important to the discussion because they bring attack vectors with them that provide adversaries means of getting into the systems. The notion of an 'air-gapped' system provides a false sense of security by ignoring the connections within these processes. An 'air-gap' may add a degree of difficulty to overcome, but an interconnected process puts the system in place with the software it is running. Any process could also have the potential of being short circuited by an insider, maliciously or otherwise.

Nuclear power plants (NPPs) are steadily increasing the number of digital systems that are used to control the reactors and balance of plant systems. While some of these systems may have some cyber security controls built in (e.g., password protection), it is generally minimal protection and ICS protection mainly relies upon boundary protection mechanisms to secure these systems (analogous to layered physical security). If malware were to get into the communications network that the systems reside upon, it could cause unknown effects within the plant systems. These effects could range from none to potential failure of components depending upon whether the malware was designed to attack control systems and if it was targeted to that specific system. With the large number of interconnected processes surrounding these systems and components, many paths exist by which an attacker could gain access to the systems.

In discussions with industry, industry researchers, and regulators, there is currently a large lack in understanding of what would happen if the plant might be under some form of attack (cyber or sabotage) or what might occur from a random component failure. The procedures operators currently use are likely inadequate for random failures and they may not adequately address targeted cyber-attacks. This work will help identify opportunities to improve the cyber resilience of the plants through procedure updates, better training, and incorporation of effective cybersecurity controls. The research goals for this project are to understand what the effects of cyber-attacks would be within the plant, as observed within the plant simulator, and what the operator perceives and how he or she responds while the attack is occurring. While random component failures are a lower priority for this effort, the research should provide preliminary insights into this aspect of the problem as well.

2 CYBER MODELING AND SIMULATION

To model the NPP digital control system communications network, a tool developed at Sandia National Laboratories called SCEPTRE is used. A representation of the digital components will be built within SCEPTRE that will be coupled to the NPP simulator. The communications networks for those components will be developed in Sandia's Emulytics™ environment to bring the network connectivity aspect into the model. This will allow for representing various networking elements and data flows within the cyber model. The underlying plant architecture for the emulated environment will be derived from plant drawings and subject matter experts (SME's). The plant simulator will be coupled to the digital components directly to allow for control through the cyber model directly into the simulator. Attack and failure scenarios will be developed and run to capture plant effects and to test and validate the coupled system.

NPP simulators are used for training and certification of operators. The simulator is that of a generic pressurized water reactor (GPWR). The fidelity contained within the simulator is adequate to mimic plant functions and responses. The operator sees the same indications that he or she would see within the Main Control Room in the exact same layout of their control console. However, the underlying communications network architecture that exists within the plant does not exist within the simulator. A simulation is generally designed to the level of fidelity needed to answer the questions that it is being used for. In this case, the simulation will provide proper indication and feedback to the operator of the physical parameters that should be occurring within the plant. By connecting the cyber model to the GPWR simulator a layer of fidelity can be added that provides the ability to begin answering a different set of questions that pertain specifically to the digital elements within the control system and the interconnected processes that those systems use.

A parallel effort is underway to develop a SCEPTRE model that can be coupled to MELCOR, a computer code that models the progression of severe accidents in NPPs [3]. In this project, The Residual Heat Removal (RHR) system, Figure 1, is evaluated while under a simulated cyber-attack. If an adversary were able to open the motor operated valves (MOVs) separating the RHR system from the high pressure within the reactor coolant system while at power, what would the effect on the RHR system and the NPP be? In this scenario, we work to understand mechanisms for how an exploit could go through notional plant network architecture and impact the plant. We gain insights into how the RHR system might physically fail from the higher pressures and how the resulting Interfacing System-Loss of Coolant Accident (IS-LOCA) will affect the plant. Fidelity will be added to the system modeled in the MELCOR project to include more components within the system for the NPP simulator model. This will allow the full array of operator instruments and control mechanisms to be included in the simulation.

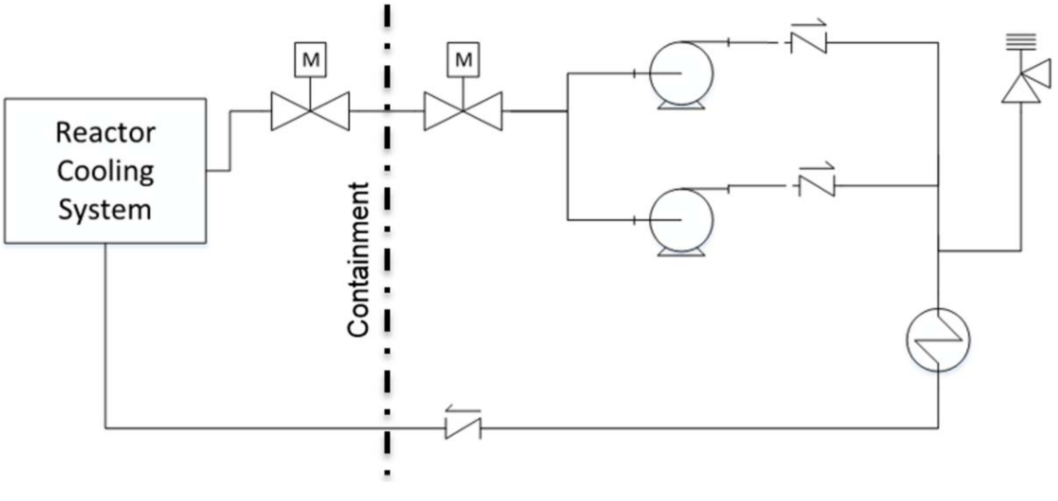

Fig. 1. Simplified Diagram of the Residual Heat Removal System

With the understanding of plant effects gained from the SCEPTRE/MELCOR research, the team will have a better understanding of what should be happening within the plant. This will allow for increased fidelity in the NPP simulation and a deeper understanding of what an operator should be seeing and how the cyber event might present plant parameters to an operator to try to obfuscate the true conditions within the plant. It will also allow for modeling different paths within the scenario, depending on what actions the operator takes.

The scenarios will vary in complexity and range from nontargeted, nuisance malware getting into the system to a full-scale attack targeting as many systems as possible. This will provide a broad representation of what an operator might expect to see during a cyber event and should provide the team with good insights into operator response for each type of event. Because of the broad array of the types of events that will be modeled, it may also be possible to get some early insights into the limitations of cyber-attack effects on the plant. This may help with understanding how varying degrees of implementation digital instrumentation and control within the plant would impact the success of a cyber-attack. This will likely be a topic for future research.

To understand how the operator will respond within this environment, several tasks will be undertaken to assess how the operator reacts. The following section describes the methodology used to assess the operator's understanding.

3 HUMAN FACTORS METHODOLOGY

To better understand the impact of cyber-attacks on control room operations, NPP SME's were consulted and interviewed. The methodology used by Stevens-Adams, et al. [4] as described below is used to better understand the control room operators' tasks and decision points. This information will inform the simulator experiment scenarios.

Operators are interviewed to gain a better understanding of the daily control room tasks and decisions required of them. The Applied Cognitive Task Analysis (ACTA) and Critical Decision Method are used to obtain this information.

All of the information collected will inform scenarios which will simulate plant conditions during a cyber event. A scenario-based experiment with NPP operators will be executed to determine how the operators perceived the cyber event and how they respond to them. The operators' performance will be measured and workload assessments will be collected. The results of the experiment will aid in the understanding of operator decision making during cyber-attacks and provide a platform to promote enhanced cybersecurity for the nuclear power industry.

3.1 Applied Cognitive Task Analysis

Applied Cognitive Task Analysis is a methodology in which interview methods are used to extract information about the cognitive demands and skills required for a task. This method is composed of three different techniques to elicit different aspects of cognitive skill: task diagram, knowledge audit and simulation [5]. The task diagram provides the researcher with a broad overview of tasks and highlights difficult cognitive portions of the task. The knowledge audit identifies ways in which expertise is used in a domain and provides examples based on actual experience. Finally, the simulation interview is based on presentation of a challenging scenario to subject matter experts, and asking the expert to identify major events, including judgments and decisions.

3.1.1 Task Diagram

The task diagram provides the interviewer with a broad overview of tasks and highlights difficult cognitive portions of the task. The interview consists of a series of questions allowing the interviewer to better understand the composition of the tasks and the underlying cognitive skills. The operator is asked to think about the tasks that must be completed and break them down into the component steps. The interviewer asks which steps require difficult cognitive skills (such as judgements, assessments, problem-solving and thinking skills).

3.1.2 Knowledge Audit

The knowledge audit identifies ways in which expertise is used in a domain and provides examples based on actual experience. As each aspect of expertise is uncovered, it is probed for concrete examples in the context of the job, cues and strategies used, and why it presents a challenge to novices. The knowledge audit consists of a series of probes for different topics to which the operator tries to offer instances that he or she has encountered before and explains why these instances would be difficult for a novice. These topics include:

- Past & Future: An instance in which the operator encountered a situation in which he or she knew exactly how things got there and where they were headed.
- Big Picture: An example of what is important about the big picture for the task in question, and identification of the major elements that must be known and kept track of.
- Noticing: An experience where part of a situation just "popped" out at the operator, and the operator noticed things going on that others did not catch.
- Job Smarts: A description of ways of working smart or accomplishing more with less that the operator has found especially useful.
- Opportunities/Improvising: An example when the operator has improvised in this task or noticed an opportunity to do something better.
- Self-Monitoring: A description of a time when the operator realized his or her performance or method would need to change to get the job done.
- Equipment Difficulties: An instance in which the there was disagreement within the operator's mind between the direction the equipment or instrumentation pointed and the operator's own judgement, or when the operator had to rely upon his or her own experience to avoid being led astray by the equipment.

3.1.3 Simulation Interview

The simulation interview allows the interviewer to better understand the SME's cognitive processes within the context of an incident. The interview is based on presentation of a challenging scenario to the SME. The SME is then asked a series of questions, such as:

- As the job you are investigating in this scenario, what actions, if any, would you take at this point in time?
- What do you think is going on here? What is your assessment of the situation at this point in time?
- What pieces of information led you to this situation assessment and these actions?
- What errors would an inexperienced person be likely to make in this situation?

3.2 Critical Decision Method

The Critical Decision Method [6] is an interview methodology that is implemented to better understand situation awareness and decision-making in non-routine situations. This approach is especially valuable for examining skilled performance under time pressure, which is likely a critical element in cyber-attacks.

The procedure directs the operator through the following steps:

1. Select an incident. The control room operators are asked to select an incident with certain defining parameters (e.g., a non-routine incident in which parameter readings were not conforming to expectations).

2. Obtain unstructured incident account. The control room operators are asked to describe the incident from the time they received the first alarm until the time that the incident was judged to be under control.
3. Construct an incident timeline. After the incident is relayed, a sequence and duration of each event is established.
4. Decision point identification. During the timeline construction, specific decisions are identified for further probing.
5. Decision point probing. Follow-up questions are asked about specific decisions. Different probe types may be used, including:
   - Cues (what were you seeing, hearing?)
   - Knowledge (what information did you use?)
   - Analogues (were you reminded of a previous experience?)
   - Goals (what were your goals at the time?)
   - Options (what other courses of action were considered?)
   - Experience (what specific training or experience was necessary?)
   - Time pressure (how much time pressure was involved in making the decision?)

4 CONCLUSION

The information obtained from the Applied Cognitive Task Analysis and Critical Decision Method discussions will be used to develop realistic scenarios for use in experiments with the simulator and the coupled cyber model. Licensed operators will participate in the experiment and will be asked to complete a series of scenarios on the simulator. Of particular interest is how long it takes the operator to notice that there is an issue (if the operator notices at all), what course of actions he or she takes to solve the problem and how cognitively taxed the operator is during the scenarios. Experiments with NPP operators will be carried out over FY 2018 and results of the research are expected by the end of FY 2018.

This research will help inform the nuclear power industry how to take appropriate actions to keep power plants safe from a cyber event. Key insights will be gained that will help improve operator training and procedures. The modeling capability will also provide a platform for further research and analysis of the cyber security controls within the plant and their efficacy for protecting against various types of threats. This will provide a means for advanced analysis of plant response and cyber security controls that will directly improve power plant safety and help reduce overall costs by focusing security efforts.

5 ACKNOWLEDGMENTS

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. SAND2017-2860 C.

6 REFERENCES

1. Duggan, D. P. Penetration Testing of Industrial Control Systems. SAND2005-2846P, Sandia National Laboratories, Albuquerque, NM. (2005).
2. Wueest, C. Security Response: Targeted Attacks Against the Energy Sector. Symantec. (2014).

3. Denman, M. R., Turner, P. L., Williams, R. A., Cardoni, J. N., Wheeler, T. A. Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model. Submitted to the American Nuclear Society Winter Meeting, San Diego, CA. (2016).
4. Stevens-Adams, S., Cole, K., Haass, M., Warrender, C., Jeffers, R., Burnham, L., & Forsythe, C. Situation Awareness and Automation in the Electric Grid Control Room. *Procedia Manufacturing*, *3*, 5277-5284. (2015).
5. Militello, L. G. & Hutton, R. J. B. Applied Cognitive Task Analysis: A Practitioner's Toolkit for Understanding Cognitive Task Demands. Ergonomics, 41(11), 1618-1641. (1998).
6. Klein, G. A., Calderwood, R. & MacGreggor, D. Critical Decision Method for Eliciting Knowledge. IEEE Transactions of System, Man and Cybernetics, 19(3), 462-472. (1989).