SAND2022-8126C

Performance Testing of Cyber Incident Response at Nuclear Power Plant Operators

Michael T. Rowland
Sandia National Laboratories

Andrew Hahn
Sandia National Laboratories

Samo Tomazic
Informacijska varnost, Samo Tomazic s.p.

Dave Trask
Canadian Nuclear Laboratories

Richard Brown
Canadian Nuclear Laboratories

Charles Nickerson
Idaho National Laboratory

Christopher Spirito
Idaho National Laboratory

ABSTRACT

Cyber-attacks targeting nuclear facilities are an increasing concern for nuclear security. However, unlike physical security, performance testing of cyber-security incident response at nuclear facilities has yet to develop mature, safe and secure methodologies necessary to evaluate facility staff in live or representative conditions.

Exercises are one way to test the effectiveness of the cyber program, train staff, increase awareness, ensure that the appropriate tools and processes are available and effective, and that pre-requisites for response and recovery systems are in place before they are needed in order to assure safety and business continuity in a cyber event. Exercises are also an effective way to strengthen interfaces with the Regulator and other regional or national departments who could support the industry in the event of a significant cyber security attack.

In 2021, a collaborative research and development project between Canadian Nuclear Laboratories, Idaho National Laboratory, and Sandia National Laboratories was commenced. This project will develop and conduct cyber security exercises to support Nuclear operators and relevant staff within the facility, in understanding how to recognize a cyber-attack, how to respond to an attack, how to conduct forensic analysis to determine the consequences of the attack, and elements to consider when developing a cyber incident response program. Exercises involving "live" attacks on Operational Technology systems are planned for March 2022 at CNL's cyber centre, with a second exercise planned for May 2023 involving a blended attack (physical intrusion supported by a cyber-attack) at Sandia's Nuclear Security Technology Complex. This paper will discuss the outcomes of the March 2022 and the planned efforts for May 2023.

INTRODUCTION

Over the past two decades, cyber security practitioners were focusing primarily on raising awareness of cyber security. The goal was to have cybersecurity considered as a key and essential part of nuclear security. However, as the nuclear industry has matured, both regulators and Nuclear Power Plant operators, the need for performance-based evaluations for cybersecurity has become critical.

One of the best ways to raise evaluate performance is by conducting exercises. During exercises the administrative and technical cyber security measures are tested, and if these exercises include hands-on experience in a real-life environment, the test results are much improved and more representative of an operator's actual response capabilities.

In 2019, Canadian Nuclear Laboratories commenced a project to develop a methodology for the conduct of cybersecurity exercises and effectiveness evaluations. This project focuses on the challenges associated with assessing a nuclear operator's ability to respond to cyber security incidents in a timely manner. Given the scope and importance of the effort, Department of Energy's Office of International Nuclear Security (INS) agreed to provide both subject matter expert (SME) support from Idaho National Laboratories (INL) and Sandia National Laboratories (SNL) and a location (i.e., SNL Integrated Security Facility). Bruce Power (operator of a NPP in Canada) will assist in scenario design and providing the "blind" participants (i.e., Central Alarm Station (CAS) Operators and Cyber Security Operations Centre (SOC) Operators).

The project will develop and conduct cyber security exercises to support Nuclear Power Plant (NPP) operators and relevant staff within the facility, in understanding how to recognize a cyber-attack, how to respond to an attack, how to conduct analysis to determine the consequences of the attack, and elements to consider when developing a cyber incident response program. The main exercise will take place on 15-19 May 2023 and will involve all the organizations listed above as well as additional observers from the Canada Nuclear Safety Commission (CNSC), Natural Resources Canada (NRCan), and other interested organizations.

RESEARCH OBJECTIVES

This research project will result in 1) a methodology and capability to plan and conduct real-time functional cyber security exercises in a state-of-the-art environment that is purpose-built to support realistic training and exercises and 2) conducting future exercises with nuclear operators either to support organizational training and coordination or evaluation of response processes.

This effort will enable research on how attacks manifest themselves, and to further enhance abilities to respond to an attack and to measure overall level of preparedness. In addition, the research will potentially yield information regarding the resources, capabilities, tools and planning needed to prepare for, conduct, and evaluate exercises.

The project is divided into two major categories of exercises. Each exercise is described below:

1. The first "functional" exercise (March 2022, Sept 2022) examines the capabilities of the NPP operators to recognize a cyber-attack and respond to cyber security incidents in real-time using simulated NPP Operational Technology (e.g., Balance of Plant, Safety) systems. The simulated environment will comprise a representative main control room (MCR) and Cyber SOC interacting with either actual and/or emulated operational technology.

2. The second "blended attack" exercise (May 2023) will examine the communications and coordination between physical and cyber security teams to respond to blended cyber-physical attacks requiring a coordinated physical and cyber response. The cyber-attack will target the Physical Protection System and possible OT systems in support of a real tactical (i.e., physical intrusion).

This project will provide valuable insights and experience on how cyber-attacks manifest themselves in both OT and PPS. The major and most significant deliverable is to develop and verify a methodology for identifying and specifying performance-based criteria associated with effective incident response, and to practice and further enhance the abilities of participating organizations to respond to an attack and to measure their overall level of preparedness. This substantial bilateral collaboration between Canada and the USA allows an opportunity to further advance nuclear security through information sharing and pooling of resources and expertise.

ORGANIZATION ROLES AND RESPONSIBILITIES

Canadian Nuclear Laboratories (CNL) is cooperating with Sandia National Laboratories (SNL) and Idaho National Laboratory (INL) on a project that aims to support the assessment of nuclear operator's ability to respond to blended cyber-physical attacks.

CNL (Method, Performance Criteria, Playbooks):

- Lead Research Effort; and
- Methodology and processes to support evaluations of organizational effectiveness in detection, assessment, and response to blended attacks at NPPs.

Sandia National Laboratories (Site, Technology, Physical Protection):

- Site for hosting event;
- Provide the infrastructure and technological platforms (PPS, CAS, Cyber SOC, Asherah Simulator/SMR Mock Up) to allow for the methodology and processes to be validated; and
- Develop adversary emulation environment (computer-animated; SCRIBE3D).

Idaho National Laboratory (Cyber Security):

- Provide Adversary characterization and emulation; and
- Perform cyber-attacks at site location to support the event.

NPP Operators (Bruce Power, Test Participants):

- Will not be assessed a Pass or Fail; the methodology validation is the primary research goal;
- Canadian and US Domestic operators have been informally requested to provide staff;
- Operator staff will be familiar with the Site and the technology platforms; and
- "Blind" research participants; no awareness or information regarding the attack steps, goals or targets.

Other Organizations (INS, NRCan, Global Affairs Canada, CNSC, IAEA):

- Funding and/or Advisory role to select candidate scenarios, specific gating criteria, and provide lessons learned.

BLENDED ATTACK LOCATION

The Integrated Security Facility (ISF) of Sandia National Laboratories delivers next generation solutions for cyber resilience and physical protection to critical national security issues by providing technical training, demonstration, and research/development, and technical testing capabilities for security related technologies.

ISF (*Figure 1*), also known as Technical Area V (TA-V), is a one-of-a-kind resource for improving global nuclear security. The center includes a decommissioned nuclear reactor and facilities that were converted into mock nuclear operational environments that mimic facilities in the nuclear fuel cycle. The ISF provides a realistic venue to demonstrate and evaluate security elements such as:

- Perimeter Intrusion Detection and Assessment System;
- Entry Control Portal (*Figure 2*);
- Central Alarm Station (*Figure 3*);
- Central Alarm Station Server Room (*Figure 4*);
- Access Delay and Response Survivability Elements;
- Mock Category I Nuclear Material Receiving and Storage Area;
- Mock Category I Nuclear Material Processing Facility;
- Mock Category II Research Reactor;
- Mock Radiological Source Facilities; and
- Mock Nuclear Power Plant and AR/SMR Reactor Facility.

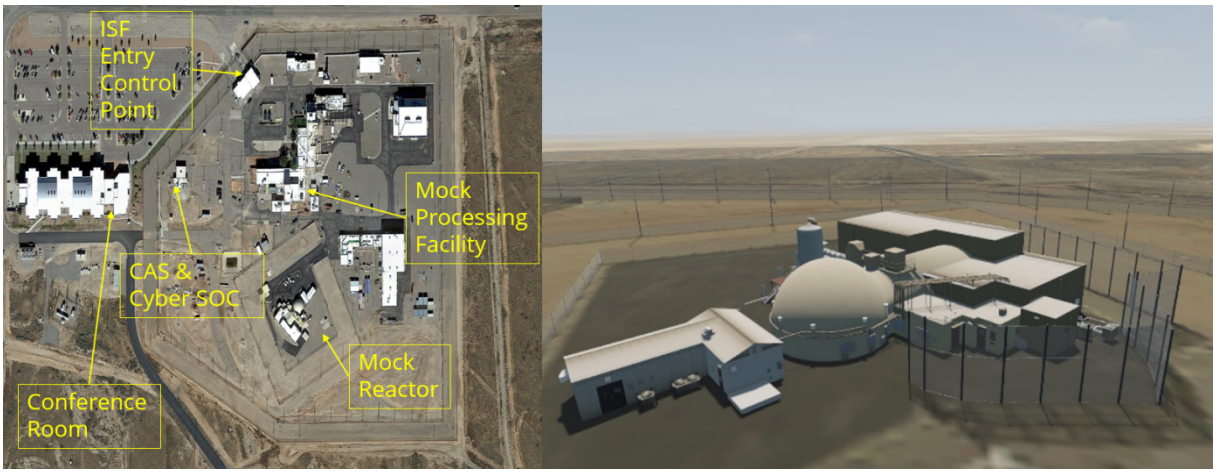

Figure 1: Integrated Security Facility (ISF) at SNL

Figure 2: Entry Control Portal

Figure 3: Central Alarm Station (CAS)

Figure 4: Central Alarm Station (CAS) Server Room

KEY CONSIDERATIONS

Cyber-attacks are getting more and more sophisticated. Adversaries aren't targeting just business systems, but also critical infrastructure facilities. Adversaries have also recognized the value of cyber capabilities to support malicious acts against nuclear sector. Cyber-attacks provide for:

- Expand of the attack surface (e.g., Supply Chain);
- Expands of the attack timeline (cyber-attack can span for months/years); and
- Provides the adversary with potential for different combinations or sequences of attack (attack does not need to be completed in a specific order; but based on opportunity).

Additional challenge arises with physical protection systems, where these typically do not have current cybersecurity design features (DCSA) or technical measures (Intrusion Detection) implemented.

In order to address those challenges, we divided the project to three main objectives:

1. Perform a blended attack event to validate a methodology and platform that:
    - Provides timing/gating criteria for completion of necessary tasks/activities by the Cyber Security Operations Center (CSOC) and Central Alarm Station (CAS) operators;
    - Establishes criteria that for quality/elements/attributes of each task/activity to be deemed successful; and
    - Will advance best practices and technology with specific focus on the integration of Physical Protection and Cyber Security.
2. Cyber-attacks will be performed on the ISF:
    - PPS and/or Cyber SOC will be compromised. May involve remote and local attacks, software, network, and/or hardware based; and
    - Adversary will be 'live' and performed by INL.

3. Physical attack will be 'live':
    - Computer Animation (SCRIBE3D) will show adversary progression in a time-based format and assist in planning activities;
    - Physical Intrusion and the associated Stimuli in real-time and space (smoke, vibration, rumble blocks) are being specified and planned for; and
    - Occupational Health and Safety and Worksite rules limit the level of physical stimuli, tactical attack/response that can be performed.

PATH AHEAD

Project started on October 25th 2021 with a Project Kick Off Meeting and will finish on May 19th 2023 with a Signature Event.

The project is now in its second year of three. The first year included a tabletop ransomware attack on a Nuclear Power Plant (NPP) and this year a functional hands-on exercise was conducted with Canadian NPP Operators at CNL's National Innovation Center for Cyber Security in Fredericton New Brunswick from 2022 March 7-10. The final year will result in a blended cyber physical attack exercise to be held at SNL (Technical Area V) from 2023 May 15-19.

MEETINGS AND EVENTS

There are eight in-person and virtual meetings planned for this project. These are listed below:

Table 1: Outline of meetings

#	Meeting	Date	Location	Status
1	Project Kick Off Meeting	25th – 28th October, 2021	SNL	Completed
2	November Fredericton Trip	29th November – 3rd December, 2021	CNL	Completed
3	Cyber Exercise at CNL	7th – 10th March, 2022	CNL	Completed
4	Agreement on the Project Plan Selection of Candidate Scenarios	2nd – 6th May, 2022	SNL	Planning
5	Methodology Review	13th – 16th June, 2022	Virtual	Planned
6	Final preparation meeting before the Dry Run	17th – 21st October, 2022	SNL	Planned
7	The Dry Run	20th – 24th February, 2023	SNL	Planned
8	Signature Event	15th – 19th May, 2023	SNL	Planned