# BUILDING CAPABILITY FOR COMPUTER SECURITY ASSURANCE ACTIVITIES THROUGH INTERNATIONAL COOPERATION

LAURENT MOUTENOT
Electricité de France (EDF) - French Nuclear Security Center of Excellence (CoE)
Paris, France
Email: laurent.moutenot@edf.fr

GUSTAVO BERMAN
Comisión Nacional de Energía Atómica (CNEA)
Bariloche, Argentina
Email: tavo@cab.cnea.gov.ar

RICARDO PAULINO MARQUES
Universidade de São Paulo (USP)
São Paulo, Brazil
Email : ricardomarques@usp.br

PAUL SMITH
Lancaster University (LU)
Lancaster, United Kingdom
Email : paul.smith@lancaster.ac.uk

RODNEY BUSQUIM E SILVA
International Atomic Energy Agency (IAEA)
Vienna, Austria
Email r.busquim@iaea.org

## Abstract

This work presents the framework and the outcomes of a pilot *Workshop on Conducting Computer Security Exercises for Nuclear Security* hosted by the French Nuclear Security Centre of Excellence, designed and organized by the International Atomic Energy Agency (IAEA) and subject matter experts from different IAEA Member States, and delivered for the European countries. Computer security exercises are assurance activities that improve cyber security response preparedness for countries, operators and organizations. This workshop employed the IAEA fictitious State of Anshar with a realistic scenario-based storyline, using a sophisticated specifically designed simulation environment capable of simulating real-time operational technology (OT) and information technology (IT) cyber-attacks, to train participants with methodologies to prepare, conduct and evaluate computer security exercises. The design of this event considered the IAEA computer security guidance applied for the State of Anshar facilities (Asherah Nuclear Power Plant, Shapash Nuclear Research Institute and Gula Regional Hospital), including simulators of: representative IT/OT systems of nuclear power plant; a heating, ventilation and air conditioning systems; physical protection systems; and a radiotherapy clinic in a simulation environment developed based on the lessons learned from the IAEA's support to the Brazilian Cyber Guardian Exercises (5 editions, from 2018 to 2023) and the Slovenia KiVA Exercise (2022). The participants were exposed to a well-organized real-time escalating campaign by a threat group aiming at different targets within the State of Anshar. They were called to play collectively as members of incident response teams and in this process, improve their capability to design and deploy similar events. The event provided information for the participants to adapt the IAEA simulation environment to their national context, organization and procedures, in order to develop future training or awareness activities more relevant to their Member States. This pilot workshop exceeded the expectations of the trainees in terms of quality of its content and sophistication of IAEA simulation environment. In addition, it increased the international cooperation and sharing of information on how to detect, response and protect against cyber-attacks.

## 1. INTRODUCTION

During the week of 18-22 March 2024, IAEA conducted a *Regional Workshop on Conducting Computer Security Exercises for Nuclear Security*. This event was hosted by the French Nuclear Security Center of Excellence (CoE). Subject matter Experts (SMEs) from different countries supported the development of the workshop training material and the delivery of the event. This event was designed to support the preparation and execution of a computer security exercise to enhance the effectiveness of nuclear organizations in responding to computer security threats, and to promote the sharing of national and international information on cyberthreats. Its objective was to raise participants' awareness of the threat of cyber-attacks, and their potential impact on nuclear security by conducting a life-fire computer security exercise for a simulated adversary cyber-attack.

Following the Brazilian Cyber Guardian Exercises (CGE) experience [1], this workshop applied the IAEA computer security publications such as Nuclear Security Series (NSS) 17-T Rev. 1 [2], NSS 42-G [3], NSS 33-T [4], TDL-005 [5] and TDL-011 [6], and international best practices. It also applied the guidance on the draft publication on “Preparation, conduct and evaluation of computer security exercises for Nuclear Security”.

The SMEs further developed a sophisticated simulated environment that comprehends:

a) representative information technology (IT) and operational technology (OT) systems within the Asherah Nuclear Power Plant Simulator 2.0 (ANS 2.0).
b) a Radioactive Material Handling Laboratory (RMHL) heating, ventilation and air conditioning (HVAC) system simulator of the Shapash Nuclear Research Institute (SNRI); and
c) radiotherapy clinic simulator of the Gula Regional Hospital (GRH).

This sophisticated simulated environment allowed the participants to have real time access to OT and IT systems, both from the physical process as the network process. For example, the participants have real time access to nuclear power plant processes variables such as temperature of moderator, density of water, fuel temperature, humidity, reactivity, pressure; to physical protection systems such as access control systems, video streams in a hospital and nuclear power plant; humidity, pressure and temperature in a specific laboratory that handles radioactivity material, and OT and IT network information using the Wireshark [7] application for network packet analysis. In addition, a built-in email system facilitates the use of the artifacts and injects and real-time communication among all participants, which provide the participants with full immersive exercise experience.

Besides presenting the theory behind executing a computer security exercise and executing an exercise, the workshop aimed to give the participants enough information to use and adapt the exercise material: simulators, environment, tools, injects and methodology. This paper describes the tools and methods used during the workshop and presents the outcomes from the point of view of participants. It also summarizes the lessons learned and next steps in the development process.

## 2. WORKSHOP OVERVIEW

This workshop comprised of state-of-the-art technical and schooling activities, designed by international experts, which were taken into account at all stages of the development:

a) motivated instructors and engaged audience;
b) sophisticated and immersive realistic environment;
c) credible scenario; and
d) adequate injects, tasks and actions as expression of the scenario and the environment.

### 2.1. Participants learning objectives

Upon completion of this workshop, the participants are able to:

e) Recognize that computer security exercises are assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security.
f) Recognize that the IAEA NSS publications provide guidance on computer security for nuclear security.
g) Recall the process of preparing, conducting and evaluating a computer security exercise specifically designed to assess capacities and capabilities for prevention and detection of, response to and recovery of computer-based systems from cyber-attacks.
h) Recall the application of the IAEA computer security exercise and training tools, i.e. the simulators, and how to adapted them for an organization or Member States needs.
i) Recognize that computer security incident response only succeeds when planned with respect to the operational domain it will be executed in.

j) Recognize the importance of an effective and credible scenario for conducting a computer security exercise.

## 2.2. Workshop Audience

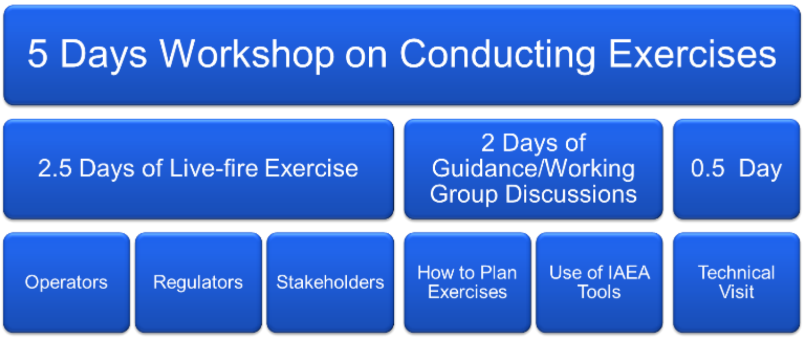
This event was designed for nuclear security professionals that have responsibilities for computer security, and allowed the participation of nuclear security professionals responsible for conducting training and exercises. 35 participants attended the event from the following Member States: Austria, France, Germany, Poland, United Kingdom and Romania. Experts from Argentina, Brazil, France, United Kingdom and Romania supported the development or the delivery of the workshop.

## 2.3. Workshop framework

The 5 days' workshop consisted of the following activities:

a. discussion-led presentations on computer security incident response.
b. discussion-led presentations on how to plan, prepare, conduct and evaluate a computer security exercise.
c. two and a half days training activity on how to conduct a real-fire computer security exercise.
d. working group discussions on how to adapt the IAEA training tools to the Member State's needs.

The high-level agenda of the exercise considered the activities presented in Figure 1:



5 Days Workshop on Conducting Exercises

2.5 Days of Live-fire Exercise

2 Days of Guidance/Working Group Discussions

0.5 Day

Operators

Regulators

Stakeholders

How to Plan Exercises

Use of IAEA Tools

Technical Visit

Figure 1 – Summary of workshop agenda

The 2,5 days of conducting a computer security exercise comprised of incident response activities with about 75% of the events or incidents being internal to the organization, i.e. requiring internal communications, and 25% being focused on communication with competent authority and technical authority, i.e. requiring external communications. These activities were conducted using an updated version of the IAEA environment for conducting training and exercises. The participants were divided into groups of 3 trainees who used this exercise environment. The roles that are external to a facility, such as the competent authority and technical authorities, are simulated in the exercise using the built-in email injects, which the participants had to respond to. The controller conducting the exercise used a Configuration and Attack Terminal to send the injects, start and stop a real-time attack.

The credible storyline explored the full potential of the IAEA environment, while also being able to provide the participants with challenging situations. Similar to the CGE 4.0, the fictitious hacker group Radionuclide Liberation Front (RLF) set up an escalating cyber-attack campaign to access to nuclear or radioactive materials in the State of Anshar. The storyline has been expressed in terms of scenarios, injects, tasks and actions. More than 100 injects were prepared and delivered using the embedded email service. All the key stakeholders had individual emails accounts, such as the CEO of the SNRI, or the maintenance engineering of ANPP, and each workstation, The injects and environment set-up are consistent, realistic and able to allow the participants an effective grasp of the scenarios while providing valuable information.

The storyline can be summarize as following:

i. it started with an OT attack against a SNRI HVAC air-gaped network, and included insider threat and supply chain issues. This scenario allowed the participants to get familiar with the exercise environment and stressed the need for a Computer Security Incident Response Team (CSIRT), as presented in Figure 2.

ii. the following scenario included an IT ransomware and OT blended attack against a GRH radioactivity clinic, with three distinct sub-networks, and stressed the need of network segregation and the importance of a computer security programme (CSP) for any facility that deals with nuclear or radioactive material.

iii. the next scenario included more complex IT and OT cyber-attacks and explored supply chain issues, insider threat, bring your own device, policy, safety and security interface, blended attack. The ANS 2.0 played was essential to present representative application of adequate defensive computer security architectures (DCSA), and explored the application of computer security control to OT systems. It exercised the role of CSIRT and the importance of a CSP in place.

During the 2 days of working group discussions, the SMEs guided the participants on how to tailored an exercise, using the IAEA tools, to the needs of their organizations. This included hands-on activities on how to install the tools, and discussions on how to prepare a storyline and a master scenario event list (MSEL).

The CoE organized a technical visit at the *Institut de Radioprotection et de Sûreté Nucléaire* (IRSN) that included discussions about use of simulators for assessment of cyber-attacks in nuclear facilities and national capabilities on responding to safety emergencies and nuclear security events.

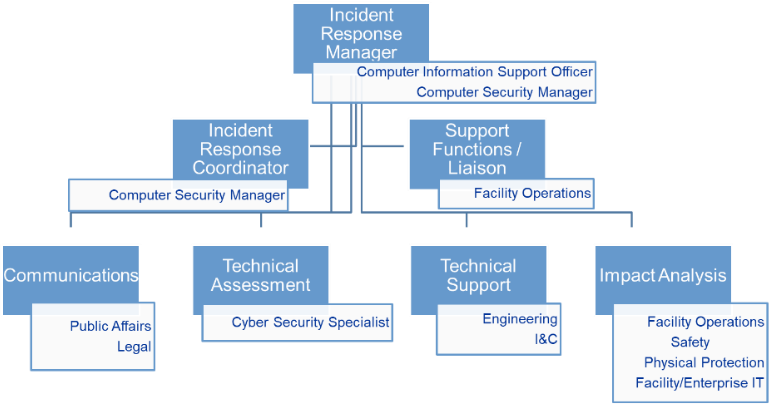

Incident Response Manager
Computer Information Support Officer
Computer Security Manager
Incident Response Coordinator
Computer Security Manager
Support Functions / Liaison
Facility Operations
Communications
Public Affairs
Legal
Technical Assessment
Cyber Security Specialist
Technical Support
Engineering
I&C
Impact Analysis
Facility Operations
Safety
Physical Protection
Facility/Enterprise IT

Figure 2: Notional roles in a computer security incident response team [5]

With the support of the Ontario Tech University, Asherah Nuclear Power Plant (ANPP) scenario included a proof of concept of a Security information and event management (SIEM), built-in the ANS 2.0 environment, using Suricata [8] for network open-source network analysis and threat detection software, and Arkime [9] for network analysis and packet capture. This proof of concept was tested to detect one of the OT attacks against the control rod drive mechanism causing power disruption.

## 3. EXERCISE ENVIRONMENT

The exercise was conducted using three simulators specially designed for conducting training and exercises, integrated in a sophisticated virtual environment for an immersive experience. This environment, developed using Docker/container technology [1] and accessed through a web browser, allows independent real-time (life-fire) experience for each team of participants. Each group of 3 participants used a workstation with a dashboard, human machine interfaces, embedded email system, and with access to all information need to react to the computer security events and incidents. In addition, a virtualized container-based framework made possible for the straightforward deployment of the scenarios without major computational requirements, being convenient for hands-on training courses.

In order to be available to all Member States, and to allow open discussion amongst participants from different countries and organizations, the exercise was implement using a sophisticated virtual environment that reproduces selected systems from three very different facilities of the fictitious State of Anshar, showed in Figure 3: a HVAC system in a laboratory in the SNRI; an access control system, a treatment planning system (TPS) and teletherapy unit (TTU) in a radiotherapy clinic in the GRH; and IT and OT systems in a complex network where 1 to 5 security levels, with respective security zones and computer security measures, delivered a DCSA in the ANPP. For each scenario videos have been created. Displayed at various stages of the scenarios, they contribute to provide a global immersive environment. Fictitious websites for each facility, accessible by the participants, are also part of the simulation environment.

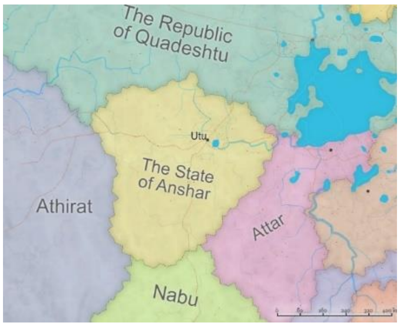


Figure 3 – The State of Anshar

## 3.1. State of Anshar

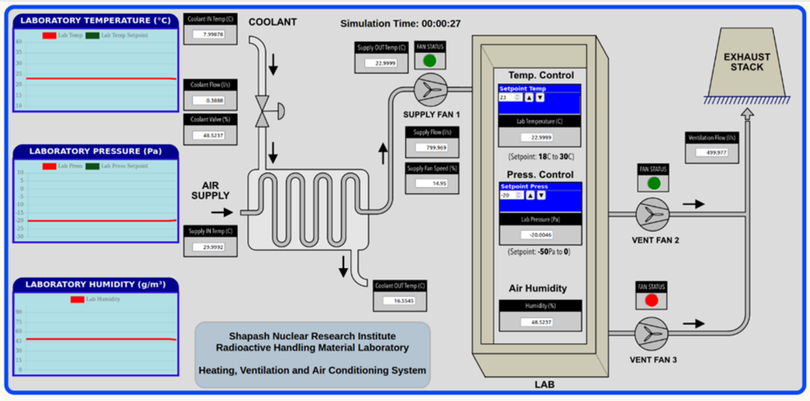
The fictitious State of Anshar is a signatory to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and it is an IAEA Member State. Anshar has completed the ratification of both the Convention for the Physical Protection of Nuclear Material (CPPNM) and its Amendment (CPPNM/A). Anshar has a well-established nuclear sector with major stakeholders and suppliers. During the exercise, besides law enforcement organizations such the Anshar Federal Police that provides responsible support to nuclear security events, the participants interacted with the following stakeholders and suppliers:

a. Anshar Atomic Energy Authority (AAEA) implements the state strategy to ensure the preservation of public health and safety by overseeing commercial uses of Nuclear Energy in Anshar
b. Anshar Cyber Security Center (ACSC) provides technical expertise to support Anshar government in the areas of Information and Computer Security.
c. Anshar Security Intelligence Service (ASIS) is the intelligence agency within Anshar charged with monitoring and protecting the country from acts of espionage, sabotage, and terrorism.
d. Cooperzino Inc. provides industry-leading system design resources, leading-edge technology options and unparalleled customer support tools to ensure reliable, long-term perimeter detection solutions for the infrastructural, asset and personnel protection challenges of their global client base.

## 3.2. SNRI exercise context

The fictitious SNRI was inaugurated in 1950 to serve as the Republic of Anshar's premier nuclear energy research facility. The Institute houses various research, fuel fabrication, administrative, and plant support facilities. It is responsible for production of radioactive sources for hospital in the State of Anshar, such as GRH, and in neighbourhood countries. The workshop participants received detailed information about SNRI, including resources, laboratories and information about its site and management and organizational structure.

The Radioactive Material Handling Laboratory (RMHL) is a sensitive laboratory where the room pressure is kept below normal atmospheric pressure by the HVAC system to prevent radioactive particles or gases to spread outside the lab. RMHL cannot operate without the HVAC and the Anshar regulator requires that scheduled maintenance be performed regularly. The exercise scenario comprehends supply chain issues, insider threat, and the compromise of an OT air-gaped network using the Modbus protocol. The participants interact with the environment through out a human machine interface (HMI) presented in Figure 4.



Simulation Time: 00:00:27

Coolant IN Temp (C) 7.99878

Coolant Flow (l/s) 0.3888

Coolant Valve (%) 48.5237

Supply IN Temp (C) 29.9992

Coolant OUT Temp (C) 16.5545

Supply OUT Temp (C) 22.9999

Supply Flow (l/s) 799.969

Supply Fan Speed (%) 14.95

Setpoint Temp 23

Lab Temperature (C) 22.9999

(Setpoint: **18**C to **30**C)

Setpoint Press -20

Lab Pressure (Pa) -20.0046

(Setpoint: **-50**Pa to **0**)

Humidity (%) 48.5237

Ventilation Flow (l/s) 499.977

Figure 4 – HVAC (HMI)

## 3.3. GRH exercise context

The fictitious GRH is in Utu, the capital of Anshar with a population of 2 million. GRH is a specialized hospital that provides a variety of medical services to the State of Anshar, primarily acting as a regional center for health service treatments utilizing radioactive materials. More than 600 patients use GRH services in a weekday, and at least 350 during the weekend. While GRH provides general services, the majority of patients are admitted for specialized treatments using radiological techniques. During regular business hours there are a minimum of 1000 patients, staff, contractors and visitors on site. The workshop participants received detailed information about GRH, including its organizational structure, medical infrastructure, and policies, site security, plans and procedures that need to be followed by its staff, doctors and nurses. The exercise scenario comprehends IT (TCP/IP protocol) and OT (Modbus protocol) attacks, a TTP ransomware, release of sensitive date to the Internet, the compromise of the access control system and a blended-attack targeting blood irradiators with Caesium 137 (Cs-137) and TTU with Cobalt 60 (Co-60). The network architecture of GRH Oncological Wing, simplified in order to exclude parts not related to the exercise, has two subnets, as shown in Figure 5.

i. GREEN: Free Public WIFI to be used by patients and staff. No password required.
ii. PURPLE: Hospital staff WIFI for GRH personnel to access patients' information, use computer resources and communicate throughout the hospital. Password required.
iii. BLUE: Security wired network. Blue network runs through GRH. Endpoints are cameras, sensors, etc. End points report to Central Alarm Station. Password required.
iv. RED: Fire and Safety wired network. Enables fire sensors and life monitoring devices to communicate with nurse station. No password required.

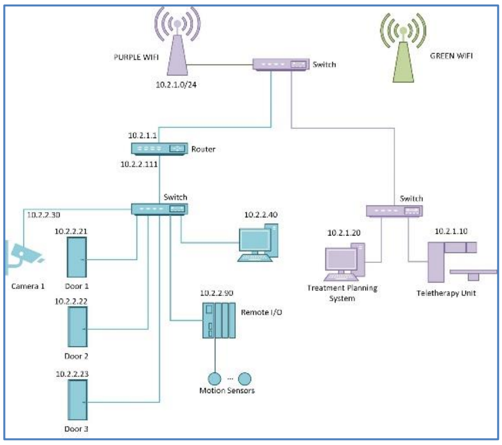


Figure 5 – Network Architecture of GRH Oncological Wing (simplified)

## 3.4. ANPP exercise context

Asherah Nuclear Power (ANP) is a leading energy company focused on electric power, distribution operations, and other energy services in the State of Anshar region, focusing on nuclear power and associated energy assets. They deliver safe, affordable, and reliable energy to approximately 500,000 customers in the northern region, including the city of Utu, Anshar capital. Customers can depend on ANP all year long, particularly during hot Anshar summers and cold winters.

ANPP shown in Figure 6, is an 830 Mwe Pressurized Water Reactor (PWR) commissioned in 1976 and has been the State's most important electricity producer for more than 45 years - all of it clean and carbon-free. The State of Anshar originally licensed ANPP to operate for 40 years. Part of ANPP instrumentation and control (I&C) has been renovated during the 40 year’s outage and digitalized. This includes for instance the control rod drive mechanism (CRDM) system and its network. ANPP get a license extension for 20 years more.

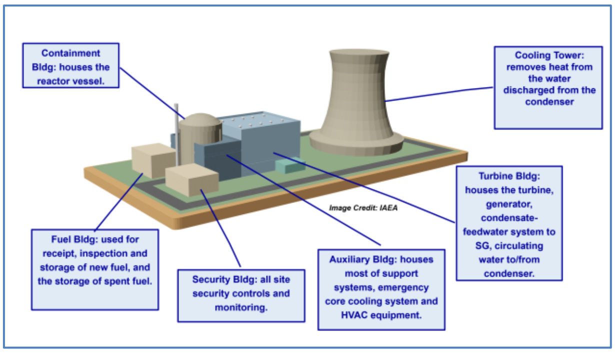
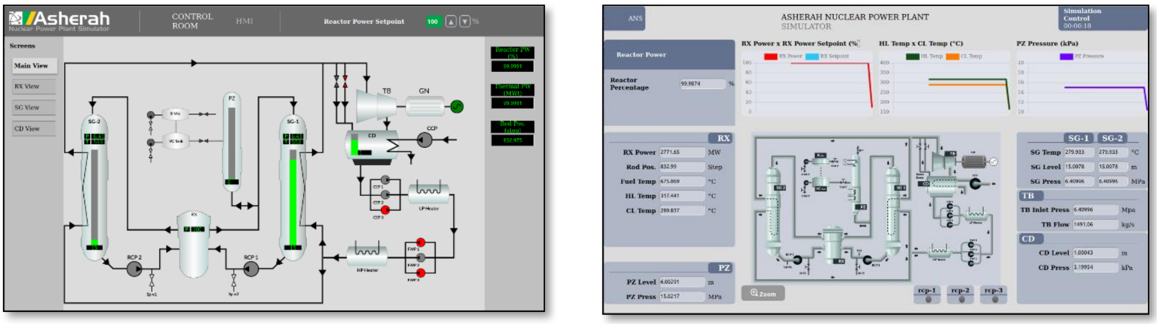

Containment Bldg: houses the reactor vessel.
Cooling Tower: removes heat from the water discharged from the condenser
Turbine Bldg: houses the turbine, generator, condensate-feedwater system to SG, circulating water to/from condenser.
Image Credit: IAEA
Fuel Bldg: used for receipt, inspection and storage of new fuel, and the storage of spent fuel.
Security Bldg: all site security controls and monitoring.
Auxiliary Bldg: houses most of support systems, emergency core cooling system and HVAC equipment.

Figure 6: Asherah Nuclear Power Plant

The workshop participants received detailed information about ANPP, including its organizational structure, engineering details about the primary, secondary and tertiary loops, security infrastructure, and policies, plan and procedures, relationship with the regulator, suppliers among others. The ANPP scenario is complex and realistic and it included: supply chain issues, cloud computing security, insider threats, safety-security interface, denial of service, breach of bring your own device procedures, release of sensitive date to the Internet, physiological warfare, facility website compromised, blended attack among others. The exercise scenario comprehends IT (TCP/IP protocol) and OT (Modbus protocol and OPC-UA) attacks. Figure 7 presented examples of the main control room HMI available for the participants.



Reactor Power Setpoint 100 %

Reactor PW (%) 99.9991

Thermal PW (MWt) 99.9991

Rod Pos. (step) 832.975

Simulation Control 00:00:18

Reactor Percentage 99.9874 %

RX Power 2771.65 MW

Rod Pos. 832.99 Step

Fuel Temp 675.059 °C

HL Temp 317.441 °C

CL Temp 289.837 °C

PZ Level 6.00291 m

PZ Press 15.0217 MPa

| | SG-1 | SG-2 | |
|---|---|---|---|
| SG Temp | 279.933 | 279.933 | °C |
| SG Level | 15.0078 | 15.0078 | m |
| SG Press | 6.40996 | 6.40996 | MPa |

TB Inlet Press 6.40996 Mpa

TB Flow 1491.06 kg/s

CD Level 1.00043 m

CD Press 5.19954 kPa

Figure 7: Examples of ANPP HMI available for the participants

The ANS 2.0 simulation environment employed a comprehensive 1 to 5 security level DCSA network that can be seen  Figure 8. Besides the simulation of all neutronics and thermohydraulic nuclear power plant processes, which allows for the assessment of the impact of a cyber-attack, all the OT and IT packets can be captured and analyzed in real time using Wireshark (also available for the SNRI and GRH scenario) independently for each participant workstation.

### 3.5. Email system and exercise network infrastructure

Each group of participant has an email box to communicate towards internal and external entities (see Figure 9 for example of tools available under the simulation environment). This is used for communication as well to receive access to artifacts and injects. The exercise book, available for all participants, had detailed information about the stakeholders, profiles and how to use the email system.

The simulation environment runs on a Docker/container implementation. This allows each group of players to have independent access to their own environment, to better understand a realistic IT and OT cyber-attack scenario following a real-time escalating adversary campaign, within a network architecture that applies the IAEA guidance on computer security. Each trainee workstation has three screens, which allows the group of participants to display various available tools, and can be deployed using a wired or wireless network.

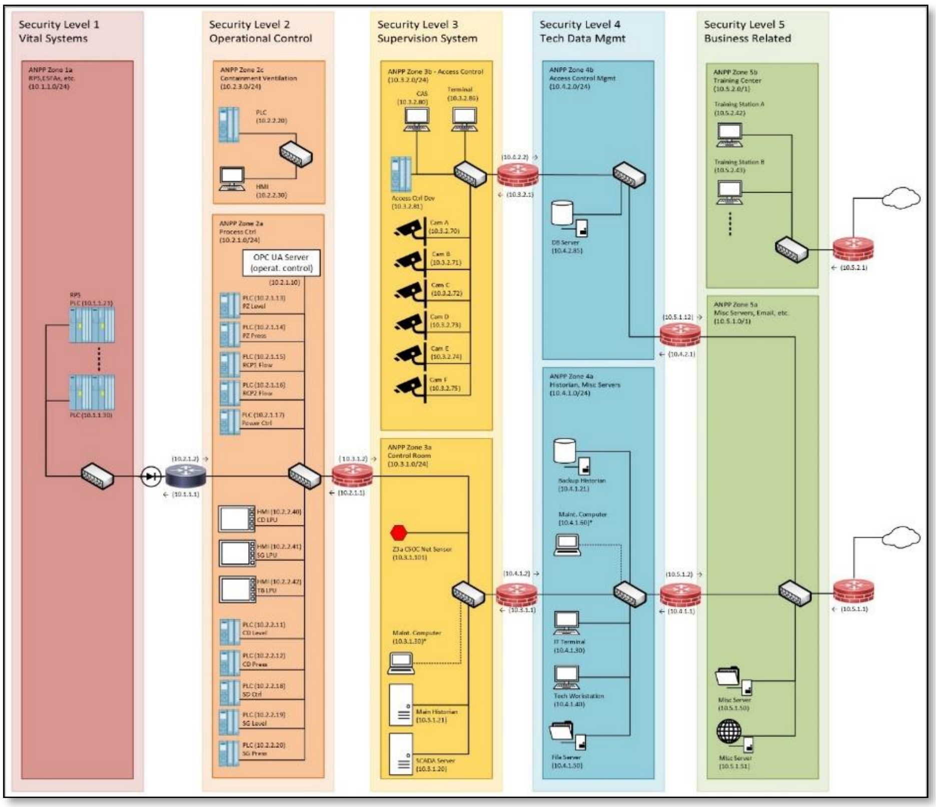


Figure 8: ANS 2.0 DCSA network deployed for the exercise

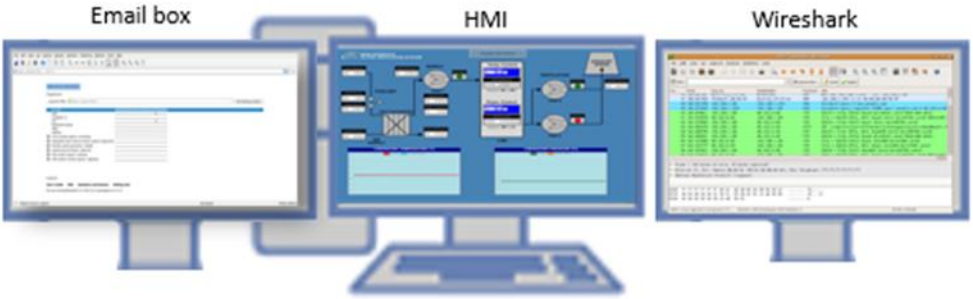


Figure 9: Example of tools available under the simulation environment

## 4. OUTCOMES, RESULTS AND SUMMARY OF PARTICIPANT’S FEEDBACK

The workshop oral and written feedback from the participants was outstanding. The participants stated that the workshop was very well developed and highlighted that the use of very sophisticated simulation environment, easy to deploy and addressing not only nuclear power plants, but also research reactors and hospitals, enriched the learning experience and facilitated group discussions.

It is worth note that the participants were from many different types of roles (regulators, systems engineering, information security, management, physical protection, safety etc.) and all were able to internalize the messages, respond to the real-time requests, and understand how to tailor the tools to the needs of their own organizations. The main outcomes and outputs of this workshop are:

1) Computer security exercises conducted: using an specially designed environment, for an international audience, and with heterogenous background allowed the exchange of knowledge and information on cyber-threats for nuclear security.
2) Enhanced participants knowledge on how to apply the IAEA computer security guidance and use the IAEA simulation environment, i.e. the simulators, and how to adapted them for an organization or Member State's needs.
3) Trainees recognized that computer security exercises are assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security.
4) Enhanced knowledge on the IAEA NSS publications on computer security for nuclear security, and on the framework for preparing, conducting and evaluating computer security exercises.
5) Trainees recognized the importance of an effective and credible scenario for conducting a computer security exercise.
6) Complete and updated threat scenario, with cyber-attacks against a HVAC system, against a radiotherapy clinic in a hospital, and complex information and operational technologies against a nuclear power plant. This updated scenario will used as reference for Agency future exercises events.
7) A revised web version of the ANS 2.0, of the simulator of HVAC system, and of the simulator of GRH radiotherapy clinic that allows each team to have access to its own real-time exercise environment.
8) Trainees stated that they would directly apply the lessons learned and adapt the associated guidance within their facilities and organization. and all were able to internalize the messages.

Table 1 summarizes the participant's feedback considering that the audience was very heterogenous with nuclear security experts with cyber security and physical security expertise, nuclear safety experts with little cyber background, cyber security specialist with little nuclear expertise. This heterogenous of the audience was taken into consideration during the design of the event and resulted in a simplified storyline and scenario.

Table 1 – Summary of participant's feedback

| | **Simulation environment** | **Workshop design** | **Workshop conduction** |
|---|---|---|---|
| **Very positive feedback** | - The modularity, flexibility of all tools that allows for different types of events (exercises, training, training, awareness, self-training) is outstanding<br>- Simulation environment is very easy to use from the player/trainee point of view<br>- Simulation environment allows for a very effective real-time demonstration of the real-world effects of cyber-attacks on nuclear installations.<br>- Simulation environment facilitate the understanding or the impact of a cyber-attack in IT, OT environment and allowed an easy access to exercise information.<br>- Simulation environment is very easy to be deployed. | - Mixed participating organizations, with different technical background (cyber and not cyber related), and international participating enhanced the trainee experience<br>- Large variety of questions (technical, managerial, legal, communication) enhanced the participants understanding of the impact of a cyber attack for nuclear security.<br>- Connection of scenarios through a continuous overall story and its staging enriched the participants learning experience.<br>- Very well-presented perspective from a player point of view and then from an instructor point of view, provided in the workshop sequence, allowed for a better understanding of the impact of cyber-attack.<br>- The workshop allowed for constant exchange of information between group participants related to decision and actions in response of a cyber-attack. | - The exercise was very interactive with a good balance between presentation, discussion and practical activities<br>- Attention and prompt and precise responses from instructors<br>- Instructors encouraged questions and communicated information well.<br>- Relaxed way of interacting among the instructors, and between the trainees and participants<br>- Periodic interventions by instructors on the substance of crisis management (as part of training) |

| | **Simulation environment** | **Workshop design** | **Workshop conduction** |
|---|---|---|---|
| **Opportunities for improvement** | - The proof-of concept SIEM could be integrated into the exercise.<br>- Integrate the connection to physical equipment, and associate physical actions to be performed on it (depend on the audience)<br>- Have all the elements that allow total transfer and permanent updating of the IAEA simulation environment<br>- Develop more activities related to the support layer (legal, human resources) depending on the audience | - The training material could be translated into the language of the participants (depend on the audience, national or international)<br>- Consider reducing the duration of the exercise (depend on the objectives)<br>- Simplify the scenario and maybe use real events (depend on the audience)<br>- Simplify the scenario and place greater emphasis on technical vulnerabilities for a more technical audience (depend on the audience)<br>- Increase the forensics analyses by collecting more evidences (depend on the audience)<br>- Increase the role of the nuclear safety authority and more broadly link with the partly underestimated safety crisis to be reinforced in the scenarios<br>- The participants could develop their own scenario and tested in the simulator (depend on the audience) | - Better explain the different tools, such Wireshark, available to players before the exercises depending on the audience<br>- Include assets, security, interactions with operational processes as the central part and have less activities on cyber (depend on the audience)<br>- More interactions between players and the fictional external<br>- Include more technical explanations related to the questions raised by the scenario (depend on the audience) |

As a result of the workshop, the host, CoE, and the French organizations that attended the event are developing a specification that could be used to adapt the simulation environment for their needs. This includes potential uses of the simulation environment such as: for training, self-training, warm-up, conducting exercises; to address functions involved or not in cyber event management; for awareness at organizational level, corporate and State level; to bringing together all the cyber nuclear event actors, including operators, regulators, original equipment manufacturer, authorities etc. The simulation environment is an opportunity to reinforce the role of computer security in nuclear safety.

## 5. CONCLUSION

This pilot workshop exceeded the expectations of the participants in terms of quality of its content and use of IAEA simulation environment. It increased the international cooperation as it was designed and organized by the IAEA and subject matter experts from different IAEA Member States, and delivered for the European countries. In addition, key experts from different Member States attended the workshop, which allowed for an exchange of information in an international level and enabled the possibility of further interactions on how to use and adapt the simulation environment. In addition, participants stated that they would directly apply the lessons learned and adapt the exercise material within their facilities and organizations.

This event accomplished a significant result in teaching the participants on how to prepare and conduct a computer security exercise using a very sophisticated web-based simulation environment - the Docker/container versions of the Asherah NPP Simulator 2.0, of the Shapash Nuclear Research Institute Heating, Ventilation and Air conditioning system and of the Gula Regional Hospital radiotherapy clinic systems, integrated with packet analyser tools, a built-in email system for communication, and a configuration and attack dashboard for running the exercise. It also provided course participants with an in-depth understanding of the IAEA Nuclear Security Series guidance, and the well-developed realist scenario enhanced the participant’s experience.

The workshop also succeeds in presenting participants with enough information to tailor the training material, and the simulation environment, to meet the needs of their organizations. The overall feedback from trainees, considering a very heterogenous audience with safety, security and cyber professionals, was outstanding. The opportunities of improvement have been taken into considerations for the next workshop event, which will be also designed and developed through international cooperation, is planned for 2025.

## REFERENCES

[1] R. Busquim e Silva, et all. *Cyber Guardian Exercise 4.0 for Protection of Critical Infrastructures and International Cooperation on Cybersecurity*. IAEA International Conference on Computer Security in the Nuclear World: Security for Safety, IAEA, Vienna (2023).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Incident Response Planning at Nuclear Facilities, Non-serial Publications, IAEA, Vienna (2016).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Approaches to reduce Cyber Risks in the Nuclear Supply Chain, IAEA Vienna (2022).

[7] Wireshark, The world's most Popular Network Protocol Analyzer. https://www.wireshark.org/, accessed on 28 April 2024.

[8] Suricata Network IDS, IPS and Network Security Monitoring Engine. https://suricata.io/, accessed on 28 April 2024.

[9] Arkime, Network Analysis & Packet Capture. https://arkime.com/, accessed on 28 April 2024.