THE ASHERAH NUCLEAR POWER PLANT SIMULATOR (ANS) AS A TRAINING TOOL AT THE BRAZILIAN CYBER GUARDIAN EXERCISE

R. A. BUSQUIM E SILVA
Polytechnic School of University of Sao Paulo - Sao Paulo, Brazil
Navy Technological Center in Sao Paulo - Sao Paulo, Brazil
Email: busquim@alum.mit.edu

D. A. CORREA
Navy Technological Center in Sao Paulo - Sao Paulo, Brazil

F. R. ANTUNES
Navy Technological Center in Sao Paulo - Sao Paulo, Brazil

F. C. S. SOUZA
Navy Technological Center in Sao Paulo - Sao Paulo, Brazil

J. R. C. PIQUEIRA
Polytechnic School of University of Sao Paulo - Sao Paulo, Brazil

R. P. MARQUES
Polytechnic School of University of Sao Paulo - Sao Paulo, Brazil

Abstract

The Brazilian Government coordinated more than 40 private and public organizations from 5 critical sectors under the second edition of the Cyber Guardian Exercise (EGC 2.0) in Brasilia, Brazil´s capital, in July 2-4, 2019. Besides more than 200 Brazilian participants, about 10 international invited observers followed the EGC 2.0. The International Atomic Energy Agency (IAEA) sent an observer to attend the exercise. The nuclear sector scheme included a fictitious country, Topazio, with a nuclear research reactor, commercial fuel facilities and a nuclear power plant (NPP) named Asherah. Moreover, a hacker group named "Incognitos" and two nearby countries completed the drill outline. The EGC 2.0 comprised three schooling activities: tabletop exercises; study group activities; and computer security simulated/hands on exercises.

Under the IAEA Coordinated Research Project (CRP) J02008, the University of Sao Paulo (USP) research team developed the Asherah NPP simulator (ANS) suitable for digital instrumentation and control (I&C) research, cyber security assessment and computer security measures development. The NPP model is based on a pressurized water reactor (PWR) implemented using Matlab/Simulink. The ANS simulates nuclear processes and controller's system dynamics and it is the heart of a comprehensive hardware-in-the-loop (HIL) simulation environment.

The ANS was used for the first time as a training tool during EGC 2.0. The ANS was also employed later in 2019, during the International Training Course (ITC) on Protecting Computer-based Systems in Nuclear Security Regime (Daejeon, Republic of Korea, in November 4-15, 2019). The ECG 2.0 ANS "live-fire exercise" (LFX) scenarios main outcome was bridging the gap between operators-human and interface-computer experts by taking advantages of the ANS advanced operational technology (OT) and information and technology (IT) capabilities.

1. INTRODUCTION

Brazil performed a cyber defence exercise from 3 to 6, July 2018 in Brasília, Brazil´s capital: the first Cyber Guardian Exercise (EGC – Exercício Guardião Cibernético). That exercise brought together 23 organizations from the public and private sectors in the first national drill towards increasing performance and stability of cyber security of Brazilian critical infrastructure [1]. The University of Sao Paulo (USP) participants of the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) "Enhancing Computer Security Incident Response at Nuclear Facilities" (J02008) planned the EGC nuclear cyber attackers' scenarios.

In 2019, for three days (from 2-4 of July, 2019 in Brasilia), the Brazilian Government coordinated more than 40 private and public organizations from 5 critical sectors under the EGC 2.0 – the second edition of the Cyber Guardian Exercise. Besides Brazilian participants, about 10 international observers followed the event - the IAEA also sent an observer to attend the exercise.

The EGC 2.0´s planning took ten months: the initial planning meeting occurred in October 2018 and the final coordination workshop in May 2019. That exercise consisted of three schooling type activities: simulated/hands on exercises; study group activities and table top exercises. These tasks were designed to train participants from the nuclear, finance, electric, telecommunication and defence sectors.

The EGC 2.0 nuclear sector adopted a fictitious country, Topazio, with a nuclear research reactor, a nuclear power plant, Asherah, and commercial fuel enrichment and fabrication facilities; two nearby countries and a hacker group, named Incognitos, for its scenarios. Also, a special test bed for the computer simulations/hands on exercise using the Asherah Nuclear Power Plant Simulator (ANS), the Request Tracker ticket-tracking tool to coordinate the response and manage requests among the groups, and the Malware Information Sharing Platform (MISP) for threat sharing was part of the nuclear sector EGC 2.0 setup. The table top exercises used a dedicated network infrastructure for all sectors.

The USP IAEA CRP J02008 team prepared and ran 4 nuclear cyber-attack scenarios. The ANS was the nuclear exercise main training tool. The ANS has been developed by the USP for digital instrumentation and control (I&C) research and as a hands-on cyber security training tool. The set up needed for any training consist of the ANS, the Control Room HMI (for the operator to interface with the ANS model) and PLCs used for hardware-in-the-loop (HIL) purposes. This setup is easy to deploy automatically employing virtual machines. The USP research team presented the ANS capabilities as a training tool during the EGC 2.0. In addition, three cyber-attack hardware-based scenarios were performed for the nuclear community to point it out the ANS training capabilities.

The ANS test bed LFX scenarios comprised technical questions and realistic situations throughout a logical flow of events that showed how impacting, quick-scalable and silence can be a cyber-attack. The realism of the exercise was based on the attacker's goal towards successful nuclear reactor sabotage. During the exercises, besides verifying the process and network ANS baseline using network sniffer and engineering codes, the participants analysed network packets and process behaviour looking for anomalies. They also performed detection, applied mitigation measures, forensics and suggested technical and administrative controls.

Practical cyber security exercises are an effective procedure to teach the specificities of OT and IT security. The purpose of the second edition of EGC 2.0 was to support and improve the prevention, detection and response to cyber security incidents involving Brazil´s critical infrastructure.

2. ASHERAH NUCLEAR POWER SIMULATOR (ANS)

Under IAEA CRP J02008, the USP research team developed a nuclear power plant (NPP) simulator suitable for digital research, cyber security assessment and computer security measures development. The NPP model is based on a pressurized water reactor (PWR) implemented using Matlab/Simulink. The Matlab/Simulink model, ANS, simulates nuclear processes and controller's system dynamics. The ANS is the heart of a comprehensive HIL simulation environment, the ANS Test Bed (ATB). The ATB has advanced operational technology (OT) and information and technology (IT) capabilities.

This simulator was designed based on a 2,772 MWt PWR Babcock & Wilcox (B&W) core [2]-[5]. The ANS integration capabilities include network connection by means of the open communication protocol Modbus and of the open cross-platform machine-to-machine OPC Unified Architecture (OPC-UA) protocol. Two USP developed Simulink interfaces allow the replacement of simulated subsystems by their real counterparts. The reactor power controller and the pressurizer pressure controller ran in a programmable logic controller (PLC) S7-1200.

The EGC 2.0 ATB HIL setup included four virtual machines (VM) and three subnets within the ATB training scenario:

- MS Windows 7 running the ANS;
- Linux Appliance running the IPFire firewall;
- CentOS Linux running a Network Time Protocol server (NTP);
- MS Windows 7 running the ScadaBR [6]; and
- Linux Ubuntu running a configuration and attack terminal (CAT).

The capture of data and cyber-attack injections at the ANS test bed were network-based. The CAT centralized the cyber-attack injections and was responsible for data collection.

ANS is a very adequate tool for cyber security training. By designing a first-of-a-kind NPP simulator that allows exchange of hardware and software and the capture of process and network data, we are extending the ability of engineers to incorporate their operational knowledge on cyber security.

3. EGC 2.0 NUCLEAR SECTOR ACTIVITIES

EGC 2.0 nuclear energy sector activities included:
- table top exercises;
- study group activities; and
- computer security simulated/hands on exercises.

The number of participants from the nuclear sector was limited to 25 by the EGC 2.0 coordination team. However, a total of 28 professionals from the following organizations attended the exercise:
- Eletrobras Eletronuclear (ETN): the company that is the sole Brazilian operator;
- Indústrias Nucleares do Brasil (INB): the company responsible for mining, uranium enrichment and fuel fabrication in Brazil;
- Brazil National Nuclear Energy Commission (CNEN);
- Nuclear and Energy Research Institute (IPEN); and
- Brazilian Navy.

Each organization sent professionals with knowledge in the nuclear sector, like operators, engineers, regulators, IT-personal, lawyers and media communication. They gave different views and perspectives to the work process. The computer security simulated group, the study group and the table top exercises were located in the same room.

3.1 Table top exercise

The table top discussion-based exercise led the participants throughout the process of testing the organizations emergency plan and dealing with simulated situations. This exercise took place in three separated tables within the same room. Each table discussed how to handle different emergency situations related to computer security emergency response. Three facilitators, one for each table, guided participants through a discussion of the scenario attacks on web sites, sensitive information data breach, data breach on transportation of nuclear material, nuclear power plant operator's data breach. The nuclear sector table top exercises considered 22 scenarios over two days. The scenarios considered IT, OT and PPS networks.

The table top exercise used Request Tracker, a ticket-tracking tool to coordinate the response and manage requests among the groups, and the Malware Information Sharing Platform (MISP) for threat sharing.

3.2 Study group

The work group activities involved one professional from each of the invited organizations working collaboratively on one subject matter. The topic of discussion, decided over four previous meetings, was "Establishing a roadmap for implementing a nuclear computer security regulatory framework in Brazil". The group reported their findings and recommendations to the Presidency Institutional Cabinet.

3.3 Computer security simulated exercises

EGC 2.0 simulated exercises employed a dedicated ATB HIL setup as presented in Figure 1. The capture of data and cyber-attack injections at the ANS test bed were network-based and performed using the CAT. A group of five instructors ran the scenarios. At the end of each scenario, the computer security impact, the facility & function impact, forensics and mitigation measures were presented to all participants.

Previously to the three HIL simulated scenarios, the participants performed an open source information recovery exercise based on websites associated to the the Shapash Nuclear Research Institute (SNRI). This intelligence gathering exercise help improving the integration among participants towards a better performance.

Figure 2 presents the ANS types of simulations and their correspondent infrastructure and Figure 3 summarizes the EGC 2.0 cyber-attack scenarios.

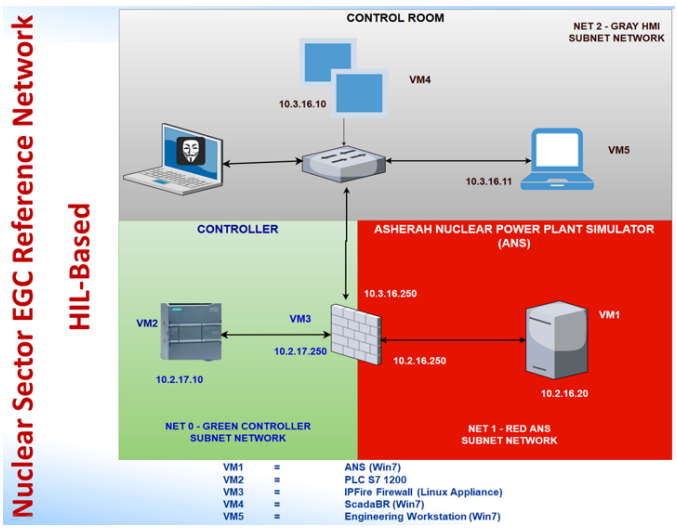

Figure 1. EGC 2.0 Dedicated network

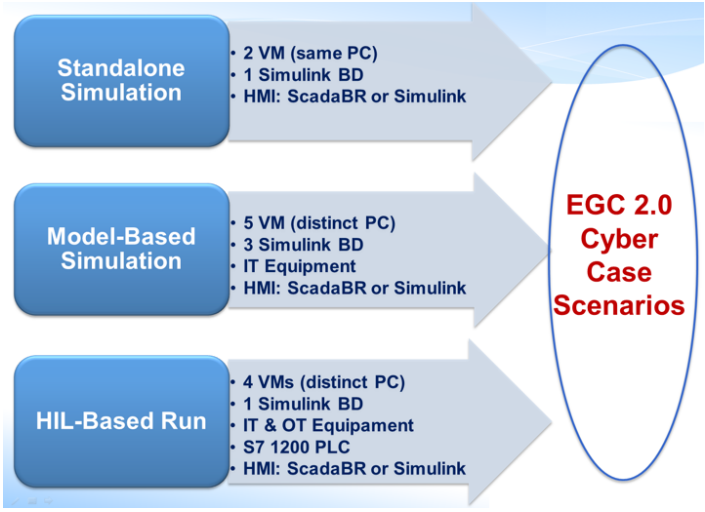

Figure 2. EGC 2.0 Simulations

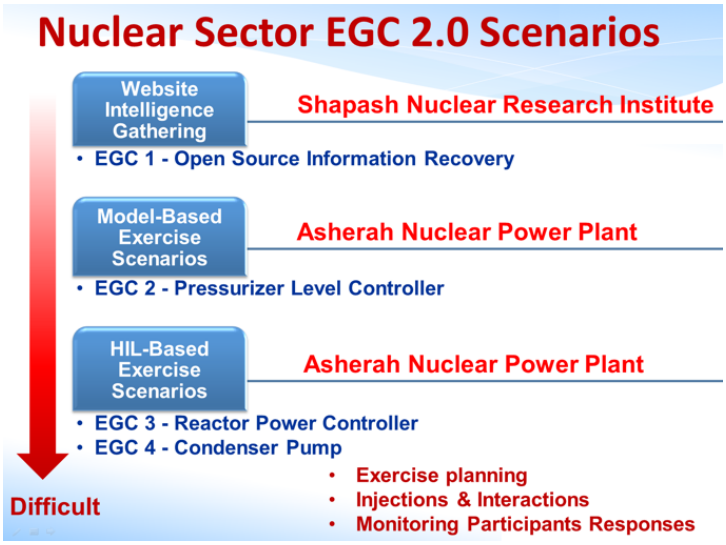

Figure 3. EGC 2.0 scenario summary

3.4 Computer security simulated exercises

The first cyber-attack scenario was model-based, i.e. the Asherah processes (and all controllers but one being attacked) ran in one virtual machine (VM) and the Asherah pressurizer level controller (security level 3 attack) ran in another one – both connected by IT equipment.

The scenario´s narrative started with the hacker group "Incognitos" using Open-Source Intelligence to identify a potential insider with authorized access, facility knowledge and some level of motivation (money). An active disgruntled employee is identified: Jane Doe. She is willing to provide information and perform actions for "Incognitos" as she has a reduced organization loyalty. During months, the insider threat sold IT/OT network information to hacker group. Using that information, "Incognitos" prepared a malware to use against the facility and wait for the right opportunity to infiltrate.

After a while, Asherah NPP bought a workstation from a well-known vendor (commercial off the shelf) to replace an engineering workstation (EW) at the human-machine-interface (HMI) control room (CR). During the EW final set up, Jane Doe uses a flash drive to execute a script that sends continuous OPC UA messages to the CR HMI. The OPC UA messages change the pressurizer level to a undesired value. By flooding the HMI with heavy traffic, the attack overwhelms the operator's resources and make it impossible to access the level set point. Then, the pressurizer level controller is compromised and the facility impact is assessed.

3.5 HIL-based Scenario: Asherah Reactor Power Controller

The second cyber-attack scenario was a HIL-based scenario: i.e. the Asherah processes (and all controllers but one being attacked) ran in one virtual machine (VM) and the Asherah reactor power controller (security level 2 and 3 attack) ran in a S7 1200 Programmable Logic Controller (PLC) – all connected by IT equipment.

The scenario´s narrative started with the hacker group "Incognitos" using Open-Source Intelligence to identify a potential insider. After the identification, social engineering (spear phishing) allows Incognitos to gain access to a third-party maintenance laptop (Unknowing Accomplice): John Doe. Next, "Incognitos" installs a malware at John Doe´s maintenance laptop that scans for Siemens data/software on computers related to OT equipment and copy them - this was done using EthernalBlue SMB exploit.

Next, during a non-scheduled maintenance activity, John Doe, who has been authorized to do maintenance at the CR for more than 10 years, access the CR network for maintenance.

The malware copies S7 1200 web server configuration backup files and OT network architecture to John´s Doe laptop. When John Doe´s maintenance laptop is connected, at his company, to the Internet, the malware sends data captured to a remote server. Using Totally Integrated Automation Portal (TIA), and the captured data, a new S7 1200 configuration file, that "stuck" the control rods in a certain position ("all rods out"), is prepared by Incognitos.

During next CR schedule maintenance, a SL 2 remote maintenance access (from SL 3) is allowed on a case-by-case access and for a short defined working period. Then, the new PLC S7 1200 configuration file is uploaded causing the PLC to restart. The Reactor Power Controller is then compromised and the facility impact is assessed.

3.6 HIL-based Scenario: Asherah Condenser Pump Controller

The third cyber-attack scenario was a HIL-based scenario: i.e. the Asherah processes (and all controllers but one being attacked) ran in virtual machine (VM) and the Asherah condenser cooling pump controller (security level 3 attack) ran in a S7 1200 PLC - all connected by IT equipment.

The scenario´s narrative started with an infected USB stick being used for data exchange between SL3-4 and the SL 3-4 kiosk antivirus engines being not up to date. The Asherah computer security policy allows access to Internet from SL 4 and remote maintenance access if the remote computer and user respect a defined security policy, contractually specified and controlled. In addition, a dedicated condenser pump controller (PLC 1200 and its HMI – tertiary loop) is wrong located in a SL3 zone.

Then, a malware that allows access throughout remote desktop was installed in one of the engineering workstations at SL3. Due to bad firewall rules, a network path allowed a remote desktop connection between SL3-4. Also, bad security gateway implemented do not protect from uncontrolled traffic from external site

network. Then, the hacker group “Incognitos” use scan/sniffer in the network and captured information to perform a man-in-the-middle type attack. The OPC communication is compromised and the condenser pump is turned off. The CR HMI does not present that information. The facility impact is assessed.

4. EGC 2.0 PARTICIPANTS EVALUATION SUMMARY

After the end of the exercise, 22 of the 28 participants filled an evaluation form. For all questions, the rating value varies from 1 to 5. The tables below present the weighted average for each question.

4.1 Computer security simulated exercise evaluation

The evaluation sheet for the computer security exercises comprised three questions. Each participant used a five-point scale to rate each one of them (1 - Poor, 2 - Fair, 3 - Good, 4 - Excellent, 5 - Exceptional). The questions and the averaged rate are shown in Table 1:

TABLE 1 – COMPUTER SECURITY SIMULATED EXERCISES EVALUATION

Question	Description	Rate
1	How clear are the nuclear sector scenarios statement and their presentation?	4.6
2	How were the participant’s engagements and the scenarios relevance for the nuclear sector?	4.7
3	How were the scenarios difficult and complexity based on the participant knowledge on computer and nuclear field?	3.5

Question 2 was detailed per scenario. The engagement and relevance for each scenario, in a 1 to 5 scale, were: EGC 2 = 4.7, EGC 3= 5.0 and EGC 4 = 4.8. It can be seen that all the scenarios were considered very significant and that their relevance does not depend on their complexity.

Question 3 was also detailed per scenario. The level of complexity and difficult for each scenario were EGC 2 = 3.3; EGC = 3.7 and EGC = 4.2. As expected, the level of difficult increases with scenario complexity.

4.2 Study group evaluation

The evaluation sheet for the study group comprised five statements. Each participant used a five-point scale to rate each statement (1 - Strongly Disagree, 2 – Disagree, 3 – Unsure, 4 - Agree, 5 - Strongly Agree). The statements and the averaged rate are shown in Table 2:

TABLE 2 – STUDY GROUP EVALUATION

Statement	Description	Rate
1	The subject under study was clear and well defined	4.8
2	The goals and objectives were measurable, achievable, realistic and timely.	4.4
3	The study group format was appropriate for reaching the stated goals and objectives.	4.8
4	The study group had positive group dynamics and positive interactions between team members.	5.0
5	The study group produced the intended outcomes	4.4

4.3 Table top exercise evaluation

The evaluation sheet for the table top exercise comprised four statements. Each participant used a five-point scale to rate each statement (1 = Strongly Disagree, 2 = Disagree, 3 = Unsure, 4 = Agree, 5 = Strongly Agree). The statements and the averaged rate are shown in Table 3:

TABLE 3 – TABLE TOP EXERCISE EVALUATION

Statement	Description	Rate Day 1	Rate Day 2
1	The table top scenarios were measurable, achievable, realistic and timely.	3.8	4.1
2	The table top scenarios were appropriate for reaching the exercise goals.	3.9	3.9
3	The table top participants had positive interactions among members.	3.7	3.8
4	The table top scenarios produced the intended outcomes.	4.2	4.3

5. CONCLUSION

EGC 2.0 increased the sharing of computer security knowledge, experiences and information in a national level by gathering five infrastructure main sectors under the same cyber security drill. From the Brazilian nuclear sector point of view, the interaction between multidisciplinary teams participating in the exercise gave useful insight about their different shortcomings. Although the planning period was relatively short, the EGC 2.0 was built over the 2018 exercise: by starting with a small exercise and adding difficulties over time, knowledge and experience from EGC 1.0 led to the EGC 2.0 planning and conducting success. Cooperation and coordination were the key words for the planning and for the exercise.

The ANS reference test bed (under development by USP - under the IAEA CRP “Enhancing Computer Security Incident Response at Nuclear Facilities”) allowed the deployment of realistic scenarios/incidents using a fictitious PWR. It also included the participation of a wide range of professionals with experience in the nuclear sector like operators, engineers, regulators, IT-personal, lawyers and media communication professionals imparting different views and perspectives in the work process. The use of the ANS allowed the assessment of the computer security impact, the facility & function impact, forensics and mitigation measures.

6. ACKNOWLEDGEMENTS

This work was supported by the São Paulo State Research Foundation (FAPESP) through Grant 2016/04600-0 and IAEA, through Research Contract No. 22527 (CRP J02008).

REFERENCES

[1] https://dialogo-americas.com/en/articles/brazilian-army-conducts-unprecedented-cyberdefense-exercise. Accessed on May 1st, 2019.

[2] U.S. Nuclear Regulatory Commission (NRC). Backgrounder on the Three Mile Island Accident. www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html. Accessed on September 16, 2017.

[3] K.N. Ivanov et al. Pressurized Water Reactor Main Steam Line Break (MSLB) Benchmark. Volume I: Final Specifications. Organization for Economic Co-Operation and Development (OECD), Nuclear Energy Agency (NEA) (1999).

[4] Busquim e Silva, R.A., “Implications of advanced computational methods for reactivity-initiated accidents in nuclear reactors”, University of Sao Paulo, PhD Thesis, 2015.

[5] Busquim e Silva, R.; Marques, A.L.F.; Cruz, J.J.; Marques, R.P.; Piqueira, J.R.C. Use of State Estimation Methods for Instrumentation and Control Cyber Security Assessment in Nuclear Facilities. International Conference on Nuclear Security: Commitments and Actions, Vienna – Austria, 2016.

[6] http://www.scadabr.com.br/ Accessed on May 10, 2019.