2021 International Nuclear Atlantic Conference – INAC 2021
Virtual meeting, Brazil, November 29 – December 2, 2021

ISBN: 978-65-594-1256-3

Computer Security on Brazilian Nuclear Facilities: challenges, actions and the path forward

Tavares, R.L.A.[1], Lemos, F. L.[2], Silva, A. T.[3]

[1] *renato.tavares@cnen.gov.br, Comissão Nacional de Energia Nuclear, Rio de Janeiro/RJ, Brazil*
[2] *fllemos@ipen.br, Instituto de Pesquisas Energéticas e Nucleares, São Paulo/SP, Brazil*
[3]*teixeira@ipen.br, Instituto de Pesquisas Energéticas e Nucleares, São Paulo/SP, Brazil*

1. Introduction

Computers and other digital systems are increasingly becoming omnipresent on several functions and aspects of critical infrastructure such as nuclear energy generation and its associated fuel cycle [1]. Along with the increase on the dependency of information technology (IT) and operational technology (OT) assets to proper and safe operation of nuclear facilities, it becomes more and more important to provide security to digital assets in order to ensure reliability and safety of nuclear operations.

On the past, when most of the critical systems on nuclear facilities, such as safety-related functions, instrumentation, process control and physical protection were implemented using analog devices, the greatest security risk posed to nuclear facilities was purely physical, i.e., theft and sabotage of nuclear materials performed by threats with purely physical capabilities such as weapons, vehicles, tools and explosives[2]. Since mid-1990´s, when the international community started experiencing cyber incidents related to nuclear infrastructure (see Table I), and the 9/11 terrorist attacks on New York, more attention was given to security, particularly nuclear security, which led to publication of several international recommendations and guidance regarding different aspects of nuclear security, including computer or cyber security.

“Computer Security” or “Cyber security” in the context of this work can be understood as the prevention of computer acts that could directly or indirectly lead to unauthorized removal of nuclear or other radioactive materials, sabotage against nuclear materials and facilities or theft of nuclear sensitive information [3]. The term “computer security” is preferred throughout this work, following IAEA guidance documents.

On table I a list of some relevant known cyber incidents at nuclear facilities is shown.

Table I: List of cyber incidents at nuclear facilities. Adapted from [4].

Month/year	Facility Name/Country	Description	Category
January 1990	Bruce Nuclear Generating Station, Canada	Software error leading to release of radioactive water	Accidental
September 1991	Sellafield reprocessing plant, United Kingdom	Software bug leading to unauthorized opening of doors; widespread software errors	Accidental
February 1992	Ignalina Nuclear Power Plant, Lithuania	Employee attempted sabotage	Intentional
June 1999	Bradwell Nuclear Power Plant, United Kingdom	Employee altered/destroyed data	Intentional

January 2000	Kurchatov Institute, Russian Federation	Bug in nuclear materials accounting software	Accidental
January 2003	Davis-Besse Nuclear Power Station, United States	Virus blocked operator access to reactor core information	Accidental
August 2006	Browns Ferry Nuclear Power Plant, United States	Technical failure	Accidental
March 2008	Edwin Hatch Nuclear Power Plant, United States	Shutdown caused by software update	Accidental
June 2010	Natanz Nuclear Facility, Iran	Stuxnet virus used to destroy enrichment ultracentrifuges	Intentional
December 2014	Korea Hydro and Nuclear Power Company, South Korea	Data theft and release	Intentional
April 2016	Gundremmingen Nuclear Power Plant, Germany	Two viruses entered plant´s fuel rod monitoring system	Unknown
February 2021	Eletrobras Eletronuclear, Brazil	Ransomware attack on corporate network	Intentional

The events listed on table I clearly demonstrate a scenario of increased threat capabilities (e.g. terrorism and organized crime, nation States) with the potential to reach nuclear materials and facilities across the world [5] which, combined the increasingly widespread use of digital devices in every industrial step on nuclear facilities' processes [6], makes imperative for States to have means to ensure availability, integrity and confidentiality of information for computer based systems that are used to process, transmit and store sensitive information in digital form, aiming to meet the primary objective of nuclear safety, which is the protection of individuals (whether occupationally exposed or the public) and the environment against the risks arising from the misuse of ionizing radiation [7]. It´s noticeable an increasing number of intentional malicious cyber acts involving nuclear infrastructure, which demonstrates that threats are evolving in terms of cyber capabilities.

Amid this context, this paper aims to outline computer security concepts, the current situation of Brazilian nuclear program in terms of legislation, regulations and propose future actions for protecting national nuclear critical digital assets.

2. Methodology

This work initiated with a bibliographic study phase, in which papers, journals, dissertations, theses, laws, regulations and international recommendations were examined in order to outline an updated overview of the implementation of computer security actions on Brazilian Nuclear Program.

Based on the information gathered on the bibliographic study, and following 2020 NTI´s Nuclear Security Index recommendations approach [8], the result of this work is a list of proposals regarding actions and measures to fulfill NTI´s recommendations to strengthen computer security on the national nuclear program, divided on the following topics:

- Require nuclear facilities to have protection from a cyber-attack;
- Require nuclear facilities to protect sensitive digital assets that impact safety, security, emergency preparedness functions, and their support systems from cyber-attack;
- Consider cyber threats in the national threat assessment or Design Basis Threat;
- Require nuclear facilities to perform tests and assessments of cybersecurity;

- Require nuclear facilities to have a cyber-incident response plan in place to respond to cyber-attacks;
- Require licensees or operators to have a cybersecurity awareness program that reaches all personnel with access to digital systems.

Other topics have also been considered in the study:

- Internet of Things (IoT) devices in nuclear facilities environment and associated risks;
- “Bring your own device” policies and other types of controlling access of external hardware;
- Supply chain attack risks;
- Security culture and, more specifically, computer security culture and how to assess them.

3. Results and Discussion

Despite the recent publication of several legal instruments that, in theory, enforce implementation of computer security actions on Brazilian nuclear facilities, the results of the study indicate some important gaps on the governance structure, regulatory instruments, oversight, preparedness and response to cyber-attacks that shall be taken in consideration and dealt seriously by competent authorities, such as:

- Lack of a specific computer security regulation to nuclear sector;
- Lack of regulatory oversight in terms of assessment and inspections;
- Lack of a national threat assessment (or design basis threat) that consider cyber capabilities;
- Lack of contingency plans with formal assignment of responsibilities and chain of communications, notifications and actions in case of cyber incidents.

4. Conclusions

The nuclear industry currently faces a complex and dynamic threat scenario, in which terrorists and criminals with cyber capabilities are improving means to take control of critical systems and perform malicious acts with potential catastrophic consequences and little or no probability of a timely detection. On the other hand, authorities with competence on the security of nuclear materials and facilities need to fill several gaps in terms of regulations, oversight and response in order to assure a proper security framework to deal with that scenario. On this effort, this paper provided an updated overview of computer security actions on the Brazilian Nuclear Program, which led to the proposal of actions intended to strengthen computer security on the sector.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY. ***Computer Security at Nuclear Facilities***. Vienna (2012). Available on: < https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf>.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY. ***Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Facilities***. Vienna (2011). Available on: < https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf>.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY. ***Computer Security for Nuclear Security***. Vienna (2021). Available on:< https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf>.

[4] NUCLEAR THREAT INITIATIVE. ***References for Cyber Incidents at Nuclear Facilities***. Available on: <https://www.nti.org/analysis/tools/table/133/>.

[5] BUNN, M., ROTH, N., TOBEY, W. ***Combating Complacency about Nuclear Terrorism***. Cambridge, MA: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019. Available on: <https://scholar.harvard.edu/files/matthew_bunn/files/bunn_nuclearsecuritypolicybrief_2 _2019.pdf>.

[6] WORLD INSTITUTE FOR NUCLEAR SECURITY. ***Effectively Integrating Physical and Cyber Security***. Ver. 1.1. Vienna, Austria: WINS Best Practice Guide, 2015. Available on: <https://wins.org/document/4-11-effectively-integrating-physical-and-cyber-security/>.

[7] COMISSÃO NACIONAL DE ENERGIA ***NUCLEAR. Glossário do Setor Nuclear e Radiológico Brasileiro***. 2.ed. Rio de Janeiro, 2020. Available on: <http://appasp.cnen.gov.br/seguranca/normas/pdf/glossario.pdf>.

[8] NUCLEAR THREAT INITIATIVE. ***The NTI Index for Brazil***. Available on: <https://www.ntiindex.org/country/brazil/>.