2019 International Nuclear Atlantic Conference - INAC 2019
Santos, SP, Brazil, October 21-25, 2019
ASSOCIAÇÃO BRASILEIRA DE ENERGIA NUCLEAR - ABEN
ISBN: 978-85-99141-08-3

METHODOLOGY PROPOSAL FOR ASSESSING SAFETY IN WSN AND IOT DEVICES IN NUCLEAR RESEARCH LABORATORY

Marcia M. Savoine[1,2], Delvonei A. Andrade[2] and Mario O. de Menezes[2]

[1]Tocantinense University Center President Antonio Carlos (UNITPAC)
Av. Filadélfia, 568 Setor Oeste
77.816-540 Araguaína, TO, Brazil
savoine@usp.br

[2]Nuclear and Energy Research Institute (IPEN/CNEN)
Av. Professor Lineu Prestes 2242
05508-000 São Paulo, SP
{delvonei,mario}@ipen.br

ABSTRACT

Nowadays there is a gap due to the absence of an updated and formalized methodology that can be used to assess security levels in WSNs (Wireless Sensor Network) under IoT (Internet of Things) devices in nuclear environments (which are considered hostile environments and require a higher level of security). This gap causes information security professionals to have difficulties in making a broad assessment of the vulnerabilities in their WSNs, with greater concern when coupled with IoT devices. This work aims to present a methodology to evaluate the reliability of the use of levels security with IoT devices for nuclear installations using WSNs. The proposal of the methodology consists of 5 main stages and 21 substages, which are part of the category of a function in groups of cyber security results that are linked to programmatic needs and specific activities of mandatory execution. Understanding so that the security of a WSN considering the current IoT context for nuclear installations is necessary, where important characteristics in these critical environments should be explored (e g., the presence of radioactivity, in addition to the decontamination of materials and equipment, determine access to authorized persons). The application of the defense-in-depth concept of anomaly solution management and prevention against atypical events to provide an effective safety mechanism, ensuring its safe use in these high criticality environments.

1. INTRODUCTION

Over the past few years, concern for safety in nuclear installations has grown considerably, and this has also led to increased standards aimed at preserving the physical integrity of these installations. The Wireless Sensor Network (WSN) has gained notoriety in various contexts of application together with new emerging technologies (e.g. Internet of Things - IoT). One of these contexts is nuclear facilities, which are environments considered critical because they require high efficiency and effectiveness to ensure their physical integrity. In these critical and hostile environments, there is a constant risk due to the presence of

radioactivity and the impact of security-related problems, as well as the need to avoid access by unauthorized users.

In this sense, WSNs associated with IoT devices can contribute to the safety management of a nuclear facility (i.e., nuclear research laboratories and reactors). These technologies are commonly connected to the same Internet access infrastructure as other devices and thus may present vulnerabilities where data may be intercepted and used illegally or inappropriately. It is, therefore important to establish appropriate levels of cybersecurity by using them when employing WSNs and IoT in such highly critical environments.

The emerging field of research and all the implications arising from the connection between the physical and digital world becomes increasingly relevant, in addition to gaining importance in the continuous advancement of information and communication technologies, especially considering their connection and integration with the Internet in various areas of applications.

Currently there is a gap due to the lack of an updated and formalized methodology that can be used to evaluate security levels in WSNs (Wireless Sensor Network) under IoT (Internet of Things) devices in nuclear environments (i.e., considered hostile environments that demand a higher level of security). This gap makes it difficult for information security professionals to perform a comprehensive vulnerability assessment on their WSNs, with greater concern when coupled with IoT devices.

The objective of this work is to present a proposal for a methodology to assess the reliability of the use of security levels with IoT devices for nuclear installations using WSNs. Following this introductory section, Section 2 defines cybersecurity in nuclear research laboratories, then, Section 3 presents the methodology proposal. Finally, Section 4, brings the final considerations.

2. CYBERSECURITY IN NUCLEAR RESEARCH LABORATORIES

Nuclear research labs are critical locations due to the magnitude of operations and, for that reason, a cyber-attack on these environments can have catastrophic and highly destructive consequences affecting their cybersecurity. For example, if a nuclear laboratory has its system invaded, its vital functions may be affected, such as temperature control, which will be compromised, spillage of radioactive material in the handling of conducted experiments, as well as changes in the storage of spent fuel from research reactors, among others.

According [1]: The protection of critical infrastructures has been a concern of governments in recent times due to the increasingly intense use of the Internet by an increasing number of users.

In this sense, cybersecurity is the term that designates the set of means and technologies that aim to protect from damage and intrusion, programs, computers, networks and data and safeguard confidentiality, integrity, and the availability of information.

Cybersecurity is a set of tools, policies, guides, risk management approaches, training, best

practices and technologies that can be used to protect the organization's assets and all users in the virtual environment. Such assets include networked devices, applications and services, telecommunications and multimedia communication systems, and information transmitted or stored in the virtual world. This protection aims to ensure the availability, integrity and confidentiality of assets in relation to cyberspace threats [2].

3. PROPOSAL METHODOLOGY FOR CYBERSECURITY ASSESSMENT

Considering all the problems that involve nuclear research laboratories, for being a critical infrastructure, the cybersecurity applied to this context should meet the following characteristics as a proposal of standard criteria, being:

- Network operation should be able to continue during any security attack or compromise (as far as possible);
- The operation of the system should recover quickly after some kind of radiological material accident or compromise of the monitored site.

In this context, the methodology was developed based on the technical standards NIST SP 800-53 Rev. 4 [3], NIST SP 800-53 Ver. 5 [4], NIST SP 800-160 Volume 1 [5], NIST Cybersecurity Framework, v1.1 [6] and ISO/IEC 27001:2013 [7], and the concept of defense in depth, in addition to the IAEA standards No. 17 [8], and IAEA Draft-Implementing Guide [9]. As shown in Fig. 1, where there are the 5 steps that make up the methodology proposed in WSN networks with IoT, being:
1º) Analyze and Recognize,
2º) Perform Protection,
3º) Develop and Execute Solutions,
4º) Perform Restoration and,
5º) Perform Continuous Improvement.

Figure 1: Complete structure that constitute the core part of the methodology.

The methodology as a whole is composed of 5 main steps and 21 sub-steps, which are part of the category of a role in groups of cybersecurity results that are linked to programmatic needs and specific activities, and which are all mandatory to be performed. Table 1 shows the complete structure of all the sub-steps that make up the main part of the methodology.

Table 1: Complete structure that constitute the core part of the methodology.

1) Analyze and Recognize - composed of 7 sub-steps:
1.1 Recognize the objective of cybersecurity in the nuclear installation;
1.2 Identify mobile devices and IoT of the wireless network;
1.3 Determine the partitioning of the nuclear facility:
  1.3.1 In two wireless access networks
  1.3.2 In safety zones
1.4 Identify and determine cybersecurity risk responsibilities;
1.5 Analyze the risk of unauthorized access and atypical activities, in case of:
  1.5.1 Nuclear disaster
  1.5.2 Cyber Invasion
1.6 Analyze risk management strategies
1.7 Identity Management, Authentication and Access Control

2) Perform Protection - composed of 3 sub-steps:
2.1 Establish identity management and access control
  2.1.1 Establish access levels to users by associating them to access zones
  2.1.2 Establish the scope of protection and determine roles and responsibilities
2.2 Establish Data Security
2.3 Establishing Protective Technology

3) Develop and Execute Solutions - composed of 5 sub-steps:
3.1 Detect Anomalies and Atypical Events
3.2 Continuous Safety Monitoring
3.3 Detection Processes
3.4 Mitigation of cybernetic anomalies and atypical radiation events
3.5 Improvements to be made

4) Perform Restoration - is composed of 4 sub-steps:
4.1 Restore Analysis
4.2 Restoration Planning
4.3 Improvements to be made
4.4 Communication

5) Effective Continuous Improvement - composed of 2 sub-steps:
5.1 Collect suggestions for improvements to the processes
  5.1.1 Information is stored and disclosed
5.2 Conduct action plan
  5.2.1 Analyze how changes are made to processes and introduce them.

3.1. Complete Structure of the Methodology

The five main steps of the structure shown in Fig. 1 are intended to form a sequential logical path to a desired final state. After the first time the five steps are executed, it is indicated that all steps and functions should be executed simultaneously and continuously to form an operational culture that addresses and mitigates dynamic cybersecurity risk.

In **"Step 1 - Analyze and Recognize":** Develop an understanding of the nuclear facility framework to manage cybersecurity risk for mobile devices (laptops, smartphones, sensors), people, assets (network routers, among others), data and resources. The activities of this stage are fundamental for the effective use of the structure. Understanding the business context, the resources that support functions and risks related to cybersecurity allow an organization to focus and prioritize its efforts according to its risk management strategy for both data security and radioactive materials. Sub-steps of results within this step include:
1.1 Recognize the objective of cybersecurity in the nuclear facility;
1.2 Identify mobile devices and IoT from the wireless network;
1.3 Determine the partitioning of the nuclear facility into:
1.3.1 Two wireless access networks: one for laboratory administrative work and the other for data security in the event of cyber intrusion;
1.3.2 Security zones: it is important to divide into five zones and assign the types of user access, as well as access levels.
1.4 Identify and determine cybersecurity risk responsibilities: based on physical location, device, and data responsibilities, identity management and access control are assigned (item 1.7).
1.5 Analyze the risk of unauthorized access and atypical activities, determining:
1.5.1 In case of nuclear catastrophe: which people are involved in th e recovery to the normal state of the site
1.5.2 In case of cyber intrusion: who is involved in data recovery and secure network reconfiguration
1.6 Analyze risk management strategies
1.7 Identity Management, Authentication and Access Control: Access to physical and logical devices, and associated resources is limited to authorized users; processes and devices and are managed in accordance with the assessed risk of unauthorized access to authorized activities and actions.

In **"Step 2 - Perform Protection":** Develop and implement appropriate safeguards to ensure the provision of critical services. It is a step to support the ability to limit or contain the impact of a potential anomalous cybersecurity event. The sub-steps of results within this step include:
2.1 Establish Identity Management and Access Control: Access to physical and logical devices as well as associated resources is limited to authorized users and processes. Also, it is managed in accordance with the assessed risk of unauthorized access to authorized activities and actions.
2.1.1 Establish levels of access to users by associating them to access zones
2.1.2 Establish the purpose of protection and determine roles and responsibilities
2.2 Establish Data Security: perform in a manner that is consistent with the risk strategy of the organization to protect the confidentiality, integrity and availability of information.

2.3 Establish Protective Technology: technical safety solutions are managed to ensure the safety and resilience in a manner consistent with policies, procedures and agreements related to nuclear facilities. (jackets, badges, access turnstiles, etc...)

In **"Step 3 - Develop and Execute Solutions:"** Develop and execute appropriate activities to identify the occurrence of an anomalous cyber security event. Also, develop and execute appropriate activities to act in relation to a detected cyber security incident or a detected radiation accident. This step must support the ability to contain the impact of a potential cyber security incident or radiation. The sub-steps of results within this step include:
3.1) Detect anomalies and atypical events: anomalous cybersecurity activity and atypical events are detected in a timely manner and the potential impact of the activity and events is understood. Data for anomalous events and activities are collected and correlated from various sources and sensors, and incident alert thresholds are established.
3.2) Continuous security monitoring: network, mobile devices and radiation events are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
3.3) Detection processes: detection processes and procedures are maintained and tested to ensure awareness of anomalous and atypical radiation events.
3.4) Mitigation of cyber anomalies and atypical radiation events: activities are performed to prevent the expansion of an event, mitigate its effects and resolve the incident of both the cyber anomaly and the atypical radiation event.
3.5) Improvements to be pointed out: Organizational response activities are improved so that lessons learned from current and past detection and response activities are incorporated.

In **"Step 4 - Perform Restoration":** develop and implement appropriate activities to maintain plans for resilience and restoration of any resources or services that have been damaged due to a cyber security incident or radiation accidents. This step supports timely recovery from normal operations to reduce the impact of a cybersecurity incident. The sub-steps of results within this step include:
4.1) Analysis: Analysis is conducted to ensure response to and support of recovery activities.
4.2) Recovery Planning: recovery processes and procedures are performed and maintained to ensure restoration of devices affected by cyber security events or radioactive material handling sites. - The recovery plan is executed during or after a cybersecurity incident.
4.3) Improvements to be pointed out: the planning and restoration processes are improved by incorporating lessons learned in future activities. Recovery plans should incorporate lessons learned and recovery strategies are updated.
4.4) Communication: restoration activities are communicated to internal and external stakeholders, as well as to management and operational teams.

In **"Step 5 - Effective Continuous Improvement":** analyze, develop and execute improvement in nuclear facility processes related to wireless network access, data monitoring. The functioning of the laboratory should be analyzed and rethought, investigating anomalies, inconsistencies, inefficiencies and opportunities for improvement. The sub-steps of

results within this step include:
5.1 Collected suggestions for process improvements
5.1.1 Information is stored and disclosed
5.2 Conduct an action plan: an action plan is defined and must be conducted to correct each non-conformity (anomaly found, atypical event found or performed).
5.2.1 Analyze how changes are made to processes and introduce them.

The sequential interconnection of the steps and sub-steps of the methodology is shown in Fig. 2, in a functional diagram.

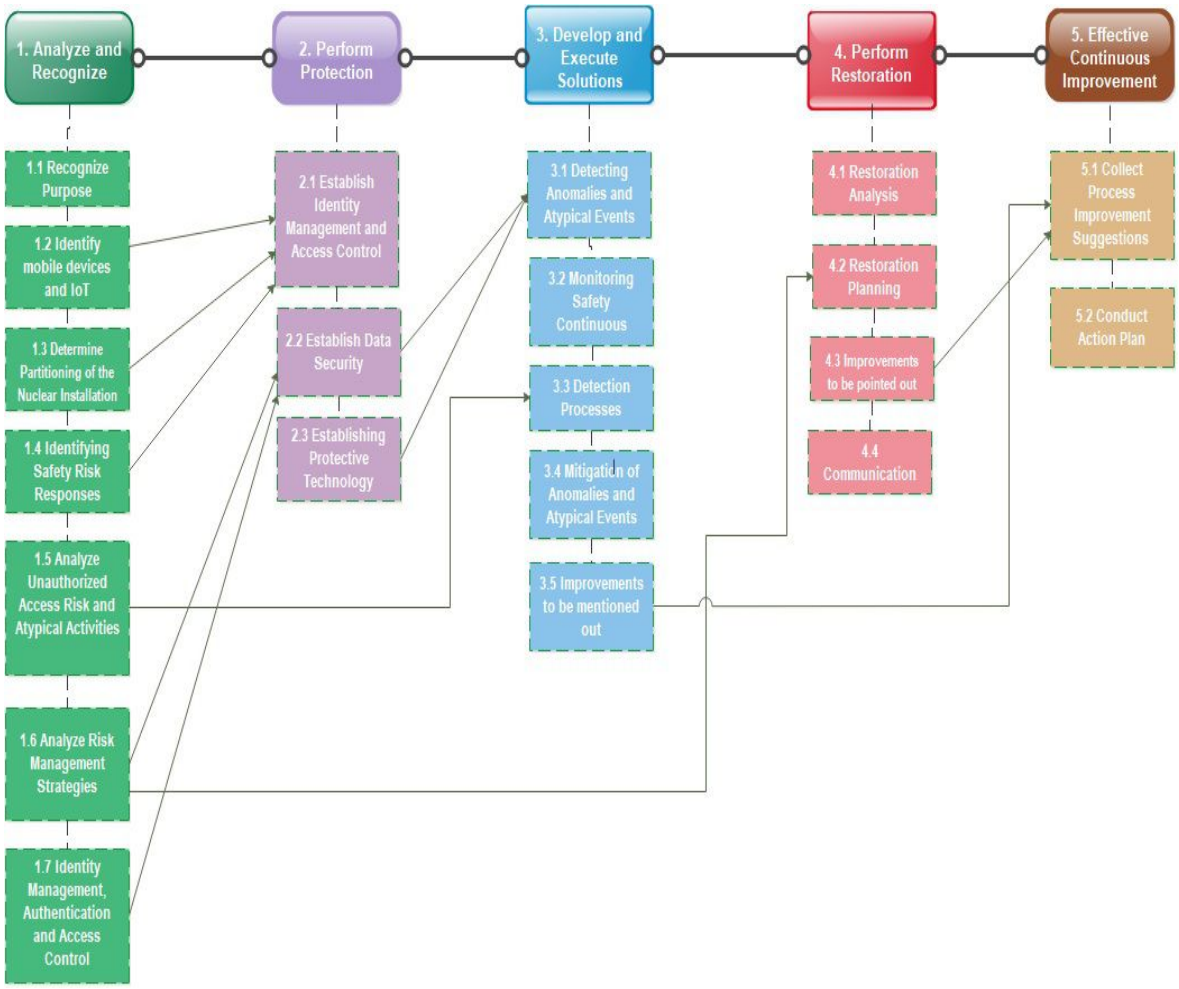

Figure 2: Functional diagram of the interconnections of the stages and sub-steps of the methodology.

It is important to remark that the **"Access Management Level"** should be created and widely applied across the wireless network of a nuclear lab or research reactor that will manage the WSN and IoT devices. Where the five levels for wireless network access are defined as: Level 1 - Extremely Criticality, Level 2 - High Criticality, Level 3 - Medium Criticality, Level 4 - Low Criticality, and Level 5 - Very Low Criticality, as shown in Fig. 3.

After the conclusion of In **"Stage 1"** and already in In **"Stage 2 - Perform Protection"** and when the five levels of access are implemented, it is already indicated that

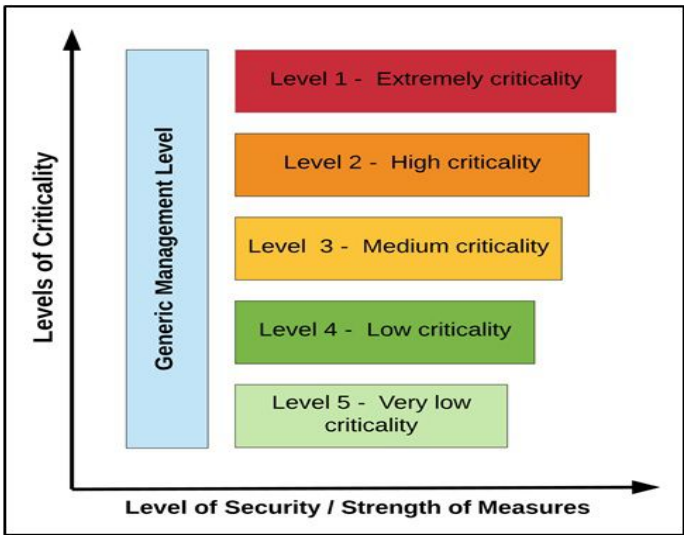

Figure 3: Structure of the security levels. [10] Adapted.

users (i.e., researchers, laboratory technicians and student-researchers) and WSN administrators receive access only in their specific functions of the network. The accumulation of permissions is not allowed in order to facilitate monitoring in case of anomalies or invasions found. In this sense, it is advisable that:

- Network administrators categorized into senior, intermediate and junior; being one senior administrator, two intermediate and two juniors;
- Researchers categorized as senior and intermediate, being allowed up to 2 researchers of each classification category;
- Laboratory technicians categorized as: senior, intermediate and junior, being allowed up to 2 technicians of each category;
- Students-researchers in: High (2 doctoral students), Intermediate (2 master students) and Junior (2 scientific initiation students).

In "Level 1 Extreme Criticality", in addition to including generic measures, preventive and protection measures should be used from the level for access to the network, because it requires the level of security of greater criticality. Only senior researchers have this type of access.

In "Level 2 - High Criticality", in addition to including generic measures, preventive and protective measures of the level for access to WSN should be used. So, at this level only intermediate researchers will be able to access the WSN.

And in "Level 3 - Medium Criticality", besides including generic measures, it includes preventive and protective measures to the network, only High and Intermediate students-researchers and senior laboratory technicians can have access.

In this next level considered "Level 4 - Low Criticality", generic measures are also included, as well as preventive and protective measures to the WSN access. Then, only intermediate

laboratory technicians and one of the junior student-researchers will be able to access the WSN.

And the last level "Level 5 - Very Low Criticality" also includes generic measures, in addition to preventive and network protection measures, only junior laboratory technicians and another student researcher-junior should have access. Internal and external access of IoT devices to WSN from unauthorized persons is not allowed.

Considering the network for access (i.e., only in case of catastrophe or cyber invasion), it consists of a network that must be used only in case of major emergency or catastrophe exclusively for users who can access and receive external messages of anomalies found. These users are registered in the "Notification List", that is, they are registered users who will receive messages via SMS (Short Message Service) and Twitter in case of any atypical event on the network.

Any atypical event is considered to be a cyber invasion, a nuclear catastrophe, or some other anomaly found (e.g., a radioactive material spill or a decontamination made in an inappropriate way). It should be emphasized that the smartphone receiving the message will be registered by its IMEI number.

These notifications will be sent according to the roles of the people and the type of notification, considering that:

- In case of nuclear catastrophe, the messages will be sent to senior researchers;
- In case of cybersecurity invasion, the messages will be sent to network administrators determining the following items of the three levels indicated in Table 2.

Table 2: Security levels in case of nuclear invasion

Security Level	Description
1	Senior network administrators only
2	Intermediate network administrators only
3	Junior network administrators only

4. FINAL CONSIDERATIONS

The growing concern about cybersecurity is technically justified because any device connected to the network is susceptible to exploitation by unauthorized persons. In this context, understanding that the security of a WSN considering the current IoT context for nuclear research laboratories is important. Relevant characteristics in these critical environments must be identified (e.g., the presence of radioactivity, in addition to the decontamination of materials and equipment); the division of the laboratories' network into functional groups together with the establishment of a severe access control into levels, provides an effective and efficient security mechanism, ensuring its safe use in highly critical environments.

As a continuation of this work, identify the main vulnerabilities existing in WSN with IoT devices to later perform simulated tests, aiming to analyze and determine the vulnerabilities with the greatest impact that the network may be susceptible, in order to verify the behavior of the presented proposal

REFERENCES

1. O. O. Sá, "A segurança das infraestruturas críticas de energia do Brasil", Programa de P'os-Graduaç ão em Energia. Dissertação de Mestrado. Universidade de São Paulo. São Paulo, (2017).
2. "ITU. Internacional Telecomunication Union", "Understanding Cybercrime: A Guide for Developing Countries. Technical Report. April, Switzerland https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-under-standing-cybercrime-guide.pdf (2009).
3. "SP 800-53A Revision 4", "Special Publication Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. July, USA https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final (2014).
4. "SP 800-53, Revision 5. Draft.", "Special Publication. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology. August, USA. July, USA https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft (2017).
5. "SP 800-160 Volume 1.", "Special Publication. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. November, July, USA https://www.nist.gov/publications/systems-security-engineering-considerations-multidisci plinary-approach-engineering-0 (2016).
6. "NIST, Framework, Version 1.1.", "Special Publication. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. April, USA https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cyber security-framework (2018).
7. "ISO/IEC 27001:2013.", "Information technology - Security techniques - Information security management systems Requirements. International Organization for Standardization. October https://www.iso.org/obp/ui/iso:std:iso-iec:27001:ed-1:en (2013).
8. "IAEA, International Atomic Energy Agency", "Computer Security at Nuclear Facilities - Reference Manual - Nuclear Security Series N. 17. June, Vienna https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (2011).
9. "IAEA, International Atomic Energy Agency", "Computer Security for Nuclear Security - Draft-Implementing Guide. December, Vienna https://www-ns.iaea.org/downloads/security/security-series-drafts/implem-guides/nst045.pdf (2016).
10. "IAEA, International Atomic Energy Agency", "Conducting Computer Security Assessments at Nuclear Facilities - Reference

Manual - Nuclear Security Series N. 17 - Draft.June, Vienna https://www-pub.iaea.org/MTCD/Publications/PDF/TDL006web.pdf (2016).