A Proposal for WSN Cybersecurity Levels for IoT Devices in Nuclear Research Facilities

Marcia Maria Savoine
Tocantinense University
Center President
Antonio Carlos – UNITPAC
Nuclear and Energy Research Institute
IPEN, Brazil
savoine@gmail.com

Mário Olimpio de Menezes
Nuclear and Energy Research Institute
IPEN, Brazil
mario@ipen.br

Delvonei Alves de Andrade
Nuclear and Energy Research Institute
IPEN, Brazil
devolnei@ipen.br

ABSTRACT

Nuclear facilities represent a growing security concern and the standards aimed at preserving the physical integrity of these highly critical environments have intensified, considering the scale of the impacts of nuclear accidents. This paper presents a proposal to establish layers, levels and zones of cybersecurity for Wireless Sensor Networks (WSNs) with IoT devices in these critical and hostile environments, taking into consideration the concept of defense-in-depth. The proposal of establishing cybersecurity through layers and levels provides the ability to control access to IoT devices in nuclear facilities, in order to maintain a high level of privacy.

CCS CONCEPTS

• ***Networks*** → *Logical / virtual topologies* • ***Hardware*** → *Wireless devices;*

KEYWORDS

Cybersecurity, Internet of Things, Levels of Security, Wireless Sensor Network.

ACM Reference Format:

Márcia Maria Savoine, Mário Olimpio de Menezes, and Delvonei Alves de Andrade. 2018. A Proposal for WSN Cybersecurity Levels for IoT Devices in Nuclear Research Facilities. In *Proceedings of the 2018 IFIP Latin America Networking Conference (IFIP LANC 2018), October 2018, São Paulo, Brazil.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3277103.3277134

1 INTRODUCTION

Wireless Sensor Networks (WSN) have gained notoriety in various contexts of application in conjunction with new emerging technologies (e.g., Internet of Things – IoT). One of these contexts are nuclear facilities, which are considered critical environments, since a high level of efficiency and effectiveness is required to ensure their physical integrity. In these critical and hostile environments, there is a constant inherent risk due to the presence of radioactivity and the impact of security-related problems, such that it is necessary to avoid access by non-authorized users.

In this sense, the WSNs associated with IoT devices can contribute to managing the security of a nuclear facility (i.e., labs and nuclear research reactors). These technologies commonly are connected to the same internet access infrastructure as other devices and, as these may present vulnerabilities where data can be intercepted and used illegally or inappropriately, it becomes important to establish levels of cybersecurity appropriate to the function of WSNs and IoT devices in such highly critical environments. Therefore, they should have restricted and controlled access due to the presence of radioactive materials, with the objective of avoiding possible catastrophes.

The present study aims to present a proposal for different levels of cybersecurity for Wireless Sensor Networks with IoT devices, for the monitoring and management of safety in nuclear installations.

This paper is organized as follows: in addition to this introductory section, Section 2 establishes related research; Section 3 presents the proposal for security levels; and the concluding remarks follow in Section 4.

2 RELATED RESEARCH

There are still not many studies on levels of cybersecurity for WSNs and IoT devices in nuclear environments, and specifically for laboratories and nuclear research reactors. In bibliographic surveys that were completed, no work was found about this issue. In fact, almost no studies have been found in the existing literature addressing additional issues outside of those related to the management of vulnerabilities or threats to networks in industrial environments [3][4] or nuclear plants [5].

Some studies [11][12] focused on the field of information security for electric power systems and the use of the standard set by the International Organization for Standardization/ International Electrotechnical Commission 17799 (ISO/IEC 17799), precursor to]the ISO/IEC 27001 and the ANSI/ISA-Guide 62443. Other studies [14][13] indicate only the recommended best practices for the use of IoT devices in industrial networks, without addressing security for wireless sensor networks.

IFIP LANC 2018, October 2018, São Paulo, Brazil
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5922-1/18/10...$15.00
https://doi.org/10.1145/3277103.3277134

The IAEA standards [6][8][7] only indicate that SDAs (Sensitive Digital Assets), which consist of files or data, must be protected against unauthorized transmission, without contemplating cybersecurity issues within the current context of WSNs with IoT.

As we can observe from this brief literature review, a formalized and updated structural layered architecture that can be used with safety levels, items, areas, and zones in WSNs with IoT devices in nuclear environments does not yet exist. This gap contributes to the emergence of certain flaws in the assessments of the risks and safety of computer systems and sensors in those nuclear installations that use WSNs and IoT. However, it is particularly important to note that, despite this shortcoming, the IAEA (International Atomic Energy Agency) does not specifically address WSNs and IoT in their documents (manuals and guides), which instead focus only on SDAs (Sensitive Digital Assets) when it comes to the issue of cybersecurity.

Our proposal consists of a layered architecture structured by levels of restricted and controlled access intended to meet the needs of different high-level security locations such as nuclear facilities (laboratories and research reactors), that have highly radioactive equipment and materials.

3 PROPOSAL FOR LAYERS OF CYBER SECURITY AT NUCLEAR FACILITIES

A WSN is a wireless network consisting of spatially distributed autonomous devices, which use sensors to monitor physical or environmental conditions, such as, for example, in a nuclear installation. Therefore, these standalone devices, called nodes, are used with routers and gateways to create a typical WSN system. Distributed measurement nodes communicate wirelessly with a central gateway which provides a connection to the real world, where it is possible to measure, process, analyze and present the collected data. A smart WSN has or accepts in its structure objects, or “things”, or smart objects or IoT (Internet of Things) devices, thus making these networks more flexible and dynamic.

In this sense, a WSN, upon being implemented in a nuclear installation (i.e., nuclear laboratory), can have access to IoT devices through Wi-Fi networks and mobile networks (e. g., 3G, 4G), among others, and may then suffer cyberattacks, intrusions or information theft, thus making these environments more vulnerable.

An environment such as a nuclear research laboratory or a research reactor conducts several activities, including: analysis of radioactive samples; irradiation tests of fuel and structural materials for nuclear reactors; project development of the mechanical design of fuel elements, components and devices of research reactors; development of devices and instrumentation for physical tests for the startup of nuclear reactors; and experiments using the research reactor at zero power for application in nuclear power reactor projects, among many others. It should be noted that these are activities that demand a high level of reliability and security, as they take place in a critical, hostile environment that can involve the manipulation of radioactivity at various moments. The use of a WSN for monitoring these environments is aimed at the prevention of accidents that can have severe impacts on users and the environment.

The proposal of this study, a structure composed of levels and areas of cybersecurity using WSNs with IoT devices, is innovative due to the fact that nothing associated with these environments exists, namely, for nuclear laboratories and research reactors.

The provision of information security can be addressed by three basic attributes, which are confidentiality, integrity and availability of data. Thus, data integrity aims to ensure that all the original features of the data are maintained throughout their life cycle. Confidentiality consists of the right to access the information, which must be attributed only to those who are authorized to access it. Authenticity aims to ensure that the data truly comes from where it was produced, such that it was not the target of any kind of modification or mutation along the way. Lastly, availability is crucial, as it allows for the data to always be available for access by authorized nodes [1].

Therefore, to meet the 3 basic attributes (i.e., confidentiality, integrity and availability) the proposal must start by separating layers, and these layers must then be divided by access levels; subsequently, the access levels must be subdivided into access zones, as shown in Figure 1.

As confirmed by [10], the concept was later incorporated into ISA-99 as the Zone and Conduit Model, which was later incorporated into the IEC-62443 standard. Also, as corroborated by [15], the firewall can block arbitrary packets from the corporate network from entering the control network and can also regulate traffic from the other network zones including the control network. With well-planned rule sets, a clear separation can be maintained between the control network and other networks, with little or no traffic passing directly between the corporate and control networks.

Moreover, [2] also confirms that any communications between zones must be via a defined conduit. Conduits control access to zones, resist Denial of Service (DoS) attacks or the transfer of malware, shield other network systems and protect the integrity and confidentiality of network traffic.

Establishing levels for the control of cybersecurity in a nuclear environment comes from the concept of defense-in-depth, where multiple layers of defense are distributed across the entire control network. In other words, it is based on the application of several layers of security controls for a system, its assets and information. The concept, initially applied to information technology, is fully adapted for wireless sensor networks with IoT devices in critical environments, such as nuclear laboratories or a nuclear research reactor. This concept, associated with other elements, can mitigate the risks and increase the security of these hostile environments.

“The implementation of defense-in-depth security controls should occur at the demarcation points where networks can be segmented. Therefore, a strong defense-in-depth security program must depend on the ability to prevent, detect, respond, and correct against not only the threats that are known today, but also those threats that may appear tomorrow” [10].

In this sense, in our proposal for mitigating risks and existing vulnerabilities, it is advisable to divide every nuclear installation in layers, and specifically in three layers: Business, Supervisory and Lab-Control. Subsequently, in monitored areas with established access controls, each layer should be subdivided into cybersecurity zones and, within these zones, access levels should be established, as can be seen in Figure 1.

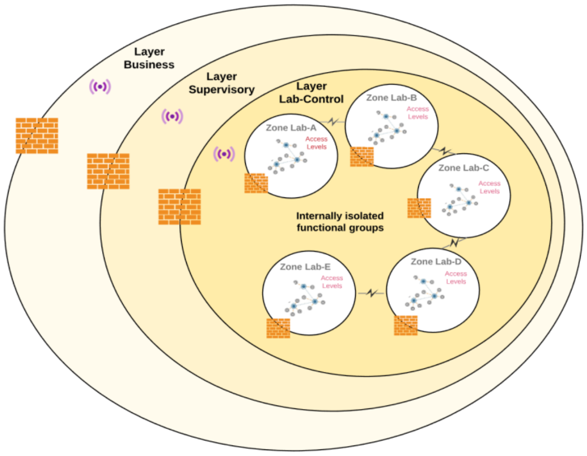

Figure 1: Cybersecurity partitioned structure in layers, levels and zones in a nuclear installation [10] – Adapted.

It also should be emphasized that the control of cybersecurity in the "Business" and "Supervisory" layers are not the focus of this work, instead we focus only on nuclear research reactors and laboratories, that is, the "Lab-Control" layer. It is justified to break up the entire network of a nuclear installation in layers, isolating the WSN laboratories in a single layer; thus the surface of attacks is diminished, mitigating anomalies and existing vulnerabilities.

Thus, a nuclear laboratory, to be monitored by a WSN and with access to IoT devices, will be inside a controlled area divided by access zones, as well as by access levels according to the user's role and the role of the device that will send or receive information.

The "Lab-Control" layer is also divided into levels and controlled access zones, as shown in Figure 2.

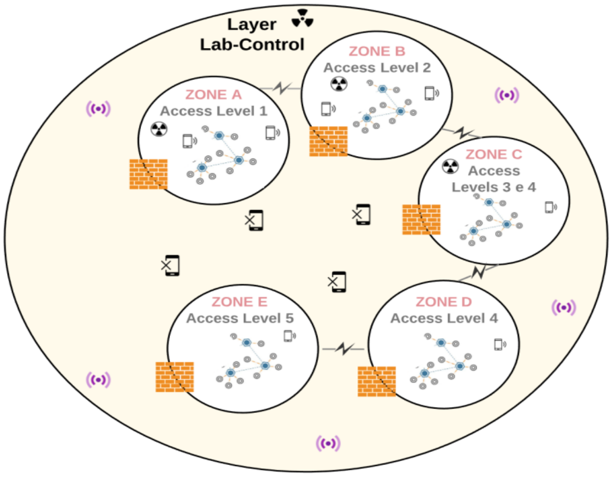

Figure 2: Controlled zones with assigned access levels.

Our proposal is that research laboratories should also be divided into 5 access zones, classified from A to E. Thus, Zone A is an area of high radioactivity, i. e., high criticality, where equipment and materials tests are carried out, in addition to the production of radioactive products, such that the physical access to these sites must take place with appropriate clothing and equipment and, after leaving these places, monitoring, and possibly radioactive decontamination, are necessary. This Zone is restricted for users who have access level 1, both on the WSN and on IoT devices.

In zone B there are also radioactive sites, but to a lesser extent and intensity; thus, level 2 access indicates access to both the WSN and IoT devices. In zone C, there are critical locations in which radioactivity may or may not be present, or in which it may exist in a much smaller quantity; in this sense, access levels 3 and 4 should be determined depending on what users need to have access to. In zone D, the corresponding access level indicated is level 4, and in for zone E, access level 5, since both are development zones for administrative or technical work that do not involve much criticality and do not need to be tracked; however, these are not entirely critical areas.

In addition to the access control levels in a research lab, as shown in Figure 2, it is important to note that there is also a generic management level coupled to each of these five levels, defined as: Level 1 - Extreme Criticality; Level 2 - High Criticality; Level 3 - Medium Criticality; Level 4 - Low Criticality; and Level 5 - Very Low Criticality, as shown in Figure 3.

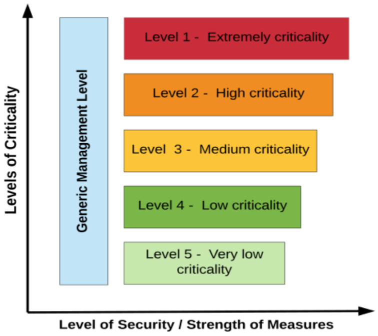
Levels of Criticality
Generic Management Level
Level 1 - Extremely criticality
Level 2 - High criticality
Level 3 - Medium criticality
Level 4 - Low criticality
Level 5 - Very low criticality
Level of Security / Strength of Measures

Figure 3: Structure of the security levels [9] – Adapted.

One aspect to be considered is that the generic management level in our proposal should be applied widely throughout the organization's communication network and not only in a nuclear reactor or research laboratory, because it should function in all aspects of the management of the WSN and IoT devices.

According to the IAEA standard [9], all technical, physical, personal and organizational safety measures for networks and systems should be planned and implemented in a systematic way and under the direction of approved processes and procedures.

Upon implementation of the five levels of access, it is advisable that users (e.g., researchers, laboratory technicians and student-researchers) and WSN administrators receive access only according to their specific functions in the network. The accumulation of permissions is not permitted in order to facilitate the monitoring in the case that anomalies are found. According to this, it is indicated that:

- Network administrators should be classified as junior, middle and senior, such that there may only be one senior administrator, and two middle and junior administrators;

- Researchers should be classified as senior and middle, such that there can be up to 2 researchers of each classification;
- Laboratory technicians should be classified as junior, middle and senior, such that there can be up to 2 technicians of each classification;
- Student researchers should be classified as: High (2 doctoral students), Middle (2 Master ' s students) and Junior (2 students from scientific initiatives).

At "Level 1 – Extreme Criticality", in addition to the inclusion of generic measures, preventive and protective measures should be used for the access level to the WSN, since it requires the highest level of safety criticality. Only the senior administrators of the network and a senior researcher have this type of access. Thus, in cases of great urgency or a catastrophe, only these users will be able to access and receive external messages of anomalies that are found. At this level is also not advised to allow remote access to the nuclear laboratory, as it can be related to a cyberattack.

At "Level 2 - High Criticality", in addition to the inclusion of generic measures, preventive and protective measures should be used for the access level to the WSN. Therefore, at this level only a medium-level network administrator and another senior researcher will have access to and receive messages regarding the anomalies that are found.

At "Level 3 – Medium Criticality", in addition to the inclusion of generic measures, preventive and protective measures for the network should be included, such that only a medium-level network administrator and another medium-level researcher can have access to and receive messages regarding the anomalies found. At this level, it is also advisable that only the IoT devices of authorized persons that are properly registered be allowed external access to the laboratory network.

The next level, assigned "Level 4 – Low Criticality", also includes generic measures, in addition to preventive and protective measures for the WSN. From this level the researchers will not have access, because these are considered to be lower critical impact levels, and thus, there are no access buildups, preventing exposure to vulnerabilities. Thus, only a junior network administrator, an experienced medium-level technician and two high-level students will have access, and only the junior administrator will receive messages of anomalies found.

For the level assigned "Level 5 – Very Low Criticality", generic measures are included, as well as preventive and protective measures for the network. Only one junior level network administrator, one junior technician and one junior and medium-level student should be allowed access, and only the junior administrator will receive messages regarding found anomalies.

Internal and external access to IoT devices and the WSN by unauthorized persons is not allowed in any of the 5 zones.

4 CONCLUDING REMARKS

It is understood that the security of a WSN, considering the current context of IoT for nuclear installations, is important. Important features in these critical environments should be identified (e. g., the presence of radioactivity, in addition to the decontamination of materials and equipment). The implementation of the defense-in-depth concept, through the isolation of networks in layers and of laboratory networks in functional groups or zones, in conjunction with the establishment of the strict control of access levels, provides an effective security mechanism, thus ensuring the safe use of these devices in highly critical environments.

As a continuation of this study, tests will be carried out on a testbed platform for WSNs specifically for IoT devices, aiming to analyze and qualify imminent risks to which the network may be susceptible, in order to verify the behavior of the proposal that has been presented.

REFERENCES

[1] M. Bishop. 2003. *Computer Security: Art and Science.* Addison-Wesley Professional. Boston, MA.

[2] E. Byres. 2014. Using ISA/IEC 62443 Standards to Improve Control System Security. White Paper, Version 1.2. Tofino Security. Lantzville, Canada. May.

[3] R. Candell, D. M. Anand, and K. A. Stouffer. 2014. Cybersecurity Testbed for Industrial Control Systems. *Symposium Process Control and Safety.* Houston, Texas USA.

[4] C. Chi-Shiang, C. Wei-Ho, and S. Yen Kuo. 2015. Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants. *IEEE Transactions on Systems, Man, And Cybernetics: Systems.*

[5] Y. L. Duan, W. F. Fu, X. W. Luo, and Y. L. Yang. 2018. A methodology for reliability of WSN based on software defined network in adaptive industrial environment. *IEEE Journal of Automatica Sinica*, vol. 5, no. 1, pp. 74-82, Jan.

[6] IAEA, International Atomic Energy Agency. 2011. *Computer Security at Nuclear Facilities - Reference Manual - Nuclear Security Series N°. 17.* Vienna, June.

[7] IAEA, International Atomic Energy Agency. 2016. *Conducting Computer Security Assessments at Nuclear Facilities.* June. Vienna, Austria.

[8] IAEA, International Atomic Energy Agency. 2016. *Computer Security for Nuclear Security - Draft-Implementing Guide.* December. Vienna, Austria.

[9] IAEA, International Atomic Energy Agency. 2017. Computer Security Techniques 10 for Nuclear Facilities. Nuclear Security Series, NST047, Draft. Vienna, Austria.

[10] R. Knapp, E. D. Langill, and J. Thomas. 2015. Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control System Second Edition. Syngress-Elsevier. Waltham, MA-USA.

[11] K. Stouffer, A. Falco, A. Joseph, and K. A. Scarfone. 2013. *Guide to Industrial Control Systems (ICS) Security.* NIST - Special Publication 800-82, Revision 1. May 14.

[12] ISA-62443-1-1. 2015. *Security for industrial automation and control systems - Models and Concepts.* Draft 5, Edit 4. North Carolina, August. USA.

[13] SP 800-53A Revision 4. 2014. NIST *Special Publication Assessing Security and Privacy Controls in Federal Information Systems and Organizations*: Building Effective Assessment Plans. July.

[14] SP 800-53, Revision 5. Draft. 2017. NIST Special Publication. *Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology. August. USA.

[15] SP 800-82 Rev.2. 2014. Guide to Industrial Control Systems (ICS) Security. Second and Final Draft Special Publication 800-82 Revision 2. National Institute of Standards and Technology. Gaithersburg, Maryland, USA.