Scientific Research Publishing

World Journal of Nuclear Science and Technology, 2018, 8, 78-85
http://www.scirp.org/journal/wjnst
ISSN Online: 2161-6809
ISSN Print: 2161-6795

# Proposal of a Methodology for the Assessment of Security Levels of IoT Wireless Sensor Networks in Nuclear Environments

**Marcia Maria Savoine[1,2], Mario Olimpio de Menezes[2], Delvonei Alves de Andrade[2]**

[1]Tocantinense University Center President Antonio Carlos—UNITPAC, Tocantins, Brazil
[2]Nuclear and Energy Research Institute, São Paulo, Brazil
Email: marciasavoine@itpac.br, mario@ipen.br, devolnei@ipen.br

**How to cite this paper:** Savoine, M.M., Menezes, M.O and Andrade, D.A. (2018) Proposal of a Methodology for the Assessment of Security Levels of IoT Wireless Sensor Networks in Nuclear Environments. *World Journal of Nuclear Science and Technology*, **8**, 78-85.
https://doi.org/10.4236/wjnst.2018.82008

**Received:** February 27, 2018
**Accepted:** April 8, 2018
**Published:** April 11, 2018





## Abstract

The use of Wireless Sensor Networks (WSN) associated with the reality of an Internet of Things (IoT) scenario in nuclear environments is a growing security concern. In this context, standards are intensified to preserve the physical integrity of these facilities considered to be highly critical due to the size of the impacts of safety accidents. This paper presents a proposal to build a methodology to evaluate the security levels of WSNs with IoT devices when used in nuclear areas. The proposal is initially based on related work to establish a more concrete initial framework and is structured in consistent steps from previous scientific studies.

## Keywords

Framework, Internet of Things, Methodology, Security, Wireless Sensor Network

## 1. Introduction

Over the last few years, safety and security concerns in nuclear facilities have grown considerably, and thus standards have been intensified to preserve their physical integrity.

Nuclear areas are considered critical and hostile environments because of the inherent risk of the presence of radioactivity and the extent of the impact of safety-related problems. Examples are the Chernobyl and Fukushima accidents and their long-standing impact on people's lives [1]. The Chernobyl accident caused the largest uncontrolled radioactive release into the environment ever recorded for any civilian operation, and large quantities of radioactive substances were released into the air for about 10 days. This caused serious social

and economic disruption for large populations in Belarus, Russia, and Ukraine [2].

As technology advances, the use of computers and computing systems in all aspects of operations, including nuclear safety and nuclear security, is expected to increase [3]. Similarly, the Internet of Things (IoT), together with Wireless Sensor Networks (WSN), is gaining importance in the continuous advancement of information and communication technologies, especially due to their connection and integration with the Internet in several application areas.

The Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) state that: "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or design basis threat" [3].

Therefore, the use WSNs for IoTs in such nuclear environments has demanded the existence of an appropriate methodology for the evaluation of issues related to their safe application in critical tasks, such as restricted area monitoring or device sensors for critical equipment.

This paper aims to present a proposal of construction of a methodology to evaluate the safety levels of WSN with IoT devices, used in nuclear areas.

The work is organized as follows: in addition to this introductory section, Section 2 establishes the theoretical background and the related works. In Section 3, the structure of the proposed methodology is presented. Finally, Section 4 brings the final considerations.

## 2. Theoretical Background

In all types of networks, but especially in wireless sensor networks (WSNs) with IoT devices, security issues are of paramount importance, mainly when it comes to their use in hostile environments, such as the nuclear ones.

Preventing, detecting and responding to malicious acts involving nuclear materials, other radioactive materials or associated facilities and activities is the goal of nuclear safety. Computers systems, and digital components, in general, play an increasingly important role in managing sensitive information, physical and logical nuclear safety, and material control at these facilities. The compromise of computational systems could have a negative impact on nuclear safety, both directly and indirectly, and could support malicious acts [4].

Nuclear security can be evaluated, considering the digital components, such as IoT devices and WSN, by means of its basic attributes necessary to provide information security, such as: "confidentiality, integrity and availability, of data". Data integrity is intended to ensure that all original data characteristics are maintained throughout their life cycle. Confidentiality consists of the right to access information, which should be assigned only to those who are authorized to access it. Authenticity aims to ensure that the data actually comes from where

it was produced, not being subject to any kind of modification or mutation along the way. Lastly, the availability is paramount, as it allows the data to be always available to the nodes authorized to access it [5].

## Related Work

There are still few studies on methodologies to evaluate the safety of wireless sensor networks, while is practically nonexistent methodologies that evaluate the security of a WSN with IoT devices. Bibliographical surveys were conducted and did not find any works concerning this problem, being even worst in nuclear area, with a totally null count of related work. The few studies that were found in the literature address only the management of vulnerabilities or threats of wireless networks or wireless sensors.

Authors such as Cansian, Grégio and Palhares, Pinto and Gomes [6] [7], present the vulnerabilities and threats of wireless networks such as, failures in the WEP protocol, report susceptibilities to external invasions and decryption of packets.

Kawai, Wakamiya and Murata [8] propose a network architecture methodology for fast and reliable transmission of urgent wireless sensor information. In the methodology, several simple and fully distributed control mechanisms that operate at different spatial and temporal levels are introduced at each node to offer a differentiated transmission option to the packets according to their importance.

The work of Oliveira [9] proposes not a methodology, but a model of security management for wireless sensor networks, including selection of security components, description of management information, description of messages and, definition of security events.

Moreover, McNab [10] proposes and emphasizes that an evaluation methodology is the best practice used to evaluate security besides being relevant to testing networks randomly on the Internet, that is, without a specific domain name or a specific block of IP addresses, and when one have limited information about the targets.

As we have seen from this bibliographical survey, there is no updated and formalized methodology that can be used to evaluate security levels of WSNs with IoT devices in nuclear environments (considered hostile, critical, and demanding on a high level of security). This gap contributes to the emergence of failures in the risk and safety assessment of the computer systems and sensors of nuclear facilities that use WSNs with IoTs. It is also important to note that, despite the concern of the IAEA (International Atomic Energy Agency) regarding cyber security, its documents (manuals and guides) do not specifically address WSN with IoT devices.

## 3. Proposed Methodology

It is known that it is not possible to have a totally secure network, however, it is

possible to control the risks by means of appropriate methodologies establishing security levels and periodic evaluations.

In this sense, Silva and Ludwig [11] propose a methodology for auditing 802.11 b/g wireless networks focused on information security, based on six phases, which are: Planning, Research and Documentation, Discovery and Validation, Development of Solutions, Report and Monitoring.

Nevertheless, McNab [10] presents a methodology for network security that has two main focuses: comprehensiveness and flexibility; the first provides consistent identification of significant failures, and the second should prioritize efforts and maximize return. This methodology is composed of four distinct steps: Recognition to identify networks, hosts and users of interest; Scanning for vulnerabilities to identify potential exploit conditions; Investigation of vulnerabilities and additional probing done manually; Exploitation of vulnerabilities and evasion of security systems.

The framework of the methodology proposed in this work consists of hybrid phases of both methodologies indicated by McNab, Silva and Ludwig [10] [11], and adapted items that are characteristic of wireless sensor networks with IoT devices. The central concept of this methodology is based on the framework depicted in **Figure 1**.

Each phase of the framework will unfold in several subphases, briefly described below, whose main objective is to provide flexibility and comprehensiveness to the methodology [10]. It's also important to mention, that most phases, if not all, of the proposed methodology, would be happening in parallel, that is, it's not a sequential execution job, except for the first run, after what


**Figure 1.** Structure of the proposed methodology framework.

there'll be several references with feedback between the phases.

In this sense, according to **Figure 1**, in phase 1 "WSN Planning and Analyzes", by means of a checklist, the WSN fundamental characteristics, its known vulnerabilities and IoT device related criticalities, according to its specificities, should be raised and analyzed. Phase 2 "Search and Documentation", will be composed of 2 subphases; in the first, 2.1, the level of criticality of each vulnerability pointed out in the previous phase, will be analyzed and in subphase 2.2, critical vulnerabilities allocated within their criticality level should be thoroughly documented. In phase 3, "Discovery and Validation", all network services will be probed to detect those that are open and could be further exploited to achieve specific objectives (e.g., execution of a code, an information leak or a denial of service, among others). Phase 4, "Solutions Development" is responsible for develop, test and implement solutions for the problems identified in previous phases. Being a dynamic framework, all new information coming from the previous phases will be used to develop, test and implement solutions. Finally, in phase 5, "Monitoring and Reporting", are included permanent activities, like monitoring and auditing, as well as, carefully reporting to support new planning and analysis, together with the remaining activities of the methodology.

Similarly, factors like the dynamic characteristics of a nuclear area WSN, along with battery consumption control for the large number of nodes in use, as well as energy efficiency, fault tolerance, and scalability need to be carefully considered. However, in an emergency, urgent information must be transmitted as quickly and reliably as possible, therefore, reliability and low latency are primary concerns.

The proposed structure is justified by the initial requirements already identified for constructing the methodology to evaluate the security of a WSN with IoT devices in a context of priority, being: high reliability and low latency, self-organization and localized behavior, and simplicity. In that way, the reliability and latency of the transmission of urgent information are the most important issues. Nonetheless, the type and scale of an emergency and the number of simultaneous emergency events are unpredictable and dynamically change as time passes. Finally, simplicity consists of simple and light mechanisms to support the fast and reliable transmission of information, since a node has low processing capacity and memory.

It is also important to establish security levels at all stages of the framework, following the practice of IAEA standards [4] [12], that indicate that security levels are a way to specify the extent and security considered necessary for different SDAs (Sensitive Digital Assets). At each level, in a graduated approach, different sets of protective measures should be applied to meet the security requirements for that level. Measures with increased stringent are applied to more critical SDAs, as shown in **Figure 2**.

The use of levels and zones is a graded approach to identify computer security measures that are proportionate to the potential consequences of the failure of

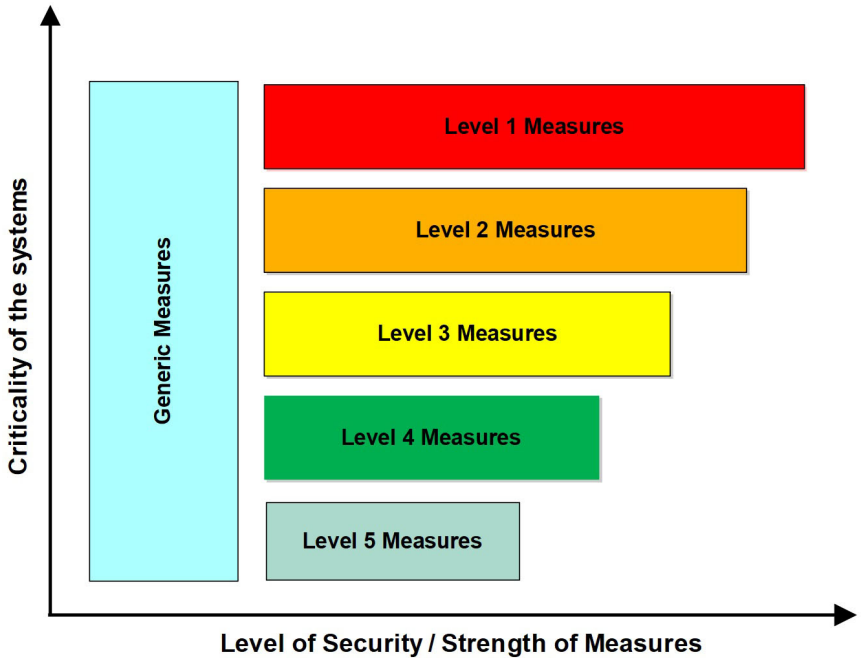


**Figure 2.** Structure of the security levels established by the IAEA [12].

those measures. Level 1 measures would be applied for those SDAs that, if compromised, their operation could lead to the most severe consequences, including the most significant nuclear security events. The Lower level measures, for example levels 4 and 5, might be applied for computer-based systems that have nuclear security related functions but that are not considered SDAs. And generic security measures should be applied to all computer-based systems with nuclear security related functions [12].

Grouping computer-based systems and the associated SDAs in zones of graded security levels, is a practical way to implement this graded approach.

Regarding these IAEA standards [3] [4] [12], however, security issues in the current context of WSN with IoT are not considered, despite of its necessity in face of the demand to establish security levels coupled to more robust protocols, which would provide an in-depth defense against cyber-attacks. In this context, robustness might mean, for instance, that communication protocols must be able to self-adjust to cope with such attacks without human intervention.

Another concern is the 6LoWPAN layer, responsible for connecting IoT devices and WSNs to the MAC and Network Layers; thus, the study of all possible usage scenarios of this layer (6LoWPAN) in critical environments, its security features, as well as other routing protocols, is a primary obligation of the proposed methodology, aiming to evaluate the reliability of the security levels of the target WSN with IoT protocols.

## 4. Concluding Remarks

The difficulties faced with WSNs security are real, as are the numerous possible vulnerabilities in WSN with IoT devices, mainly in a nuclear environment due to

the impact of their exploitation. The specification of a methodology to assess the security levels and all security related items is extremely important for the nuclear area in the scenario of possible security threats.

In view of all the bibliographical research conducted, it was verified the inexistence or scarcity of publications or studies under development about methodologies for the evaluation of WSNs with IoT devices in the nuclear area, even considering the series on computer security in nuclear environments of the IAEA, "Computer Security for Nuclear Security: Draft-Implementing Guide", December 2016 [3], Nuclear Security Series No. 17, "Conducting Computer Security Assessments at Nuclear Facilities", June 2011 [4], "Objective and Essential Elements of a State's Nuclear Security Regime", June 2016 [12] and which emphasizes the importance of cyber security assurance activities.

The proposed approach is unique in the sense that it intends to incorporate several important items from a nuclear context (e.g., temperature, fire alarm, invasion warning, seismic movement, cyber-attacks, radiation, among others), to design a methodology that provides a fast and reliable transmission of information considered critical and urgent due to the inserted environment.

## References

[1] Ikeda, A., Tanigawa, T., Charvat, W.H., Shigemura, J. and Kawachi, I. (2017) Longitudinal Effects of Disaster-Related Experiences on Mental Health among Fukushima Nuclear Plant Workers: The Fukushima NEWS Project Study. Cambridge University Press, Psychological Medicine, Page 1 of 11.

[2] Bennett, B., Repacholi, M. and Carr, Z. (2006) Health Effects of the Chernobyl Accident and Special Health Care Programmes Report of the UN Chernobyl Forum. Expert Group "Health", Geneva, Switzerland.

[3] IAEA, International Atomic Energy Agency. (2016) Computer Security for Nuclear Security: Draft-Implementing Guide.

[4] IAEA, International Atomic Energy Agency. (2011) Computer Security at Nuclear Facilities: Reference Manual—Nuclear Security Series No. 17. Vienna.

[5] Bishop, M. (2003) Computer Security: Art and Science. Addison-Wesley Professional, Boston, MA.

[6] Cansian, A.M., Grégio, A.R.A. and Palhares, C.T. (2004) Failures in Configuration Policies: A Risk Analysis for Wireless Networks in the City of São Paulo. Paulista State University, São Paulo, SP.

[7] Pinto, P.M. and Gomes, A.R.L. (2011) Security in Wifi Connectivity in Mobile Devices: iPhone Case Study. Journal Exacta, Belo Horizonte, MG, Brazil.

[8] Kawai, T., Wakamiya, N. and Murata, M. (2007) Design Methodology of a Wireless Sensor Network Architecture for Urgent Information Transmission. Graduate School of Information Science and Technology. *WICON*'07, *Proceedings of the* 3*rd International Conference on Wireless Internet*, Austin, Texas, 22-24 October 2007, 1-30.

[9] de Oliveira, S. (2008) Study of Security Mechanisms for Protection of Routing in Wireless Sensor Networks. Doctoral Thesis, Federal University of Minas Gerais, Department of Computer Science, Belo Horizonte, MG.

[10] McNab, C. (2016) Network Security Assessment: Know Your Network. 3rd Edition,

O'Reilly Media, Sebastapol, CA.

[11] Silva, F. and Ludwig, G.A. (2008) Development of a Methodology for Auditing in IEEE 802.11b/g Wireless Networks. *VIII Brazilian Symposium on Information Security and Computational Systems*, Gramado, RS, Brazil.

[12] IAEA, International Atomic Energy Agency. (2016) Conducting Computer Security Assessments at Nuclear Facilities. Vienna.