Risk Assessment in IoT Case Study: Collaborative Robots System

Salim Chehida, Abdelhakim Baouya
University of Grenoble Alpes, CNRS, VERIMAG F-38000
Grenoble, France
{name.surname}@univ-grenoble-alpes.fr

Paul-Emmanuel Brun, Guillemette Massot
Airbus CyberSecurity SAS
Elancourt, France
{name.surname}@airbus.com

Miquel Cantero
Robotnik Automation S.L.L
Valencia, Spain
mcantero@robotnik.es

***Abstract*—Security is one of the crucial challenges in the design and development of IoT applications. This paper presents an approach that focuses on existing security standards to evaluate and analyse the potential risks faced by IoT systems. It begins by identifying system assets and their associated vulnerabilities and threats. A list of security objectives and technical requirements are then defined to mitigate the risks and build a secure and safe system. We use our approach to assess risks in the robotic system for supporting the movement of loads in a warehouse.**

***Index Terms*—Security Risk Assessment, IoT, Threats, Security Requirements.**

I. Introduction

Internet of Things (IoT) is a promising technology that offers significant improvements to various domains such as health, commerce, construction, buildings management, energy, and transport. It reduces management costs, automates the monitoring of infrastructures and equipment, saves energy, and more. An IoT system consists of a network of smart devices that collaborate with users to accomplish intelligent services. It generally groups a large number of devices that interact using multiple communication technologies and protocols.

In the last decade, IoT systems are increasingly susceptible to various security issues, such as malicious access to services and network attacks. These problems have caused considerable damage and affected the secrecy, integrity, and availability of information. There are several surveys, such as [1]–[4], that discuss vulnerabilities that can be exploited by attackers to damage IoT systems. Taking into account these risks and their possible consequences constitute one of the principal challenges for the designer and developer of these systems.

Security Risk Assessment (SRA) is the process that aims to identify the most critical threats and provide the required measures to avoid these threats. It aims to mitigate the risks and build a secure system while covering its vulnerabilities. Several SRA methodologies [5]–[9] have been proposed to evaluate risks and enforce a common level of security. However, these methods are generic, and they do not consider the complexity and the dynamic of IoT systems.

In this work, we present a new approach that considers existing methodologies and standards for risk assessment in IoT systems. It starts by identifying the assets that should be protected and evaluating the threats they face. Then, a list of security objectives and requirements are defined to defend the system against potential threats. We apply our approach to the collaborative robots system. Our approach is different from all the generic approaches mentioned above and presented in Section II. It is dedicated to IoT systems and takes into account the relevant domain model and standards, as well as the need for evolution of these systems.

This paper is organized as follows: Section II presents the main approaches and standards for security assessment. We give an overview of our risk assessment approach in section III, then we describe its different stages and apply them to our case study in sections IV to VI. Finally, we give our conclusions in Section VII.

II. State of the art

We first present the main security standards, then the existing methods for risk assessment.

A. Security Standards

Security standards guide an organization in best security practices in order to enforce a common level of security by ensuring availability, integrity, and confidentiality requirements. Many countries and organizations have established standards for risk assessment and analysis. In this section, we briefly present the relevant common and IoT security standards.

(a) *Common Standards*

- ISO/IEC 27002 [10]: International standard that gives general guidance on the commonly accepted goals of information security management. It describes general principles structured around 36 security objectives and 133 controls.

- AS/NZS 4360 [11]: The joint Australian/New Zealand risk management standard that provides a generic framework for identifying, analysing, evaluating, treating, monitoring, and communicating risk.
- ISO/IEC 27005 [12]: International standard that provides guidelines for managing information security risks in an organization. The standard describes the risk management process, which includes context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.
- BS7799 (ISO17799) [13]: British Standard (Code of Practice for Information Security Management), evolved into ISO17799 (The Information Security Standard). It gives a basis guide for risk assessment and information security management.
- NIST SP 800-30 [14]: Special Publications Risk Management Guide for Information Technology Systems standard that provides practitioners with practical guidance for carrying out each of the three steps in the risk assessment process (i.e., prepare for the assessment, conduct the assessment, and maintain the assessment). It also discusses how organizational risk management processes complement and inform each other.
- NIST SP 800-82 [15]: This standard guides on improving security in Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).
- IEEE 1686 [16]: Standard for Intelligent Electronic Devices Cyber Security Capabilities' that defines functions and features to be provided in Intelligent Electronic Devices (IEDs). The document addresses access, operation, configuration, firmware revision, and data retrieval of an IED.

(b) *IoT Security Standards*

The authors in [17] analyse the existing regional and international standards for IoT security and indicate their limitations. Among international standards:

- ITU-T standards[1] :
  - Y.2060 provides reference models of IoT and shows generic security capabilities on every layer.
  - Y.2063 covers the authorization of heterogeneous devices of WoT.
  - Y.2066 defines common requirements of IoT and also security and privacy protection requirements related to all the IoT actors.
  - Y.2067 covers gateway security mechanisms including authentication, data encryption, privacy protection, etc.
  - Y.2068 defines concepts of functional framework and capabilities of IoT, including service provision security, security integration, security audit, etc.
  - Y.2075 specifies the security capabilities of EHM (e-health monitoring) with IoT.
  - Y.4112/Y.2077 specifies the concept, purpose, and components of plug and play (PnP) capability of the IoT, including security-related requirements.
  - Y.4553 specifies the requirements of the smartphone as a sink node for IoT applications, including authentication and data protection capabilities.
  - Y.4702 provides common requirements and capabilities of device management (DM) in IoT, including security management capabilities such as security event detection and reporting, device security assurance, and device security control.
- ISO/IEC standards: ISO/IEC 30128 [18] covers IoT security related to sensor network application interface.

Among regional standards, ETSI (standards organization in the telecommunication industry in Europe) recently provided "ETSI TS103645" [19] (Cyber Security for Consumer Internet of Thing) standard that gives security practices for consumer devices connected to the Internet.

According to [17], most of the IoT security standards presented above are just specification-level standards and a few of them are involved in availability and non-repudiation.

B. Risk Assessment Methods

EBIOS [9] is used for the assessment and treatment of risks associated with an Information System (IS). Its steps are: definition of the context, identification and estimation of the security needs and eventual sources of threats, identification and analysis of threat scenarios, and finally specification of security objectives and measures to be implemented for risk treatment. The goal of the EBIOS method is to create a common ground for security discussion between various stakeholders in order to support management-level decision-making. One of the main strengths of the EBIOS approach is its modularity; its knowledge bases can be tuned to comply with local standards and best practices, and to include external repositories of attack methods, entities or vulnerabilities [20].

CRAMM [7] (CCTA Risk Analysis and Management Method) is a qualitative risk assessment methodology that consists of the following steps: collection of data and definition of objectives, identification and evaluation of system assets, threat and vulnerability assessment, and finally determining countermeasures.

AURUM [5] (Automated Risk and Utility Management) supports the NIST SP 800-30 standard [14]. It consists of the following steps: identification of risks and their impacts, implementation of adequate countermeasures, and evaluation of the impact of countermeasures.

CORAS [6] allows risk assessment, documentation of intermediate results, and presentation of conclusions. The main steps of the methodology are: definition of security goals,

[1]https://www.itu.int/en/ITU-T/Pages/default.aspx

description of threats, risk estimation by giving likelihood values for identified unwanted incidents, and risk treatment.

MEHARI [8] (MEthod for Harmonized Analysis of RIsk) aims to provide a risk management model compliant to ISO-27005 [12]. The steps of MEHARI are: establishment of the organization context, identification and classification of assets, identification and analysis of risks, and finally quantification and management of risks. MEHARI allows the analysis of the security stakes and the preliminary classification of the IS entities according to three basic security criteria (confidentiality, integrity, and availability).

OCTAVE [21] (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method allows to define a risk-based strategic assessment and planning technique for system security. It is based on process broken into three phases : development of initial security strategies, identification of infrastructure vulnerabilities, and development of final security strategy and plans.

IT-Grundschutz [22] provides methods, processes, procedures, and measures to establish a system for information security management. It describes a two-tier risk assessment: one is designed for reaching a *standard* level of security, while a second *supplementary risk analysis* can be undertaken by companies that desire an approach customized to their specific needs or sector or that have special security requirements. IT-Grundschutz also provides lists of relevant threats and required countermeasures that can be adapted to the needs of an organization.

III. An outline of our Methodology

Starting from standards and methods presented in the previous section, we define the risk assessment methodology depicted in Figure 1.

Our method consists of four steps:

1) The first step identifies the assets based on the IoT domain model.
2) The second step specifies threats on the assets based on common threats database proposed by the risk assessment methods presented in Section II. In this work, we consider EBIOS database [9], which is compatible with all relevant ISO standards and provides a complete list of possible threats (42 threats) relative to information systems. EBIOS threats database is widely used in risk assessment. Some works like [23] have used it for risk analysis of IoT systems.
3) In the third step, security objectives are derived from the threats. In this step, we extract relevant objectives (13 objectives) for IoT systems from ISO-27002 [10] that provides a set of generic security objectives supported by a set of controls that are an important part of information security management.
4) In the last step, security requirements are built in order to implement the security objectives and provide countermeasures of the identified threats.

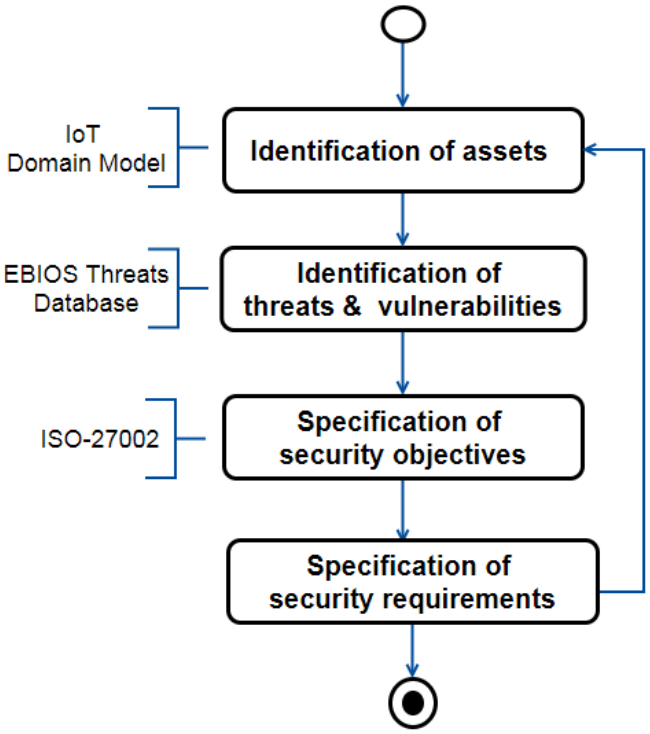

Fig. 1. IoT Risk Assessment Methodology.

Our approach is iterative, and security requirements can be revised after the system assets have been refined. The results of each step should be checked with the customer.

In this work, we apply our method to the service robotics system. As shown in Figure 2, our system consists of a fleet of robots installed in a warehouse to support the movement of different loads.

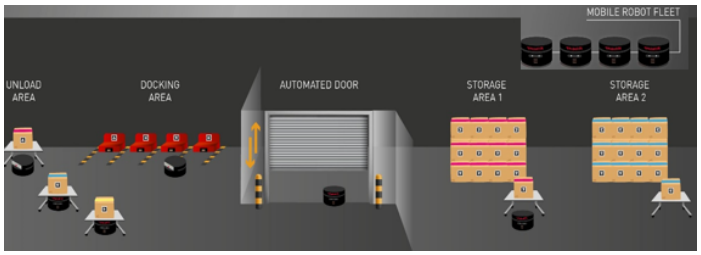

Fig. 2. Service Robotics System.

The flow of these loads does not require any operator to command the fleet. Robots are expected to empty continuously an “unload area” where different loads are put together. At some point, the system needs to identify the different items and then asks a specific robot to pick it and place it in a specific storage area following some predefined rules. It is also foreseen that in order to perform such activity, the system will need to actuate IoT devices, for example, an automated door in the middle of the robot’s path to “storage areas”.

IV. Identification of assets

ISO-27001 [24] defines an asset as "*any tangible or intangible thing or characteristic that has value to an organization*". In our approach, we refer to IoT domain model proposed by [25] to facilitate the identification of the system assets. In this model, the main concepts are: *thing*, *device*, *user* and *resource*.

As shown in Figure 3, *Thing* is the combination of PE (Physical Entity) together with its digital representation VE (Virtual Entity).

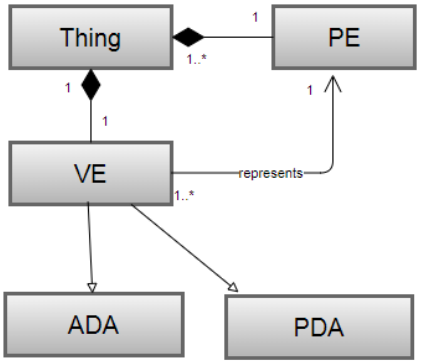

Fig. 3. IoT Things.

VE can be of both types:

- Passive Digital Artefact (PDA): a digital representation of PE stored in a database or similar form.
- Active Digital Artefact (ADA): any type of active code or software program usually be some sort of software agent or embedded application.

Device is a hardware with computing and network capabilities that allows to monitor or interact with PE. As shown in Figure 4, device can be:

- Sensor : allows to monitor PE.
- Actuator : allows to act on PE.
- Tag : allows to identify PE and can be read by sensors.

User represents who interacts with PE physically or through software interfaces. Users can either be humans or ADA.

Resource is software components that can provide information about PE, allow the execution of actuation tasks, or analyse data provided by multiple sensors. Resources may be hosted on a Device, or they could be hosted anywhere in the network.

Table I presents examples of 16 assets identified in our case study. The system includes different types of devices, such as sensors (e.g., A3, A4, A5) and actuators (e.g., A13, A14, A15).

V. Identification of threats and vulnerabilities

ISO-27001 [24] defines a threat as "*a potential cause of an unwanted incident, which may result in harm to a system or organization*" and considers vulnerability as "*weakness that is related to the organizations' assets, which sometimes could cause an unexpected incident*".

As mentioned in Section III, our method considers a list of generic threats from EBIOS database. In Table II taken from

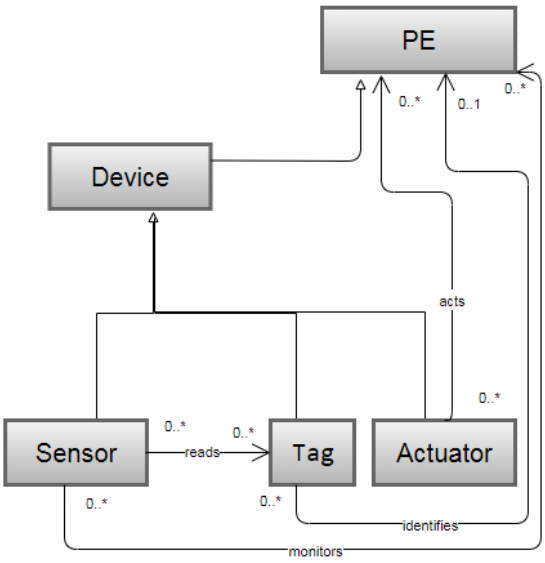

Fig. 4. IoT Devices.

Asset ID	Asset Description
A1	Mobile Robot: Embedded Computer
A2	Mobile Robot: Motion Control (motor driver)
A3	Mobile Robot: Sensor 1, RGBD Camera
A4	Mobile Robot: Sensor 2, Lidar
A5	Mobile Robot: Sensor 3, Odometry
A6	Mobile Robot: Lift Mechanism
A7	Mobile Robot: Battery (LiFePo)
A8	Mobile Robot: Network (Card)
A9	System: User Computer
A10	System: Network (Router and infrastructure)
A11	System: Mission Command (Outwards)
A12	System: Robot State (Inwards)
A13	Door PLC
A14	PLC WiFi Gateway
A15	PLC: Opening order (Inwards)
A16	Operator HMI

TABLE I
Robots System Assets.

the EBIOS knowledge bases, threats are classified into eight main categories:

- Physical damage: T-1010 to T-1050.
- Natural events : T-2010 to T-2050.
- Loss of essential services : T-3010 to T-3030.
- Disturbance due to radiation : T-4010 to T-4030.
- Compromise of information : T-5010 to T-5110.
- Technical failures : T-6010 to T-6050.
- Unauthorized actions : T-7010 to T-7050.

ID	Threats Description	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
T-1010	Fire	X	X	X	X	X	X	X	X	X	X			X	X		
T-1020	Water damage	X	X	X	X	X	X	X	X	X	X			X	X		
T-1030	Pollution	X	X	X	X	X	X	X	X	X	X			X	X		
T-1040	Major Accident	X	X	X	X	X	X	X	X	X	X			X	X		
T-1050	Destruction of equipment or media	X	X	X	X	X	X	X	X	X	X			X	X		
T-2010	Climatic Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2020	Seismic Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2030	Volcanic Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2040	Meteorological Phenomenon	X	X	X	X	X	X	X	X	X	X			X	X		
T-2050	Flood	X	X	X	X	X	X	X	X	X	X			X	X		
T-3010	Failure of air-conditioning	X	X							X				X			
T-3020	Loss of power supply	X	X	X	X	X	X	X	X	X	X			X	X		
T-3030	Failure of telecommunication equipment	X							X		X	X	X		X	X	X
T-4010	Electromagnetic radiation								X		X	X	X		X	X	X
T-4020	thermal radiation	X	X	X	X	X	X	X	X	X	X			X	X		
T-4030	Electromagnetic pulses	X	X	X	X	X	X	X	X	X	X			X	X		
T-5010	Interception of compromising interference signals										X	X	X		X	X	X
T-5020	remote spying			X													X
T-5030	eavesdropping	X							X		X	X	X		X	X	
T-5040	Theft of media or documents													X	X		
T-5050	Theft of Equipment	X	X	X	X	X	X	X	X	X	X			X	X		
T-5060	Retrieval or recycled or discarded media																X
T-5070	disclosure																X
T-5080	data from untrustworthy sources	X											X				X
T-5090	Tampering with hardware	X	X	X	X	X	X	X	X	X	X			X	X		
T-5100	Tampering with software	X	X							X		X		X	X	X	X
T-5110	Position detection				X	X											
T-6010	Equipment failure	X	X	X	X	X	X	X	X	X	X			X	X		
T-6020	Equipment malfunction	X	X	X	X	X	X	X	X	X	X			X	X		
T-6030	Saturation of the information system	X														X	X
T-6040	Software malfunction	X								X							X
T-6050	Breach of information system maintainability	X								X				X			X
T-7010	Unauthorised use or equipment	X								X							X
T-7020	Fraudulent copying of software	X								X				X			X
T-7030	use of counterfeit or copied software	X								X				X			X
T-7040	corruption of data	X							X	X	X			X	X		X
T-7050	Illegal processing of data	X		X					X	X	X			X	X		X
T-8010	Error in use	X							X	X	X			X	X		X
T-8020	Abuse of rights	X							X	X	X			X	X		X
T-8030	Forging of rights	X							X	X	X			X	X		X
T-8040	Denial of actions	X								X				X			X
T-8050	Breach of personnel availability	X								X				X			X

TABLE II
THREAT-ASSET MATRIX.

- Compromise of functions :T-8010 to T-8050.

The threat factors can be divided into two categories:

- *Environment factors* such as earthquakes or floods, cannot be avoided. The risk manager should always consider environment threats according to their operating environment, even if it is difficult to consider them.
- *Human factors*, which are more of our concern because they are vagrant regarding different people and different situations, and it is more difficult to predict human behavior than regular natural disasters. We distinguish persons who belong to the organization like different users of the system and persons from outside the organization such as recipient, provider, and competitor.

In Table II, we show the threats associated to each asset presented in Table I.

VI. Specification of security objectives and requirements

In this step, we based on ISO-27002 [10] generic list to specify security objectives needed to protect the system assets against the identified threats. We also map each security objective with the threat list. Table III gives an example of security objectives that cover the most potential threats presented in the previous step.

After the specification of security objectives, we define security requirements. In Table IV, each security objective from Table III leads to the implementation of one or more technical requirements.

ID	Security Objective	Security Objective Description	Threats
O1010	Protection Against Malicious Code	Prevent and detect the allocation of any malicious code, as well as connections of any unprivileged user to the robot network	T-50xx
O1020	Backup	The data from the initial robot setup and the robot firmware require regular backup	T-10XX T-20XX
O1030	Network Security Management	Protect the information and communication in network from a client to robot. Sending REST Command once authenticated in the same network can modify the operations	T-5030 T-5090 T-7010 T-7020 T-7040
O1040	Exchange of information	Secure the interaction between the platform and robot system	T-5070 T-5080
O1050	Monitoring	Logs and robot system state shall be secured to prevent a bad usage (i.e. a door opened)	T-5030 T-5040 T-60xx T-70xx T-80xx
O2010	User Access Management	Authentication and authorization of the robot and any user or system accessing the robot	T-7010 T-7020 T-7040 T-8020 T-8030
O2020	Network Access Control	Prevent unauthorized use of robot network services	T-6030 T-70xx
O2030	Operating System Access Control	Rely on the access control mechanism offered by Ubuntu	T-8020 T-8030 T-8040
O3010	Correct processing in applications	Check any command received by the robot and the processing status of the robot. No robot shall accept commands out of reach by itself	T-60xx
O3020	Cryptographic controls	Protect the sensible information in the robot network and also the authentication operations of the users or systems accessing the robot	T-8020 T-8030
O3030	Security of system files	Rely on the security mechanisms and limitation rules offered by Ubuntu to protect the system files	T-8020
O3040	Security in Development and support process	Control of information flow and integrity in robot systems	T-6040 T-6050 T-8040 T-8050
O3050	Technical vulnerability management	Detect and deal with the technical vulnerabilities to reduce the risks such as physical interfacing of robots.	T-6020 T-6040

TABLE III
Security Objectives of Service Robotics System

Objective ID	Requirement ID	Requirements Description
O-1010	R-1010-0010	REST API must detect malformed commands
	R-1010-0020	Access to the REST API must be authenticated
	R-1010-0030	Robot firewall should block all the connection except SSH
	R-1010-0040	SSH connection should be restricted to unprivileged users
O-1020	R-1020-0010	Robot firmware should be stored in a non-erasable memory
O-1030	R-1030-0010	Network access must require authentication
	R-1030-0020	Network communication from a client with a robot must be authenticated and encrypted
O-1040	R-1040-0010	Communication from platform to robot must be authenticated and encrypted (e.g: using protocol like TLS1.2 minimum)
O-1050	R-1050-0010	Access to log information must be limited to authorized person only
O-2010	R-2010-0010	System account management (right, password, creation, deletion, ...) should be done in a central application (to avoid account / password duplication and error in duplicated right management system)
	R-2010-0020	User (or technical account) password should be at least 12 characters, with at least one upper case, lower case, number and special character)
O-2020	R-2020-0010	Network equipment should implement network access control (e.g: 802.1.X)
O-2030	R-2030-0010	Sudo account should be blocked
	R-2030-0020	Sudoers rules should be set up according to the system privileged action to perform
O-3010	R-3010-0010	Commands received by the robot should be parsed and checked using whitelist approach
	R-3010-0020	The robot should monitor its processing status (to avoid overprocessing)
O-3020	R-3020-0010	Authentication operation should be performed using cryptographic signature (at least SHA256 combined with RSA or ECC algorithms)
	R-3020-0020	Operating system integrity should be guarantee using cryptographic proof (signature) securely stored (e.g: TPM)
O-3030	R-3030-0010	File systems access must be limited to authenticated and allowed users (or technical account)
	R-3030-0020	File systems should be encrypted
O-3040	R-3040-0010	Source code and binaries should be signed to ensure their integrity
	R-3040-0020	Binaries compilation should be done using hardening arguments (memory randomization, ...)
O-3050	R-3050-0010	Software vulnerability should be managed
	R-3050-0020	Outdated packaged should be upgradable

TABLE IV
SECURITY REQUIREMENTS OF SERVICE ROBOTICS SYSTEM

VII. CONCLUSION

In this paper, we have tackled the highly vast subject of IoT systems security while concentrating on risk assessment. The proposed approach provides several advantages, including:

- It considers IoT domain model to identify all system assets.
- It follows relevant security standards to define security requirements.
- It is an iterative approach and responds to the need for evolution of IoT systems.

We have applied this methodology to a robotic system that supports the movement of loads in the warehouse. We started by identifying the critical assets and the potential threats that might compromise them. Then, we defined the technical requirements considering the identified threats and a list of security objectives extracted from a common database. All the steps of our approach was understandable and easy to follow by the case study owners and several threats related to the target infrastructure not previously considered were discovered in this study.

In the analysis performed in this paper, we have taken into account all system assets and a complete list of possible threats taken from the standards, which allows us to identify all potential risks and the requirements needed to mitigate those risks.

After the specification of security requirements, appropriate countermeasures can be deployed to protect the system against the identified risks. There are also approaches such as [26] that helps security experts to determinate impactful and adequate countermeasures considering organization defense budget.

In future work, we plan to apply our method to other systems. We also plan to support our approach with a tool that automates the various analysis activities.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union through the BRAIN-IoT project H2020-EU.2.1.1. Grant agreement ID: 780089.

REFERENCES

[1] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[3] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, Jan. 2020.

[4] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, Mar. 2019.

[5] A. Ekelhart, S. Fenz, and T. Neubauer, "Aurum: A framework for information security risk management," in *2009 42nd Hawaii International Conference on System Sciences*, 2009, pp. 1–10.

[6] F. den Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen, "Model-based security analysis in seven steps — a guided tour to the CORAS method," *BT Technology Journal*, vol. 25, no. 1, pp. 101–117, Jan. 2007. [Online]. Available: http://link.springer.com/10.1007/s10550-007-0013-9

[7] Z. Yazar, "A qualitative risk analysis and management tool–CRAMM," *SANS InfoSec Reading Room White Paper*, vol. 11, pp. 12–32, 2002.

[8] "MEHARI: MEthod for Harmonized Analysis of RIsk," 2010. [Online]. Available: https://en.wikipedia.org/wiki/MEHARI

[9] The National Cybersecurity Agency of France (ANSSI), *EBIOS 2010 - Expression of Needs and Identifiation of Security objectives.*, 2010. [Online]. Available: https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[10] ISO/IEC 27002:2013. (2013) Information technology — Security techniques — Code of practice for information security controls. [Online]. Available: https://www.iso.org/standard/54533.html

[11] AS/NZS 4360-2004. (2004) Risk management. [Online]. Available: https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/as-slash-nzs–4360-2004

[12] ISO/IEC 27005:2011. (2011) Information technology — Security techniques — Information security risk management. [Online]. Available: https://www.iso.org/standard/56742.html

[13] ISO/IEC 17799:2005. (2005) Information technology — Security techniques — Code of practice for information security management. [Online]. Available: https://www.iso.org/standard/39612.html

[14] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist special publication*, vol. 800, no. 30, pp. 800–30, 2002.

[15] K. Stouffer, J. Falco, and K. Scarfone, "Nist special publication 800-82, guide to industrial control systems (ics) security," *NIST Special Publication*, pp. 800–882, 01 2011.

[16] IEEE 1686. (2013) IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities. [Online]. Available: https://standards.ieee.org/standard/1686-2013.html

[17] I. Hwang and Y. Kim, "Analysis of Security Standardization for the Internet of Things," in *2017 International Conference on Platform Technology and Service (PlatCon)*, 2017, pp. 1–6.

[18] ISO/IEC 30128:2014. (2014) Information technology — Sensor networks — Generic Sensor Network Application Interface . [Online]. Available: https://www.iso.org/standard/53248.html

[19] ETSI TS 103 645. (2019) Cyber Security for Consumer Internet of Things .

[20] European Network and Information Security Agency, *Inventory of risk management/ risk assessment methods*, 2013. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

[21] C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0," 6 1999.

[22] Federal Office for Information Security . (2005) IT Grundschutz. [Online]. Available: http://www.bsi.de/gshb/

[23] B. F. Zahra and B. Abdelhamid, "Risk analysis in Internet of things using EBIOS," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2017, pp. 1–7.

[24] ISO/IEC 27001:2013. (2013) Information technology — Security techniques — Information security management systems — Requirements. [Online]. Available: https://www.iso.org/standard/54534.html

[25] S. Haller, A. Serbanati, M. Bauer, and F. Carrez, "A Domain Model for the Internet of Things," in *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, 2013, pp. 411–417.

[26] S. Chehida, A. Baouya, M. Bozga, and S. Bensalem, "Exploration of impactful countermeasures on iot attacks," in *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, 2020.