Asset-Driven Approach for Security Risk Assessment in IoT Systems

Salim Chehida[1(✉)], Abdelhakim Baouya[1], Diego Fernández Alonso[2],
Paul-Emmanuel Brun[3], Guillemette Massot[3], Marius Bozga[1],
and Saddek Bensalem[1]

[1] University of Grenoble Alpes, CNRS, VERIMAG, 38000 Grenoble, France
salim.chehida@univ-grenoble-alpes.fr
[2] EMALCSA, A Coruña, Spain
[3] Airbus CyberSecurity SAS, Elancourt, France

Abstract. The growth of damage caused by security issues in IoT-based systems requires the definition of a rigorous methodology allowing risks assessment and protecting the system against them. In this work, we propose an approach that follows the security standards to identify and analyse the potential risks. Our approach starts by specifying the system assets considering IoT domain model and the potential threats that might compromise them. Starting from the list of threats, we define the security objectives then technical requirements and countermeasures that can cover these objectives. We apply our approach to an IoT system for monitoring and control the management of the urban water cycle.

Keywords: Risk assessment · IoT · Asset · Threat · Security objectives · Security requirements · Countermeasures

1 Introduction

An IoT-based system consists of a collection of devices that collaborate through the Internet to provide numerous services. The capability of these devices is to achieve smart tasks while communicating between them, with users. Computer systems have permitted the integration of IoT in several applications such as (i) smart air conditioning in buildings, (ii) health monitoring for early detection of illnesses, (iii) control and optimization of energy consumption, and (iv) environmental monitoring for detection of emergencies. However, the incorporation of a large number of devices using several communication technologies and protocols leads to many security challenges. Several papers such as [11,14,15,17] have portrayed many vulnerabilities that can be exploited by attackers to circumvent the security measures and to damage IoT systems.

Security Risk Assessment (SRA) is the process that aims to improve confidence and security level by mitigating risks while covering system vulnerabilities. According to [16], SRA methods are classified in three perspectives: *Asset-driven*, *Service-driven*, and *Business-driven*. The asset-driven perspective assesses risks

J. Garcia-Alfaro et al. (Eds.): CRiSIS 2020, LNCS 12528, pp. 149–163, 2021.
https://doi.org/10.1007/978-3-030-68887-5_9

starting from the assets. Business-driven considers risks in the business processes level. The service-driven perspective uses services as an input of risk analysis. Several generic methodologies based on the different perspectives have been proposed. However, the complexity and the dynamic of IoT systems highlights the need for new approaches that allow defining a trust security policy.

In this work, we propose an asset-driven approach adapted for the security risk assessment of IoT systems. Our approach considers existing methodologies and standards for the identification of the threats associated with IoT infrastructures and the security requirements that allow dealing with these threats. Then, a set of defences is deployed to ensure requirements and protect the system against relevant risks. Among the specificities of our method compared to the other methods presented in Sect. 2: (i) It is dedicated to IoT systems and it considers the IoT domain model to identify the assets list, (ii) It follows the relevant security standards to define the security requirements and an iterative analysis approach to manage the complexity and the dynamic of IoT systems.

The rest of this paper is organized as follows. Section 2 briefly explains the main approaches proposed for SRA. Section 3 presents the different steps of our approach, and Sect. 4 applies it to assess the risk of an IoT-based system for water management infrastructure. Finally, we give our conclusions in Sect. 5.

2 State of the Art

The paper [16] presents a survey and taxonomy for SRA methods. In this section, we present the most methods and tools used in practice.

2.1 Aurum

AURUM (Automated Risk and Utility Management) method [5] supports the NIST SP 800-30 risk management standard [18]. It consists of three main steps: (i) identification of potential risks and their impacts,(ii) prioritization and implementation of adequate preventive countermeasures, and (iii) evaluation of the impact of countermeasures and whether they decrease the risks. Among the advantages of AURUM:

- It uses *Bayesian threat likelihood determination* for threat evaluation.
- It allows automated calculation of threat impacts and automated definition of controls for the risks mitigation.
- It provides interactive decision and analysis system to support risk manager investigating possible scenarios and characterizing the problems.

2.2 CORAS

CORAS [3] is a model-based risk assessment methodology. It uses the Unified Modelling Language (UML) [13] for describing the target of assessment at the hight level of abstraction, communication with different stakeholders involved in risk assessment, documenting intermediate results, and presenting the overall conclusions. The CORAS method includes seven main steps:

- Introductory meeting to discuss the overall goals of the analysis.
- High-level analysis and description of threats and vulnerabilities.
- Refinement and approval of documentation by the client.
- Identification of risk and potential unwanted incidents by people with expertise on the target of the analysis.
- Risk estimation by giving likelihood values for identified unwanted incidents.
- Evaluation and correction of identified risks with the client.
- Discussion about risk treatment and countermeasures cost and benefit.

2.3 CRAMM

CRAMM (CCTA Risk Analysis and Management Method) [21] is a tool based on qualitative risk assessment methodology proposed by *UK government's Central Computer and Telecommunications Agency* for demonstrating the need for action and justifying prioritized countermeasures at the managerial level, based on quantifiable results. CRAMM consists of the next steps:

- Initial meetings, interviews and structured questionnaires for data collection and objectives definition.
- Identification and evaluation of different assets such as data, application software and physical assets based on the impacts of breaches of confidentiality, integrity, availability and non-repudiation.
- Threat and vulnerability assessment using predefined tables for threat/asset group and threat/impact combinations.
- Risk management by providing a set of countermeasures for mitigating the identified risks.

2.4 EBIOS

EBIOS method [20] allows the assessment and treatment of risks associated with an Information System (IS) and the implementation of a security policy adapted to the needs of an organization. It groups five steps :

- The first step deals with context establishment and the relationship between the business context and the IS.
- In the second step, security requirements are determined based on feared security events.
- In the third step, a risk study is conducted in order to identify and analyze threat scenarios.
- In the fourth step, information from the previous steps is used to identify risks and describe the necessary and sufficient security goals relating to the risks.
- In the final step, the necessary security controls are determined, and any residual risk is made explicit.

2.5 MEHARI

MEHARI (MEthod for Harmonized Analysis of RIsk) [1] is a method for risk analysis of IS. It involves the following steps [19]:

- Context establishment of the entire organization or particular parts (business activity, type of asset or threat, etc.).
- Stakes analysis and assets classification as primary and secondary, according to ISO/IEC 27005 [9].
- Risk identification by collecting threats and security measures needed to reduce the risks.
- Risk analysis by providing possible risk scenarios associated with the assets and the various threats.
- Risk assessment by the quantification of risk scenarios on 4 levels and the management of the most serious scenarios.

3 BRAIN-IoT Risk Assessment Methodology

BRAIN-IoT project[1] aims to develop a framework for reducing the effort of developing, validating, operating and monitoring IoT-based systems. As part of this project, we propose a risk assessment methodology depicted in Fig. 1.

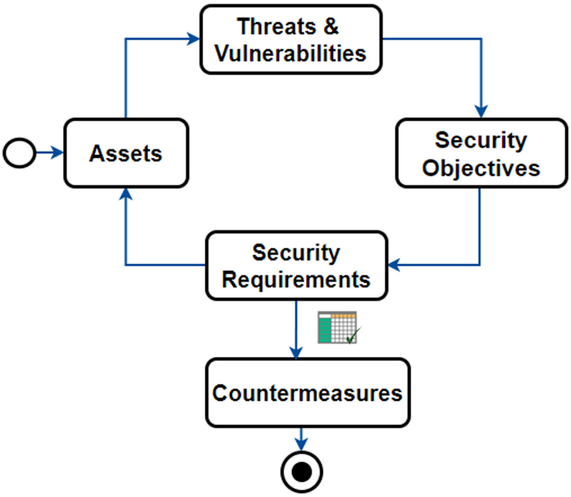

Fig. 1. BRAIN-IoT risk assessment methodology.

This method is appropriate for risk analysis of IoT systems, and it inspires the best practices from existing approaches presented in Sect. 2. Our approach

[1] http://www.brain-iot.eu/.

is iterative, and technical requirements could be refined following the refinement of the system assets. It involves the client, and the results of each phase must be checked. After validation of the requirements with the client, countermeasures are provided to protect the system against the identified risks. The next sections will detail the different steps.

3.1 Identification of Assets

The specification of assets is the first phase of our methodology. This phase plays a significant part because it is central to determine the risks. Following the ISO/IEC 27001 definition [7], an asset is "*any tangible or intangible thing or characteristic that has value to an organization*". Therefore, an asset could be in different forms, tangible or intangible, hardware or software, service or infrastructure, etc. After the identification, the assets can be evaluated using a qualitative or quantitative way. The qualitative way highlights the importance of the assets based on their security level determined by three aspects: confidentiality, integrity, and availability. The quantitative evaluation is based on the actual environment and the value of the assets.

To establish a common definition of IoT systems assets and their relationships, an IoT domain model is required. In this work, we refer to the model proposed by [6] (see Fig. 2) that allows avoiding fuzzy terminologies and helping in the risk analysis of IoT systems. This model has been developed within the IoT-A project[2], and it aims to come to a common understanding. It defines five main concepts.

(a) **User**
The user represents who interacts with a real-world object. The interaction between User and Physical Entity (PE) is carried out physically or through software interfaces and electronic devices. Users can either be humans or Active Digital Artefacts (ADA), e.g., programs embedded in manufacturing robots.

(b) **Augmented Entity (AE)**
AE is the combination (composition) of PE together with its digital representation, and it can be considered as "Thing". VE (Virtual Entity) is a kind of digital artefact that represents PE.

(c) **Device**
The device is hardware with computing capabilities. It can be physically attached to PE, or may also be in its environment. There are three types of devices. *Sensors* that allow PEs monitoring, *Actuators* that can act on PEs, and *Tags* that allow to identify PEs and can be read by sensors.

(d) **Resource**
Resources are software components that implement certain functionalities, for example: providing information about PE's, allowing the execution of actuation tasks or analysing data provided by multiple sensors. They may be hosted on a device, or they could be located anywhere in the network.

[2] http://www.iot-a.eu.

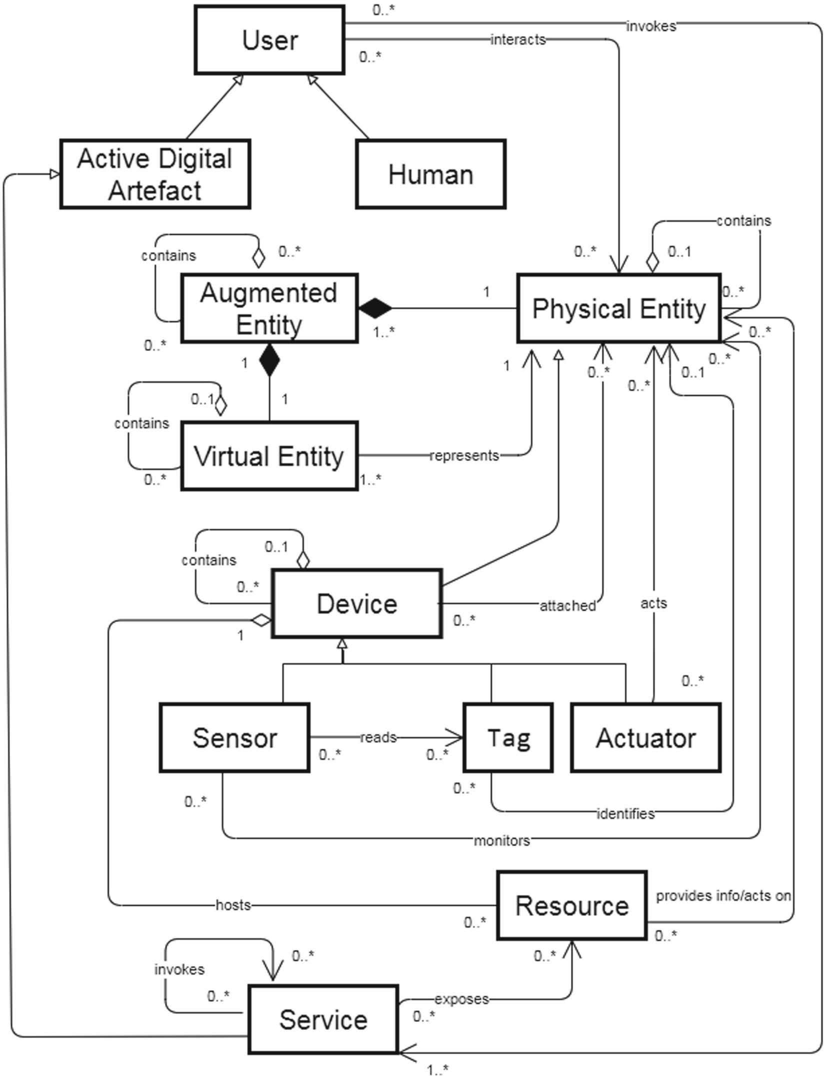

Fig. 2. Domain model for IoT.

(e) **Service**
Service exposes the resources through a common interface and makes them available for users and other services. It may also invoke other services and combine the results.

In our methodology, we rely on the IoT domain model to identify the different assets of IoT systems and to understand the correlation between them. We can also distinguish between *hardware assets*, such as the different types of devices and *software assets*, such as services, resources, and ADA. Assets should be listed in a table. We give *an ID* to the asset, which will be used in the next steps for traceability and also *a description* that provides a quick overview of the asset and its perimeter.

3.2 Threats and Vulnerabilities

According to ISO/IEC 27001 [7], a threat is a "*potential cause of an unwanted incident, which may result in harm to a system or organization*". In NISP SP800-30 [18], threat is "*a potential, for a particular threat-source, to successfully exercise a particular vulnerability*". A threat could be the result of an external and non-controllable incident or an attack on the system. Threat-sources can be categorized into environment factors or human factors.

Vulnerability refers to the openness of a system to the threats. According to [7],"*vulnerability refers to the weakness that is related to the organizations' assets, which sometimes could cause an unexpected incident*". In NISP SP800-30 [18], "*vulnerability means a flaw or weakness of the systems' security flow, design, and implementation that could lead to a security breach or violation of the security policy*". Vulnerabilities can be divided into two categories. The first type of vulnerabilities affects the asset itself, such as technical issues, system breaches, etc. The second ones are caused by insufficient organization management at a higher level [7].

A list of generic threats is provided by SRA methodologies presented in Sect. 2. In our method, we consider EBIOS database [20], which is compatible with all relevant ISO standards (13335, 15408, 17799, 31000, 27005, and 27001) and provides a complete list of possible threats (42 threats) designed to be exhaustive (see Table 1). EBIOS threat database is widely used in risk assessment. Some works like [22] have used it for risk analysis of IoT systems. In Table 1 taken from the EBIOS knowledge bases, threats are classified into eight main categories. Threat impact in terms of Availability (A), Confidentiality (C), and Integrity (I) is assessed.

In our approach, all potential threats towards the essential assets should be recognized using *threat-asset matrix* that allows the traceability of threats for each asset. The matrix should be completed and validated with the client.

3.3 Security Objectives

Security objectives are derived from threats. They are the main guideline to counter the identified threats and to satisfy the security principles. In our methodology, we consider security objectives from the standard ISO/IEC-27002 [8]. This standard gives general guidance on the commonly accepted goals of information security management. It describes general principles structured around 35 security objectives and 114 controls. The risk managers should specify security objectives that cover the full list of threats for each asset. After the

Table 1. EBIOS threat list.

Type	ID	Description	A	C	I
Physical damage	T-1010	Fire	x		x
	T-1020	Water damage	x		x
	T-1030	Pollution	x		x
	T-1040	Major accident	x		x
	T-1050	Destruction of equipment or media	x		x
Natural events	T-2010	Climatic phenomenon	x		x
	T-2020	Seismic phenomenon	x		x
	T-2030	Volcanic phenomenon	x		x
	T-2040	Meteorological phenomenon	x		x
	T-2050	Flood	x		x
Loss of essential services	T-3010	Failure of air-conditioning	x		
	T-3020	Loss of power supply	x		
	T-3030	Failure of telecommunication equipment	x		
Disturbance due to radiation	T-4010	Electromagnetic radiation	x		x
	T-4020	Thermal radiation	x		x
	T-4030	Electromagnetic pulses	x		x
Compromise of information	T-5010	Interception of compromising interference signals		x	
	T-5020	Remote spying	x	x	x
	T-5030	Eavesdropping		x	
	T-5040	Theft of media or documents		x	
	T-5050	Theft of Equipment	x	x	
	T-5060	Retrieval or recycled or discarded media		x	
	T-5070	Disclosure		x	
	T-5080	Data from untrustworthy sources	x		x
	T-5090	Tampering with hardware		x	
	T-5100	Tampering with software	x	x	x
	T-5110	Position detection		x	
Technical failures	T-6010	Equipment failure	x		
	T-6020	Equipment malfunction	x		
	T-6030	Saturation of the information system	x		
	T-6040	Software malfunction	x		x
	T-6050	Breach of information system maintainability	x		
Unauthorised actions	T-7010	Unauthorised use or equipment	x	x	x
	T-7020	Fraudulent copying of software		x	
	T-7030	Use of counterfeit or copied software	x		
	T-7040	Corruption of data		x	x
	T-7050	Illegal processing of data		x	
Compromise of functions	T-8010	Error in use	x	x	x
	T-8020	Abuse of rights	x	x	x
	T-8030	Forging of rights	x	x	x
	T-8040	Denial of actions			x
	T-8050	Breach of personnel availability	x		

identification of security objectives, a mapping of each security objective should be done with the threat list. This will help to identify any gaps in the security objective coverage. The mapping could be done with an *objectives traceability matrix*.

3.4 Security Requirements and Countermeasures

This phase provides the technical security requirements, which are a set of rules broken down into three main categories: confidentiality, integrity, and availability. Each security objective should lead to the implementation of one or more technical requirements that could be defined in the *requirements table*.

Countermeasures are mechanisms that can be deployed to defend the system, and thwart attacks exploiting its vulnerabilities. They should cover all security requirements. Several recent surveys like [15] and [14] present countermeasures for IoT systems security. They can be secure protocols, secure frameworks, authentication and encryption solutions, hardware security solutions such as TPM (Trusted Platform Module), and more. There are some approaches like [4] that can help risk managers to determinate impactful and adequate countermeasures considering organization defense budget. In [4], the *Attack-Defense Tree* (ADT) [10] is used for modeling the combination between countermeasures and attacks that can exploit the threats and vulnerabilities presented in the second phase of our approach. Then, the *Attack-Defense Strategies Exploration* tool [12] evaluates the impact of the countermeasures on the attack cost and pinpoints defense actions portraying a good balance between defenses and their provided impact on the attack cost regarding the organization's defense budget.

4 Case Study

We apply our methodology on the industrial case study of water infrastructure that manages the urban water cycle in the city of la Coruña in Spain. An IoT system controls a large number of devices dispersed in large and varied geographical sites, with numerous interactions with other elements and services related to human activities.

In our water management system, we have identified 55 assets with their associated threats, security objectives, requirements, and countermeasures. The complete study is given in the excel file at [2]. Table 2 shows examples of 11 assets. For each asset, we can have many of the same model installed in the infrastructure. We classify the assets according to the IoT domain model presented in Sect. 3.1. In Table 2, we distinguish six devices of type sensor and four devices of type actuator. The asset A-1093 is an active digital artefact.

Table 2. Water management system assets.

Asset ID	Asset description	Asset type
A-1050	Submersible probe with vented cable. Probe of hydrostatic level 0,6 BAR 10 m per cable IFM	Sensors : water level
A-1051	Ultrasonic sensor with reaching of 1.300 mm	
A-1053	MEASURING TRANSDUCER SITRANS P, FOR PRESSURE AND ABSOLUTE PRESSURE SERIES Z	Sensors : pressure
A-1054	Pressure sensor with screen (range 0 to 6 bar) PT-006-SEG14-A-ZVG/US/ /W	
A-1056	Flow meter SIEMENS SITRANS F M MAG 5000	Sensors : water flow
A-1057	NUBIS MWN65-NKOP 18337996	
A-1060	Submersible centrifuge electric pump Pedrollo MC 30/50 Series	Actuators : pumps
A-1064	Water pump speroni SCR 25/80–180 NF.0215	
A-1065	Servo control Diamant PILOT. Electric regulatory valve (identification pending)	Actuators : electric valves
A-1066	Servo control Diamant PILOT. Electric regulatory valve 24V-50/60 Hz. UP04420/19	
A-1093	SICA-MEDUSA platform that receives/send information from/to devices	ADA

In Table 3, we present threats from Table 1 related to assets presented in Table 2. Sensors and actuators are generally vulnerable to physical damage that can be caused by external events linked to the natural or industrial environment and person gaining access to equipment and causing its destruction. They are also susceptible to risks of natural events (specific climatic conditions, volcanic and meteorological phenomenons, etc.), failure of telecommunication equipment, tampering attacks, events causing equipment failure or malfunction, error in use and malicious access. There are also other threats that are related to specific devices. The SICA-MEDUSA platform is vulnerable to compromise of information and functions, technical failures, and unauthorized actions. Besides, the software infrastructure is deployed independently of the physical platform, so it is not vulnerable to environmental and physical impedances.

Table 3. Threat-asset matrix.

	A-1050	A-1051	A-1053	A-1054	A-1056	A-1057	A-1060	A-1064	A-1065	A-1066	A-1093
T-1010	X	X	X	X	X	X	X	X	X	X	
T-1020					X	X			X	X	
T-1030					X	X	X	X	X	X	
T-1040	X	X	X	X	X	X	X	X	X	X	
T-1050	X	X	X	X	X	X	X	X	X	X	
T-2010	X	X	X	X	X	X	X	X	X	X	
T-2020			X	X	X	X	X	X	X	X	
T-2030	X	X	X	X	X	X	X	X	X	X	
T-2040	X	X	X	X	X	X					
T-2050					X	X		X	X	X	
T-3010							X	X			
T-3020			X	X	X						
T-3030	X	X	X	X	X	X	X	X	X	X	
T-4010		X			X						
T-4020					X						
T-4030		X			X						
T-5010											
T-5020											
T-5030											X
T-5040											X
T-5050					X		X	X	X	X	
T-5060											X
T-5070											X
T-5080											X
T-5090	X	X	X	X	X	X	X	X	X	X	
T-5100					X						X
T-5110											
T-6010	X	X	X	X	X	X	X	X	X	X	
T-6020	X	X	X	X	X	X	X	X	X	X	
T-6030											X
T-6040					X				X		X
T-6050					X						X
T-7010											X
T-7020											X
T-7030											X
T-7040					X						X
T-7050											X
T-8010	X	X	X	X	X	X	X	X	X	X	X
T-8020	X	X	X	X	X						X
T-8030											X
T-8040											X
T-8050											

In Table 4, we provide examples of 9 security objectives, the threats they cover, and their rationale for considering them for the water management system. For instance, *network security management* objective can prevent eavesdropping, tampering attacks, and some unauthorized actions.

Table 4. Security objectives.

ID	Security objective	Security objective description	Threats
O-1020	Back-up	Back-up of data and software from water management platform should be taken and tested regularly	T-10XX
			T-20XX
O-1030	Network security management	Ensure the protection of the communication between the gateway and internet, the LAN network, the access from the outside, and to the devices	T-5030
			T-5090
			T-7010
			T-7020
			T-7040
O-1040	Security of exchanged information	Protect the exchange of information between the devices, as well as the data collected by the sensors and devices connected through the edge nodes	T-5070
			T-5080
O-1050	Monitoring	Observe and check the processes, infrastructures and logs from water management platform in order to detect unauthorized information processing	T-5030
			T-5040
			T-60xx
			T-70xx
			T-80xx
O-2010	User access management	Manage the users account information, the users passwords, and the users registration to guarantee and secure access to systems and services	T-7010
			T-7020
			T-7040
			T-8020
			T-8030
O-2020	Network access control	Protect data center, network ports, and the equipment in networks and the servers to prevent unauthorized use of networked services	T-6030
			T-70xx
O-3010	Correct processing in applications	Check the data input and the data output of water management applications in order to know that they are correct and to prevent errors and unauthorized modification	T-60xx
O-3020	Cryptographic controls	Protect the sensible information in the communication between the devices and the nodes by applying cryptographic techniques	T-8020
			T-8030
O-3030	Security of system files	The access to system files should be restricted. The infected system files should be detected	T-8020

Table 5. Security requirements and countermeasures.

SR ID	Security requirements description	Countermeasures
R-1030-0020	The access from the outside must be allowed only to authorized users and machines	VPN and DMZ (demilitarized zone) allow to reach this requirement
R-1030-0030	The communication between the gateway and internet shall be encrypted and authenticated	TLS (Transport Layer Security) allows to perform such kind of encryption and authentication
R-1030-0040	The communication point to point shall be encrypted and authenticated	SMQTT protocol integrates Attribute-Based Encryption (ABE) algorithm to secure IoT networks
R-1030-0050	Unknown devices must be unauthorized to connect to the LAN network	SRAM-PUF protocol allows to check the authenticity of devices by using unclonable device IDs
R-1030-0060	Only the system staff shall be allowed to deploy devices into the network	Authentication technology combined with TLS allow to ensure this requirement. Trust aware RPL routing protocol allows to detect malicious nodes
R-1030-0070	Computers and laptops shall have authentication system for logging	Access control technologies on computer and laptop allow to reach this requirement
R-1030-0080	If there is a file that contains the user's authentication keys this file shall be stored using a secure environment	TPM (Trusted Platform Module) allows a good security level for key protection. LEA-M encryption algorithm allows to mask secret keys Of cryptographic implementations

In Table 5, we give examples of security requirements and countermeasures that can implement *network security management* objective (O-1030). Several requirements are defined to ensure the authentication of the devices and the security of the communication between them. Also, several secure protocols such as TLS, SMQTT, and SRAM-PUF are proposed to implement security requirements. Security requirements and countermeasures implementing the other security objectives from Table 4 are given in [2].

5 Conclusion

We have presented a risk assessment methodology that follows the security standards to prevent possible threats in IoT systems. Our method provides several advantages. We relied on the IoT domain model to identify the assets of the system. We used a complete list of possible threats extracted from standards to identify all the potential risks and the requirements needed to mitigate these risks. We have followed an iterative approach that responds to the need for evolution. If the system incorporates new assets, we identify the threats related to these assets, then the requirements and countermeasures needed to prevent the identified threats.

In this paper, we have also provided the implementation of our methodology on water management infrastructure. In the analysis carried out, several threats related to the target infrastructures not previously considered were discovered in this study. We are planning in the future to apply our method to other IoT systems.

Acknowledgments. The research leading to these results has been supported by the European Union through the BRAIN-IoT project H2020-EU.2.1.1. Grant agreement ID: 780089.

References

1. MEHARI: Method for Harmonized Analysis of Risk (2010). https://en.wikipedia.org/wiki/MEHARI
2. Risk assessment in water management infrastructure (2020). https://github.com/SafetyAnalysis/Asset-driven-Approach-for-Security-Risk-Assessment-in-IoT-Systems/blob/master/EMALCSA-RiskAssessment.xlsx
3. den Braber, F., Hogganvik, I., Lund, M.S., Stølen, K., Vraalsen, F.: Model-based security analysis in seven steps – a guided tour to theCORAS method. BT Technol. J. **25**(1), 101–117 (2007). https://doi.org/10.1007/s10550-007-0013-9, http://link.springer.com/10.1007/s10550-007-0013-9
4. Chehida, S., Baouya, A., Bozga, M., Bensalem, S.: Exploration of impactful countermeasures on IoT attacks. In: 2020 9th Mediterranean Conference on Embedded Computing (MECO) (2020)
5. Ekelhart, A., Fenz, S., Neubauer, T.: AURUM: a framework for information security risk management. In: 2009 42nd Hawaii International Conference on System Sciences, pp. 1–10 (2009)
6. Haller, S., Serbanati, A., Bauer, M., Carrez, F.: 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, pp. 411–417 (2013)

7. ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements (2013). https://www.iso.org/standard/54534.html
8. ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls (2013). https://www.iso.org/standard/54533.html
9. ISO/IEC 27005:2011: Information technology – Security techniques – Information security risk management (2011). https://www.iso.org/standard/56742.html
10. Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Foundations of attack–defense trees. In: Degano, P., Etalle, S., Guttman, J. (eds.) FAST 2010. LNCS, vol. 6561, pp. 80–95. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19751-2_6
11. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Int. Things J. **4**(5), 1125–1142 (2017)
12. Mediouni, B.L., Nouri, A., Bozga, M., Legay, A., Bensalem, S.: Mitigating security risks through attack strategies exploration. In: Margaria, T., Steffen, B. (eds.) ISoLA 2018. LNCS, vol. 11245, pp. 392–413. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03421-4_25
13. Object Management Group: Unified Modeling Language (UML): Superstructure, version 2.0 (2005)
14. Radoglou Grammatikis, P.I., Sarigiannidis, P.G., Moscholios, I.D.: Securing the internet of things: challenges, threats and solutions. Internet Things **5**, 41–70 (2019). https://doi.org/10.1016/j.iot.2018.11.003
15. Sengupta, J., Ruj, S., Das Bit, S.: A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. **149**, 102481 (2020). https://doi.org/10.1016/j.jnca.2019.102481
16. Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M.: Taxonomy of information security risk assessment (ISRA). Comput. Secur. **57**, 14–30 (2016). https://doi.org/10.1016/j.cose.2015.11.001,https://linkinghub.elsevier.com/retrieve/pii/S0167404815001650
17. Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A.: Security, privacy and trust in internet of things: the road ahead. Comput. Netw. **76**, 146–164 (2015). https://doi.org/10.1016/j.comnet.2014.11.008
18. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems. Nist Spec. Publ. **800**(30), 800-830 (2002)
19. The European Union Agency for Cybersecurity: Mehari (2010). https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html
20. The National Cybersecurity Agency of France (ANSSI): EBIOS 2010 - Expression of Needs and Identifiation of Security objectives. (2010). https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
21. Yazar, Z.: A qualitative risk analysis and management tool-CRAMM. SANS InfoSec Reading Room White Paper **11**, 12–32 (2002)
22. Zahra, B.F., Abdelhamid, B.: Risk analysis in Internet of things using EBIOS. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–7. IEEE (2017)