model-Based fRamework for dependable sensing
and Actuation in INtelligent decentralized IoT systems

D5.1 - Initial Threat modeling and Security assessment of target scenarios, solutions

Deliverable ID	D5.1
Deliverable Title	Initial Threat modeling and Security assessment of target scenarios, solutions
Work Package	WP5
Dissemination Level	PUBLIC
Version	Final
Date	2018-08-07
Status	Final
Lead Editor	AIRBUS and UGA
Main Contributors	Saddek BENSALEM (UGA), Paul-Emmanuel BRUN (AIRBUS)

Published by the BRAIN-IoT Consortium

This project has received funding from the European Union’s Horizon 2020 research
and innovation programme under grant agreement No 780089.

Document History

Version	Date	Author(s)	Description
0.1	2018-06-27	Paul-Emmanuel Brun	Added methodology description
0.2	2018-07-06	Saddek Bensalem	Input from UGA : RA key concepts + RA Standards
0.3	2018-07-19	Saddek Bensalem	Added RA methods and tools + IoT standards + references
0.4	2018-07-24	Nicolas Pabst	Minor correction and updates
0.5	2018-07-30	Diego Fernández	Added asset identification and 5.2 Threats and Vulnerabilities
0.6	2018-08-07	Miquel Cantero	Added Asset identification
0.7	2018-08-07	Diego Fernández	Tables, format and values updated
0.8	2018-08-20	Diego Fernández	Description updates
0.9	2018-09-03	Paul-Emmanuel Brun	Section 5 and section 6 minor changes
1.0	2018-09-05	Saddek Bensalem	Added Executive summary + Introduction + Conclusion+ minor updates
Final	2018-09-17	Saddek Bensalem	Updates according to reviews

Review History

Version	Review Date	Reviewer	Summary of Comments
1.0	2018-09-11	Enrico Ferrera, Davide Conzon (ISMB)	Approved with minor comments.
1.0	2018-09-10	Mario Diaz Nava (STMicroelectronics)	Approved with minor comments.

Executive Summary

The present document is a deliverable of the BRAIN-IoT project, funded by the European Commission, under its Horizon 2020 Research and innovation program (H2020), reporting the results of the activities carried out by WP5 – End-to-end Security, Privacy and Trust Enablers. The main objective of the BRAIN-IoT project is to focus on complex scenarios, where sensing, actuation and control are cooperatively supported by populations of heterogeneous IoT systems. In such a complex context, many initiatives fall into the temptation of developing new IoT platforms, protocols, models or tools aiming to deliver the ultimate solution that will solve all the IoT challenges and become "the" reference IoT platform or standard. Instead, usually they result in the creation of "yet-another" IoT solution or standard. More specifically, the project revolves around two vision scenarios; Service Robotics and Critical Infrastructure Management. The scenarios were outlined in the proposal and are refined within the engineering efforts alongside the project, driven by WP2.

Deliverable D5.1 is compiled with a collaborative effort of all partners who actively participated in the task 5.1 – Threat Modeling and Assessment. This document reports on the initial threat modeling and security assessment of the BRAIN-IoT proposed scenarios and the followed security methodology which is based on known threats analyzed by international initiatives undergoing in the EU and worldwide. Starting from the scenarios and architectural solutions defined by WP2, the authors performed an initial analysis considering intentional threats that may result in BRAIN-IoT services to be compromised or disrupted.

The work presented in this deliverable should be seen as preliminary results which the project will evolve. It will be updated in the deliverable D5.4 and the final results will be documented in D5.5.

Table of Contents

Document History ... 2
Review History ... 2
Executive Summary ... 3
Table of Contents ... 4
1 Introduction ... 5
1.1 Related documents ... 5
2 Risk assessment key concepts and scope ... 6
2.1 Risk identification ... 6
2.2 Assets ... 7
2.3 Threats ... 8
2.4 Vulnerabilities ... 8
2.5 Risk analysis ... 8
2.6 Risk evaluation ... 8
3 Risk assessment methods, standards and tools ... 10
3.1 Standards ... 10
3.2 Risk Assessment Methods and Tools ... 12
4 BRAIN-IoT approach ... 16
4.1 Methodology overview ... 16
4.2 Asset Identification ... 16
4.3 Threats and Vulnerabilities ... 17
4.4 Security Objectives ... 22
4.5 Security Requirements ... 23
5 Critical Infrastructure Management Use Case Risk assessment ... 24
5.1 Asset Identification (Software and Hardware) ... 24
5.2 Threats and Vulnerabilities ... 24
6 Service Robotics Use Case: Risk assessment ... 28
6.1 Asset Identification (Software and Hardware) ... 28
6.2 Threats and Vulnerabilities ... 28
7 Conclusions ... 30
Acronyms ... 31
List of figures ... 32
List of tables ... 33
References ... 34

1 Introduction

This deliverable presents the results of Task 5.1 *Threat Modelling and Assessment*. The purpose of this deliverable is to analyse scenarios defined in WP2 , more specifically in D2.1, in terms of security risks and countermeasures needed to protect the sensitive features as well as data exchanged using the BRAIN-IoT solutions respecting the privacy of its users. The considered use cases are the **Service Robotics** and the **Critical Water Infrastructure**.

This document describes the BRAIN-IoT security assessment methodology, the activities and the concepts to support it, i.e., risk identification, risk analysis and risk evaluation. It overviews existing risk assessment approaches and standards relevant to the BRAIN-IoT project and provides a first risk assessment of the project use cases. This methodology, along with the initial analysis of use cases, will guide the upcoming phases, and therefore, this deliverable will be a common reference point for the BRAIN-IoT consortium with respect to security assessment. This deliverable focuses on the definition of the risk assessment methodology which will be used during the project and provides an initial risk assessment of the use cases as an illustration of the first phases of the methodology, namely, the identification of critical assets and associated threats.

The main activities performed by Task 5.1 so far are the following:

- Definition of a risk assessment methodology;
- Study of the state of the art;
- An initial risk assessment of the project use cases;

The ultimate objectives are the identification of the security objectives and the associated technical requirements towards proposing adequate counter-measures to protect the BRAIN-IoT system.

Deliverable D5.1 will be continuously updated and refined through an iterative process that will lead to the production of two additional deliverables; D5.4 Updated Threat modelling and Security assessment of target scenarios, solutions planned on month M16 and D5.5 Final Threat modelling and Security assessment of target scenarios, solutions panned on M26. UGA is in charge to coordinate this deliverable with contributions from AIRBUS, EMALCSA and Robotnik.

1.1 Related documents

ID	Title	Reference	Version	Date
D2.1	Initial Visions, Scenarios and Use Cases		1.1	2018-06-04

2 Risk assessment key concepts and scope

Following many risk management standards, such as ISO 27005 and ISO 31010, the risk assessment process is not an isolated procedure but depends on the context of the risk management process, something that requires pre-analysis, post-countermeasures and continuous coordination, monitoring and feedback. Figure 1 shows the risk assessment structure and its relationship with risk management.

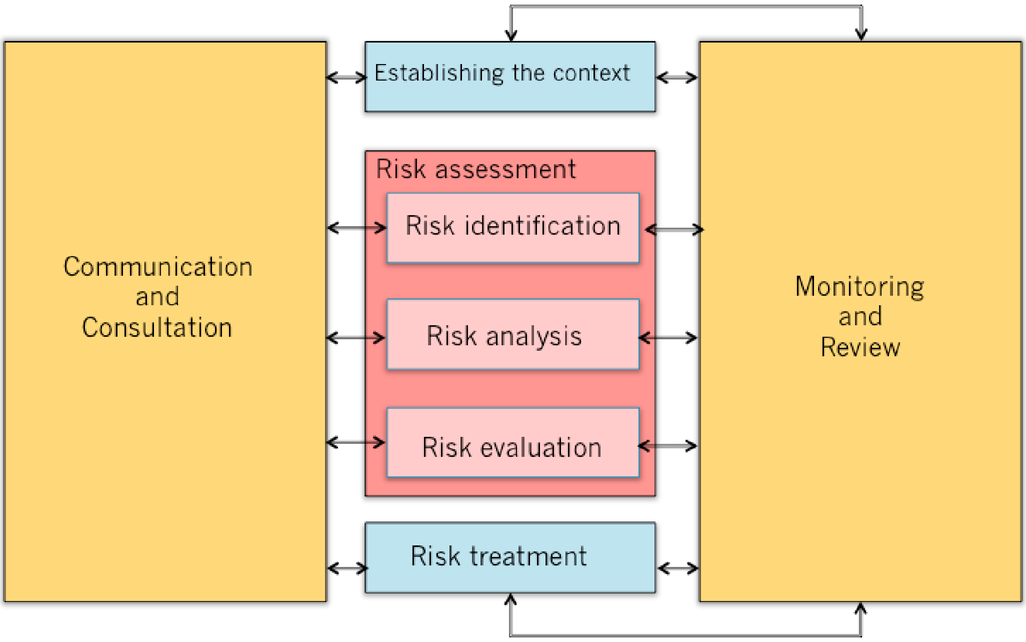

Figure 1 Risk assessment and relation with risk management process

The following paragraphs present the key concepts available in the literature.

2.1 Risk identification

Risk identification is the process of finding, recognizing and recording risks [1]. According to [2], Risk can be described as a function of three variables: *threats, vulnerabilities* and *assets value*. The external influence is *threat*, and internal influence is *vulnerability*. They act as input and source of the security incident. The final consequence also depends on the asset value and environment. So these three variables will be used as the basic input for a function that assesses risks **R = f(a,t,v)**, where :

- 'a' represents the assets value,
- 't' represents the likelihood that the threat will occur, and
- 'v' represents the number of the vulnerabilities a system contains.

There are other definitions of the concept of risk. For example, in [3], the authors consider risk as the combined effect of asset, threat type, threat source, vulnerability and countermeasure. Since most interpretations are expanded version of the basic three elements of risks, in this deliverable, the authors will use the basic triplet to evaluate risk.

2.2 Assets

In information systems, the assets value is the worth of property for the organization, which is in danger. The assets can exist in different forms, tangible or intangible, hardware or software, service or infrastructure, etc. There are three parts of information assets that must be considered: the information itself, the facilities that deals with information, and the people who deal with the information. The information itself will be the core part to consider in assessing the assets of the information systems. Categorization of the assets in order to carry out more efficient risk assessment is also important. According to [3], the assets can be categorized based on usage, e.g. information assets, software assets, human assets, intangible assets, etc.

Assets identification in risk assessment is a prior step to assessing the value. An important issue is to identify a large number of assets, and the correlation between them. During the first round of assessing, it should be conducted as thoroughly, in order to identify all the assets. Then the important assets and segments of the system can also be identified, in an assets table [4].

After the identification of assets they need to be evaluated, in order to achieve a categorization of assets. The evaluation can be done in qualitative or quantitative way. The qualitative way is to identify the importance of the assets, based on their security level determined by three aspects: *confidentiality, integrity* and *availability*. The quantitative way for evaluating the assets is based on the actual environment and the value of the assets.

- For Qualitative analysis the risk level is usually described in words or scales. It is normally based on previous survey records, employees' experiences, and experts opinions. The data is gathered from surgery or interview around the organization, then use the data to analyze the threats, weakness and control aspects towards the organization to quantify the existing risks. Qualitative methods are useful in situations when the analyzer did not have enough information or do not have qualified conditions to apply mathematic and statistic methods to the risk model. It can identify the risk in high, middle, low level without drawn into analysis of different figures of the organization's operational data. Also, it makes it easier for professional employers without much risk knowledge background to participate in the analysis process. On the negative side, qualitative analysis usually lacks the support of figures. It mainly relies on subjective judgment, i.e. on like analyzer's experience and can not offer very objective decisions.

- Quantitative analysis uses mathematical and statistic methods to convert the risk information gathered at previous stages into a measureable value. It supports the risk analysis result with quantitative value and standard, so that the objective result (compared to qualitative method) is more dependable and easy to accept and understand. But the process is usually very complicated and time consuming. There are various methods and standards to gather data and to calculate the quantitative value of risks, and they usually have very high requirement on the accuracy and integrity of the data that being collected for the analysis. So usually it is quite impossible to quantify the whole process of the risk assessment.

It is hard to judge whether quantitative or qualitative method is better, we need different approaches in different situations. Under the same budget and time consideration, user would want the assessed result to be as accurate and convincing as possible. If we can have data to prove that, even though it might cost more time, and data itself in some situation is hard to collect or difficult to standardize, we would still consider that quantitative results would be more dependable and trustworthy than qualitative result. In the situation that a quantitative result is not the priority, we can lower the weight of this factor to minimize the influence of it in the decision process.

2.3 Threats

Threats refer to those events that cause harm to information systems in general. More precisely, according to NISP SP900-30 [1] a threat is a potential, for a particular threat-source, to successfully exercise a particular vulnerability. There are three aspects to consider in threat likelihood: threat-source, potential vulnerabilities, and existing controls. To identify threat-sources, all potential threats towards the important assets should be recognized. Threat-sources can be categorized into environment factors or human factors. Environment factors such as earthquake or flood cannot be avoided. User should always consider environment threats according to their operation environment even if it is difficult to consider them. Meanwhile human factors are more of our concern because they are vagrant regarding to different people and different situations, and it is more difficult to predict human behavior than regular nature disasters.

The existing form of a threat can be a direct or indirect attack against the systems, such as unauthorised modification, leaking, etc, that leads to violation of the confidentiality, integrity or availability of the system, or an unintentionally incident. In NIST SP300-30, the human factors threats are listed as source, motivation, and threat actions.

The following three aspects should be considered to quantify the likelihood of threats:

- Statistics of threats in previous security reports;
- Collection of data in a practical environment, using intrusion detection tools, by checking the log files or other methods;
- Reference of authoritative sources that have a database of the popular threats.

2.4 Vulnerabilities

Vulnerability refers to the openness of an information system to the threats. System vulnerabilities are usually exploited by the identified potential threats. In [4], vulnerability refers to the weakness that is related to the organizations' assets, which sometimes could cause an unexpected incident. In [1], vulnerability means flaw or weakness of the systems' security flow, design and implementation that could lead to 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 in higher level [4]. Vulnerabilities and threats can be identified through documents auditions, people's interviews and questionnaires, on-site inspection, vulnerability scanner, etc. [5].

2.5 Risk analysis

According to the ISO 27000 definition [6], risk analysis (RA) is the process of comprehending the nature of risk and to determine the level of risk. The risk analysis definition explains that the nature of risk is the cause and the source. Then, from the cause and the source it is possible to identify and locate the risks. Different risks being identified in the RA process requires quantitative or qualitative methods to compare and decide the priorities. This will lead to a priority table of different risks after analysis, and it would provide a database for the next step risk evaluation and mitigation.

2.6 Risk evaluation

After the analysis of the risks, which usually is in the form of quantified or qualified risks list, the results should be compared with the given risk criteria, which is the reference for severity. The risk criteria can include cost-benefits, laws and regulation, economic and social environment, human factors, etc. With the comparison to a standard reference, it is easier for users to evaluate risks and take countermeasures under different circumstances. For taking actions against different levels of risk in various environments, there are four basic approaches [7]:

- Mitigate the risks, such as patch the system;
- Transfer the risks, such as outcome the unfamiliar operations to professionals;
- Avoid the risks, such as isolate internal network from outside network;
- Accept risks, if the potential risk consequences are acceptable under certain situation.

3 Risk assessment methods, standards and tools

Different risk analysis methods, techniques and tools are used for the security risk analysis and assessment process. In this section we give an overview of risk analysis methods, tools and standards.

3.1 Standards

Security standards guide and enforce a common level of security capability across an industry. Compliance with a standard requires taking steps to achieve the prescribed alignment, theoretically avoiding financial or other penalties for deviations from the standard's requirements. Standards rarely govern implementations, so a solution may be compliant with the standard, but the resulting security posture may not be optimal. Design tradeoffs may also be necessary between levels of compliance and cost, ease of operation, maintainability and interoperability.

The objective of securing IoT systems is to address their availability, integrity and confidentiality requirements. The realization of an adequately secure environment should be guided by a series of informed decisions, intended to ensure that the identified threats, vulnerabilities and countermeasures are commensurate with an acceptable level of risk. Security standards compliance is intended to guide an organization in best security practices, but it does not imply that the organization's products will be free of vulnerabilities or impenetrable to exploit.

3.1.1 Common Standards

Many countries and organizations have established the risk assessment audit standards such as CC, SSE, CMM, ISO/IEC 1799, BS 7799, ISO 13335, IATF, and GB/T. Audit methodologies, especially within IT environments, and related governance and quality standards include ISA, COBIT, ITIL, ISO9000, and ISAE 3402, while standards for internal audit and external assessment against adopted standards include ISAE 3402, ISAE 3000, COBIT, and ISO 9001.

There are already standards, which are commonly accepted and publicly available. In the following, the authors give briefly a description of the standards in use at this time.

- **AS/NZS 4360**: The joint Australian/New Zealand 4360:1999 Risk management standard provides generic framework for establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk. It originated as AS/NZS 4360:1995, with Second edition 1999, and Third edition in 2004. Detailed information about this joint Australian/New Zealand Standard can be found from the Standards Web site [1] or Standards New Zealand web site [2]. The AS/NZS 4360 risk management process has the following steps [3]: i) establish the context, ii) risk identification, iii) risk analysis, iv) risk evaluation, v) risk treatment, vi) monitoring and review, and vii) communication and consultation.

- **BS7799 (ISO17799)**: The BS7799 (British Standard 7799: Code of Practice for information Security Management), evolved into ISO17799 – The Information Security Standard. BS7799 Part 1 becomes ISO 1799, then ISO 27002, while BS7799 Part 2 remains a British Standard only and 'forms the basis for an assessment of the Information Security Management System (ISMS) of the whole, or part, of an organization [3] . BS7799 (BS7799-2:2005), which now the international number ISO 27001:2005, is the international best practice information security management standard, defining and guiding ISMS development.

[1] www.standards.com.au

[2] www.standards.co.nz

[3] http://www.itgovernance.co.uk/bs7799.aspx

- **NIST SP 800-30**: The NIST SP 800-30 (Special Publications Risk Management Guide for Information Technology Systems) 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) and how risk assessment and other organizational risk management processes complement and inform each other. It also provides guidance on identifying risk factors to monitor on an ongoing basis so that organizations can determine whether levels of risk have increased to unacceptable levels (i.e., exceeding organizational risk tolerance) and different courses of action should be taken. National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the US Department of Commerce.

There are nine steps for risk analysis in the NIST SP 800-30: i) system characterization, ii) threat identification, iii) vulnerability identification, iv) control analysis, v) likelihood determination, vi) impact analysis, vii) risk determination, viii) control recommendations, and ix) results documentation.

- **NIST SP 800-82**: The NIST-800-82 'revision 2' provides guidance 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). Performance, reliability and safety requirements are also considered. Comprehensive security controls, presented in this document, map to additional NIST recommendations such as those listed in SP 800-53, 'Recommended Security Controls for Federal Information Systems and Organizations [16].

- **IEEE 1686**: The IEEE 1686 'Standard for Intelligent Electronic Devices Cyber Security Capabilities' [25] 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.

- **ISO/IEC standards**: There are many ISO/IEC standards related to security. However, The ISO/IEC standards that relevant to either risk assessment and/or risk management are:

    - **ISO/IEC 27002**: ISO/IEC 27002 is the common name for a comprehensive set of best practices used in establishing and managing ISMS. It describes and establishes guidelines and general principles for initiating the 36 control objectives and 133 controls outlined. It provides general guidance on the commonly accepted goals of information security management.

    - **ISO/IEC 27005**: ISO/IEC 27005 (Information Technology – Security – Information Security Risk Management) is an International standard that provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of an ISMS according to [4] but does not provide any specific methodology for information security risk management. The standard describes the information security risk management process, which consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.

3.1.2 Cloud Security Standards

There are a great number of guidelines and standards pertaining to cloud security, devised and used in various countries. The authors briefly describe a few notable ones below.

- **ISO/IEC 27017**: The ISO/IEC 27017 standard provides guidance on the information security elements of cloud computing. It assists with the implementation of cloud-specific information security controls, supplementing the guidance in ISO 27000 series standards, including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO 27nnn standards [17], [23], [24] and [18].

- NIST has also published the following standards on cloud computing: NIST SP 800-146, 'Cloud Computing Synopsis and Recommendations', NIST SP 500-291, 'Cloud Computing Standards Roadmap', NIST SP 800-144, 'Guidelines on Security & Privacy in Public Cloud Computing', NIST SP 500-292, 'Cloud Computing Reference Architecture' and NIST SP 500-293, 'US Cloud Computing Technology Roadmap' [21], [20], [14] and [15].

- European Union Agency for Network and Information Security (ENISA) has published an auditable standard titled 'Cloud Computing: Benefits, risks and recommendations for information security [5] to which many cloud providers are certified.

- 'Cloud Computing Security Considerations [26] by the Australian Signals Directorate provides analysis and measurement of risk that will be considered by cloud Software as a Service (SaaS) customers when evaluating the cloud as a potential solution.

- Cloud Security Alliance has published many guidelines, including: 'Security Guidance for Critical Areas of Focus in Cloud Computing Version 3.0,' [27] that contains practical, current guidance and advice for both cloud computing customers and providers.

- 'Practices for Secure Development of Cloud Applications' [26] provides practical guidance relevant to cloud SaaS such as secure design recommendations for multi-tenancy and data encryption, and secure implementation recommendations for securing APIs.

3.2 Risk Assessment Methods and Tools

Due to the very large and diverse methods to Risk Assessment, this section contains a survey of the relevant methods and tools used in practice,

- **EBIOS Method and Tool**: Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) allows to evaluate and act on risks relative to information systems security, and proposes a security policy adapted to needs of an organization. The risk assessment method was originally developed by the Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), a department of the French Ministry of Defense. Now, it is maintained by a private club of experts from various fields and origins (Club EBIOS) [11]. The goal of the EBIOS method is the assessment and treatment of risks associated with an Information System (IS) in order to support management-level decision-making and to create a common ground for security discussion between various stakeholders. There are five steps for risk analysis in the EBIOS : i) The first phase deals with context establishment, the relationship between the business context and the IS (contribution to business goals, boundary, decomposition), ii) In the second phase, security requirements are determined based on feared security events, iii) In the third phase, a risk study conducted in order to identify and analyze threat scenarios, iv) In the fourth phase, information from the previous steps is used to identify risks and describe the necessary and sufficient security goals relating to these risks, v) In the final phase, the necessary security controls are determined, and any residual risk is made explicit.

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 [12].

EBIOS can be used either in the design or against existing systems [10]. Instead of a scenario-based risk analysis, EBIOS goes for a more structured approach, allowing a more exhaustive analysis through the identification of various sub-components or causes of risk (e.g. entities, vulnerabilities, attack methods, threat agents, etc). The different phases presented above can be also applied somewhat independently, allowing for only certain parts of the analysis to be (re)done, e.g. vulnerability analysis [10].

The EBIOS method is compatible with all relevant ISO standards (13335, 15408, 17799, 31000, 27005, 27001) [11]. Furthermore, the method is supported by a dedicated tool developed by Central Information Security Division (French government). The EBIOS tool helps the user to produce all risk analysis and management steps according the five EBIOS phases methods and allows all the study results to be recorded and the required summary documents to be produced. The tool is capable of matching a threat with relevant vulnerabilities and even building up risk scenarios automatically [13].

- **IT Grundschutz Method**: IT Grundschutz is part of series of standards published by the German Federal Office for Information Security (BSI) describing « methods, processes, procedures, approaches and measures relating to information security » [8]. The goal of the IT Grundschutz risk assessment is to provide a qualitative method for identification, analysis and evaluation of security incidents that might be damaging to the business, that is also consistent and usable with the rest of the standard, and be applied efficiently. The IT Grundschutz 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. For companies implementing a Security Management System based on IT Grundschutz, the risk assessment is done by using the IT Grundschutz Catalogs. These contain repositories of common threats scenarios and standard security countermeasures applicable to most IT environments, and grouped by modules corresponding to various business environments and Information System components. A supplementary risk analysis based on IT Grundschutz can also be performed by taking the following steps [9]: i) prepare an overview of threats, ii) determine additional threats, iii) assess the threats, iv) select safeguards for handling risks, v) consolidate results. The main body of the IT Grundschutz method does not describe a specific risk assessment, but instead gives suggestions for safeguard appropriate for typical business processes, applications and IT systems that have normal security requirements. As such, typical IT assets and components are described, including organizational, infrastructural and personnel aspects, potential threats are enumerated and necessary countermeasures suggested. In order to identify basic deficiencies in the IT security of the target system and achieve basic compliance with the IT Grundschutz method, the relevant modules are selected and applied to each aspect of the information System. This allows for a fast and cost-effective way of achieving a reasonable level of security.

However, the standard also describes in detail a process it calls "Supplementary Risk Analysis" that is used in contexts that differ significantly from standard IT security application scenarios and requirements. It is the responsibility of the (IT) management to decide whether or not such a supplementary analysis is warranted and for which assets or components.

IT Grundschutz is designed to be compatible with established Information Security standard ISO/IEC 27002 Although it is not the indented purpose, the IT Grundschutz methodology can be used to show compliance to this standard.

The two-tiered approach means that the IT Grundschutz method can be useful for SME's trying to achieve 'good enough" security with limited resources, while also allowing scaling up to full-fledged, customized Information Security Risk Management system, suitable for large companies with extraordinary security requirements.

- **MEHARI Method**: MEHARI (Méthode Harmonisée d'Analyse des Risques – Harmonized Risk Analysis Method) is a method for risk analysis and risk management by CLUSIF (French association of information security professionals) [4]. The general step of MEHARI consists of the analysis of the security stakes and the preliminary classification of the IS entities according to three basic security criteria (confidentiality, integrity, availability). The typical MAHARI process is the following: i) Involved parts list the dysfunctions having a direct impact on organization activity, ii) Then, audits are carried out to identity potential IS vulnerabilities, and iii) Finally, the risk analysis itself is carried out.

MAHARI complies by design with ISO 13335, in order to manage risks. This method can take part in a stage of the ISMS model promoted by ISO 27001.

- **COBIT**: Control Objectives for Information and related Technology (COBIT) IT control framework, created by the Information System Audit and Control Association (ISACA) [5]. COBIT is a major information security governance model that provides a set of generally accepted measures, indicators, processes, and best practices for the use, governance, and control of information technology [6]. COBIT can be illustrated by a process model that subdivides IT into four domains (Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate) and 34 processes in line with the responsibility areas of plan, build, run and monitor, and has been aligned and harmonized with other, more detailed IT standards and good practices such ISO 27000.

- **OWASP Risk Rating Methodology**: It stands for the Open Web Application Security Project (OWASP), and is a non-profit community comprised of private organization, educational institutions and private individuals aiming at developing at improving the security of software. The OWASP approach mostly geared towards software products and less towards Information Systems and enterprise-wide security. However, the framework does describe a decomposition of Risk into driving factors as well as describe a method for computing Risk in their OWASP Risk Rating Methodology [22]. The decomposition is, in theory, applicable to a IS as well as complex software applications.

The OWASP methodology follows a traditional conceptualization of Risk as Likelihood versus impact and suggests the following decomposition of risk:

- Threat Agent Factors: **Skill level** of Threat Agent, **Motive** is influenced by the reward the Threat Agent is hopping to receive, **Opportunity** reflects the amount of resources required for the Treat Agent to succeed in the Attack, **Size** of the group of Threat Agents seeking goals w.r.t. the system.
- Vulnerability Factors: **Ease of discovery** or how easy is it to discover a certain vulnerability, **Ease to exploit** or how easy is it to exploit certain vulnerability, **Awareness** or how well known is a particular

[4] http://en.wikipedia.org/wiki/Mahari
[5] http://www.isaca.org/knowledge-Center/COBIT/Pages/Overview.aspx
[6] www.isaca.org/Template.cfm?Section=CONIT6

vulnerability to this group of threat agents, **Intrusion detection** or how likely is it detect attack attempts.

Impact is determined by:

- Technical Impact Factors (Loss of confidentiality, Loss of integrity, loss of availability, Loss of accountability).
- Business Impact Factors (Financial damage, Reputation damage, Non-compliance damage, Privacy violation).

While the methodology suggests the above factors, it is also very clear on the fact that particular organizations might wish to augment the pre-defined set factors by adding ones that are important to the organization. Furthermore, weights can be applied to each factor on the significance it carries for the particular business model.

It is also obvious that this methodology also employs a Likelihood X Impact approach with Vulnerability again being viewed as a factor of likelihood.

4 BRAIN-IoT approach

4.1 Methodology overview

In order to build a modular and secure BRAIN-IoT architecture considering the use case contexts, BRAIN-IoT partners aims at performing a risk assessment to identify security requirements that need to be implemented in order to reach the security objectives for each use case.
This risk assessment is limited to the BRAIN-IoT scope for each use case, which is dealing with:

- IoT devices
- IoT platforms

External systems (such as the OT for critical water management use case), are not in the scope of this risk assessment.

The proposed risk assessment methodology is depicted in Figure 2 below. First, the assets are identified, based on the use cases description from D2.1. Then, threats on the system and the assets are identified, based on common threats databases (EBIOS, OWASP, etc.). Thirdly, security objectives are derived from the threats, to identify security level targeted for each environment. Finally, Security technical requirements are built in order to implement the security objectives to counter the threats identified.

This methodology is iterative, and technical requirements could be refined following the refinement of use case assets and its impact on the BRAIN-IoT architecture.

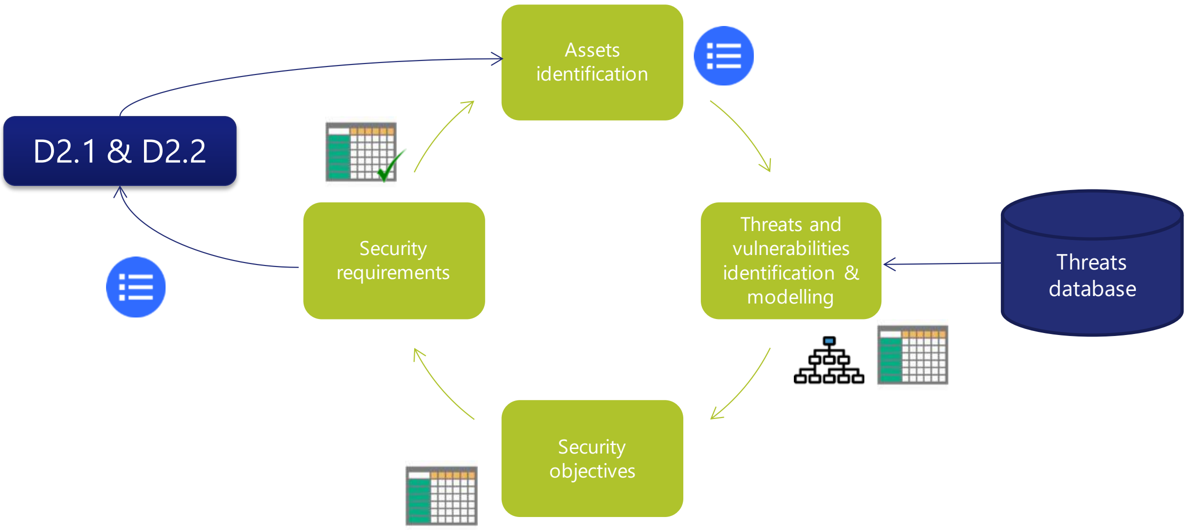

Figure 2: Risk assessment methodology

4.2 Asset Identification

Following the ISO27001 definition, an asset is "any tangible or intangible thing or characteristic that has value to an organization". Therefore, an asset could be:

- A software (e.g., an operating system)
- A hardware (e.g., a sensor, CPU, memory, etc.)
- A data (e.g., sensor status transmitted over a network, robot location in memory, etc.)

Asset identification should be listed using Table 1 below. This table gives an ID to the asset, which will be used in the next steps for traceability and a description which should give a quick overview of the asset and its perimeter (e.g.: "Operating System of robot" or "hardware motion sensor of robot").

Use Case 1	
ID	Description
A-1010	Robot Operating system
A-1020	FMS
A-1030	Lift PLC software
A-1040	Opening order

Table 1: Example of assets list

Assets could be classified based on the impact on the whole system safety and security if a corruption occurs. This classification could help to identify the level of security objective.

4.3 Threats and Vulnerabilities

Following the ISO27001 definition, a threat is a "potential cause of an unwanted incident, which may result in harm to a system or organization". A threat could be the result of an external and non-controllable incident, or an attack on the system. Following the French EBIOS methodology, threats are classified into 8 main categories:

- Physical damage
- Natural events
- Loss of essential services
- Disturbance due to radiation
- Compromise of information
- Technical failures
- Unauthorized actions
- Compromise of functions

In order to be able to derive security objective, the threat impact in terms of Availability (A), Confidentiality (C) and Integrity (I) is assessed. The full list is available in the Table 2 .

Type	ID	Description	A	C	I	Description
Physical damage	T-1010	Fire	x		x	Concentration of flammable or explosive materials in a confined environment, catching fire through an external event or internal accident. Terrorists or vandals gaining access to property in order to set light to flammable or explosive materials directly or indirectly (incendiary bombs, tampering with ventilation devices, etc.).
	T-1020	Water damage	x		x	Flood due to a leak or burst pipe. Terrorists or vandals gaining access to the property to cause flooding in the rooms.
	T-1030	Pollution	x		x	Presence of dust, vapours, corrosive or toxic gases in the ambient air. Deliberate pollution of the ambient air by tampering with air-conditioning devices or placing a source of pollution in the rooms.

	T-1040	Major Accident	x		x	External event or damage linked to the natural or industrial environment close to the assets and capable of causing them very serious physical damage. External event or damage linked to an act of vandalism or terrorism close to the assets capable of causing them very serious physical damage.
	T-1050	Destruction of equipment or media	x		x	Negligence or accidental event causing destruction of equipment or media. Person gaining access to equipment and causing its destruction.
Natural events	T-2010	Climatic Phenomenon	x		x	Specific climatic conditions (at operating limits of the equipment).
	T-2020	Seismic Phenomenon	x		x	Earth tremor or earthquake causing extreme vibration or triggering a disaster (tidal wave).
	T-2030	Volcanic Phenomenon	x		x	Volcanic eruption causing vibrations or triggering another disaster (tidal wave).
	T-2040	Meteorological Phenomenon	x		x	Isolated atmospheric disturbance causing extreme climatic conditions. A saboteur gains access to lightning protection devices.
	T-2050	Flood	x		x	River, watercourse or underground water table causing periodic or exceptional flooding of land close by.
Loss of essential services	T-3010	Failure of air-conditioning	x			Failure, shutdown or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction or fail completely. A person can sabotage the equipment used to operate the air-conditioning system (cut off the water or power supply, destroy the system).
	T-3020	Loss of power supply	x			Failure, shutdown or incorrect sizing of the power supply to the assets arising either from the supplier's service or from the internal distribution system. Sabotage or disturbance of the electrical installation by someone gaining access to the equipment (head-end, low voltage transformer, inverter, etc.)
	T-3030	Failure of telecommunication equipment	x			Disturbance, shutdown or incorrect sizing of telecommunications services (telephone, Internet access, Internet network). Sabotage or disturbance of the Telecom installation by someone gaining access to the telecommunications equipment (head-end, PABX, distribution frame, external cables, etc.)
Disturbance due to radiation	T-4010	Electromagnetic radiation	x		x	Electromagnetic interference from an internal or external device. Person using stray radiation to jam or saturate communications or disturb the operation of an appliance.
	T-4020	thermal radiation	x		x	Thermal effect caused by damage or exceptional weather conditions. Device causing a thermal effect resulting in malfunction or destruction of equipment.
	T-4030	Electromagnetic pulses	x		x	Damage causing an exceptional electromagnetic effect. Electromagnetic pulses from nuclear sources.

Compromise of information	T-5010	Interception of compromising interference signals		x		Interfering signals from an electromagnetic source emitted by the equipment (by conduction on the electrical power supply cables or earth wires or by radiation in free space). Capture of these signals depends on the distance to the targeted equipment or the possibility of connecting to cables or any other conductor passing close to the equipment (coupling phenomenon).
	T-5020	remote spying	x	x	x	Personnel actions observable from a distance.
	T-5030	eavesdropping		x		Someone connected to communication equipment or media or located inside the transmission coverage boundaries of a communication can use equipment, which may be very expensive, to listen to, save and analyse the information transmitted (voice or data).
	T-5040	Theft of media or documents		x		Someone inside or outside the organization accessing digital media or paper documents with the intention of stealing and using the information on them.
	T-5050	Theft of Equipment	x	x		Someone inside or outside the organization accessing equipment located on the premises or transported outside, out of greed or for strategic reasons.
	T-5060	Retrieval or recycled or discarded media		x		Retrieval of electronic media (hard discs, floppy discs, back-up cartridges, USB keys, ZIP discs, removable hard discs, etc.) or paper copies (lists, incomplete print-outs, messages, etc.) intended for recycling and containing retrievable information.
	T-5070	disclosure		x		Someone inside the organization who, through negligence, passes information to others in the organization who have no need to know or to the outside (the latter case usually having greater consequences). Someone knowingly passing on information inside the organization to others who have no need to know or to the outside (the latter case usually having greater consequences).
	T-5080	data from untrustworthy sources	x		x	Receiving false data or unsuitable equipment from outside sources and using them in the organization. Someone transmitting false information for integration in the information system with the intention of misinforming the recipient and attacking the reliability of the system or validity of its information.
	T-5090	Tampering with hardware		x		Someone with access to a communication medium or equipment installs an interception or destruction device in it.
	T-5100	Tampering with software	x	x	x	Unintentional action involving software carried out from inside or outside the organization and resulting in corruption or destruction of programs or data, impaired operation of the resource or even execution of commands in a user's name without his/her knowledge. The attacker introduces a program or commands in order to modify the behaviour of a program or add an unauthorised service to an operating system. This threat agent may act on the information system during the design, pre-production, production, operating, transport or maintenance phase.

	T-5110	Position detection		x		Someone with access to equipment used to detect the position of an information system user.
Technical failures	T-6010	Equipment failure	x			Event causing equipment failure.
	T-6020	Equipment malfunction	x			A logical or physical event causing an equipment item to malfunction.
	T-6030	Saturation of the information system	x			Hardware, software or network resource inadequate for meeting users' needs. An attacker simulates an intense demand on resources by setting up continuous bombardment.
	T-6040	Software malfunction	x		x	Design error, installation error or operating error committed during modification causing incorrect execution.
	T-6050	Breach of information system maintainability	x			Lack of expertise in the system making retrofitting and upgrading impossible; for example, inability to correct an operating problem or respond to new needs. Someone making the system difficult, or even impossible, to upgrade.
Unauthorised actions	T-7010	Unauthorised use or equipment	x	x	x	A person inside or outside the organisation accesses the information system and uses one of its services to penetrate it, run operations or steal information.
	T-7020	Fraudulent copying of software		x		Someone inside the organisation makes fraudulent copies (also called pirated copies) of package software or in-house software.
	T-7030	use of counterfeit or copied software	x			Loss or destruction of documents proving the purchase of licences or negligence committed by installing software without paying for the licence. Someone inside the organisation makes illegal use of copied software.
	T-7040	corruption of data		x	x	Someone gains access to the communication equipment of the information system and corrupts transmission of information (by intercepting, inserting, destroying, etc.) or repeatedly attempts access until successful.
	T-7050	Illegal processing of data		x		A person carries out information processing that is forbidden by the law or a regulation.
Compromise of functions	T-8010	Error in use	x	x	x	A person commits an operating error, input error or utilisation error on hardware or software.
	T-8020	Abuse of rights	x	x	x	Someone with special rights (network administration, computer specialists, etc.) modifies the operating characteristics of the resources without informing the users. Someone accesses the system to modify, delete or add operating characteristics or carry out any other unauthorised operation possible to holders of these rights.
	T-8030	Forging of rights	x	x	x	A person assumes the identity of a different person in order to use his/her access rights to the information system, misinform the recipient, commit a fraud, etc.
	T-8040	Denial of actions			x	A person or entity denies being involved in an exchange with a third party or carrying out an operation.
	T-8050	Breach of personnel availability	x			Absence of qualified or authorised personnel held up for reasons beyond their control. Deliberate absence of qualified or authorised personnel.

Table 2: EBIOS threat list

To prepare the security objective definition, assets defined in step 1 should be mapped with this threat list. This could be done using the threat matrixshown in Table 3. This allows the traceability of threats for each asset.

Assets				
Threats	A-1010	A-1020	A-1030	A-1040
T-1010				
T-1020				
T-1030				
T-1040				
T-1050				
T-2010				
T-2020				
T-2030				
T-2040				
T-2050				
T-3010				
T-3020				
T-3030				
T-4010				
T-4020				
T-4030				
T-5010				
T-5020				
T-5030				
T-5040				
T-5050				
T-5060				
T-5070				
T-5080				
T-5090				
T-5100				
T-5110				
T-6010				
T-6020				
T-6030				
T-6040				
T-6050				
T-7010				
T-7020				
T-7030				
T-7040				
T-7050				

T-8010				
T-8020				
T-8030				
T-8040				
T-8050				

Table 3: Threat matrix

4.4 Security Objectives

Security objectives are derived from threats. It should be a main guideline to counter the identified threats and to satisfy the security principle. This step helps to identify the security functional objectives to reach in order to secure an asset, or a group of assets. The security objectives should cover the full list of threats for each asset, and could be classified in terms of Integrity, Confidentiality, and Availability. Those objectives could be defined in Table 4 containing an ID and a full description.

ID	Description
O-0010	Sensors information needs to be protected in terms of integrity before any transmission on the bus
O-0020	Robot communication to the FMS needs to be authenticated
O-0030	Robot communication to the FMS needs to be encrypted

Table 4: Security objectives list

After the objective identification, 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. This mapping could be done with the Table 5.

Objectives Threats	O-0010	O-0020	O-0030
T-1010			
T-1020			
T-1030			
T-1040			
T-1050			
T-2010			
T-2020			
T-2030			
T-2040			
T-2050			
T-3010			
T-3020			
T-3030			
T-4010			
T-4020			
T-4030			
T-5010			

T-5020			
T-5030			
T-5040			
T-5050			
T-5060			
T-5070			
T-5080			
T-5090			
T-5100			
T-5110			
T-6010			
T-6020			
T-6030			
T-6040			
T-6050			
T-7010			
T-7020			
T-7030			
T-7040			
T-7050			
T-8010			
T-8020			
T-8030			
T-8040			
T-8050			

Table 5: Objectives traceability

4.5 Security Requirements

The final step of the methodology is the technical requirement identification. Each security objective should lead to the implementation of one or more technical requirements. This could be defined in a table such as Table 6.

Objective ID	Requirement ID	Requirements description
O-0010	R-0010-0010	Sensor software should add a signature before sending any data
	R-0010-0020	the Robot software should check data signature before computing, store or transmit the sensor value

Table 6: requirement list

This requirement list could then be used as input for the technical design definition.

5 Critical Infrastructure Management Use Case Risk assessment

In order to build a secure BRAIN-IoT system, security requirements need to be defined according to the security level target for each use case. The following section implements the methodology described in Section 0 in order to define the most appropriate security requirements for the Water Critical Infrastructure Management that should be implemented in the architecture.

5.1 Asset Identification (Software and Hardware)

As described in Section 4.2, the first step for security requirement definition is the critical asset identification. For this early stage, the assets identified for the water critical infrastructure use case are presented in Table 7 following the template described Table 1.

A-1050	SERVER IP (Station A TELVA) Data capture
A-1051	SERVER 01 (WinCC System)
A-1052	SERVER 03 (Station and Central Server)
A-1053	Profiler YSI with multiparametric probe
A-1054	Secondary hidrostactic dam level probe
A-1055	Dam level probe
A-1056	PLC module in dam top
A-1057	Meteorological device
A-1058	Industrial Ethernet Switch no managed
A-1059	PLC in Dam Room
A-1060	Interface Module
A-1061	Ethernet optical fiber
A-1062	Profinet
A-1063	Profibus
A-1064	PC1-SCADA WinCC NT
A-1065	PC2-SCADA EMALCSA
A-1066	Router
A-1067	Gaugin Station
A-1068	Flow meter Sitrans MAG 5000
A-1069	Flow meter Sitrans MAG 8000
A-1070	Flow meter Fus-1010
A-1071	Flow meter Woltman
A-1072	Flow meter Vortex
A-1073	SensiNact
A-1074	Tecdesoft new remote station
A-1075	Water valve
A-1076	Profibus Repeater

Table 7: EMALCSA case study assets list

The assets are retrieved from the different use cases and related to the architecture.

5.2 Threats and Vulnerabilities

As described in Section 4.3, threats need to be identified for each asset. This "mapping" helps to define the security requirements needed to secure the system. According to the threats list presented in Table 2, the assets identified in this use case are related to them following the matrixes shown in Table 8 and Table 9. The "X" indicates that the threat applies to the asset.

Assets Threats	A-1050	A-1051	A-1052	A-1053	A-1054	A-1055	A-1056	A-1057	A-1058	A-1059	A-1060	A-1061	A-1062	A-1063
T-1010		X	X	X	X	X	X	X	X	X	X	X	X	X
T-1020	X	X	X				X		X	X	X	X	X	X
T-1030	X	X	X							X	X	X	X	X
T-1040	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-1050	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2010	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2020	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2030	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2040	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2050	X			X					X	X	X	X	X	X
T-3010		X	X											
T-3020	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-3030	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-4010	?	?	?	X			X	X	X	X	X	X	X	X
T-4020	X					X	X	X	X	X	X	X	X	X
T-4030				X			X	X	X	X	X	?	?	X
T-5010														
T-5020				X	X	X								
T-5030	X	X	X											
T-5040	X	X	X											
T-5050	X			X	X	X	X	X	X	X	X	X	X	X
T-5060	X	X	X											
T-5070														
T-5080		X	X											
T-5090	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-5100	X	X	X				X			X				
T-5110	X	X	X											
T-6010	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-6020	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-6030	?	?	?											
T-6040	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-6050	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-7010	X	X	X				X			X				
T-7020	X	X	X				X			X				
T-7030	X	X	X				X			X				
T-7040	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-7050	X	X	X											
T-8010	X	X	X	X	X	X	X	X	X	X	X	X	X	X
T-8020	X	X	X	X	X	X	X	X	X	X	X			
T-8030	X	X	X											

T-8040	?	?	?											
T-8050	X	X	X											

Table 8: Threats and Vulnerabilities (1/2)

Assets / Threats	A-1064	A-1065	A-1066	A-1067	A-1068	A-1069	A-1070	A-1071	A-1072	A-1073	A-1074	A-1075	A-1076
T-1010	X	X			X	X	X	X	X	X	X	X	X
T-1020	X	X	X		X	X	X	X	X		X		X
T-1030	X	X	X		X	X	X	X	X	X	X	X	X
T-1040	X	X	X	X	X	X	X	X	X	X	X	X	X
T-1050	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2010	X	X	X	X	X	X	X	X	X		X	X	X
T-2020	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2030	X	X	X	X	X	X	X	X	X	X	X	X	X
T-2040	X	X	X	X	X	X	X	X	X		X		X
T-2050	X	X	X	X	X	X	X	X	X		X	X	X
T-3010	X	X								X			
T-3020	X	X	X	X	X	X	X	X	X	X	X		X
T-3030	X	X	X	X	X	X	X	X	X	X	X		X
T-4010	?	?	X	?	X	X	X	X	X	X	X		X
T-4020	X	X	X	X	X	X	X	X	X	X	X		X
T-4030	?	?	?	?	X	X	X	X	X	X	X		?
T-5010			X	X									
T-5020				X									
T-5030	X	X	X	X						X	X		
T-5040	X	X								X			
T-5050	X	X	X	X	X	X	X	X	X		X		X
T-5060	X	X								X			
T-5070													
T-5080	X	X	X							X			
T-5090	X	X	X	X	X	X	X	X	X	X	X		X
T-5100	X	X	X	X						X	X		
T-5110	X	X	X							X			
T-6010	X	X	X	X	X	X	X	X	X	X	X	X	X
T-6020	X	X	X	X	X	X	X	X	X	X	X	X	X
T-6030	?	?								?	?		
T-6040	X	X	X	X	X	X	X	X	X	X	X		
T-6050	X	X	X	X	X	X	X	X	X	X	X		
T-7010	X	X	X							X	X		
T-7020	X	X								X	X		
T-7030	X	X											

T-7040	X	X	X	X	X	X	X	X	X	X	X		
T-7050	X	X								X			
T-8010	X	X	X	X	X	X	X	X	X	X	X		X
T-8020	X	X	X	X						X	X		
T-8030	X	X	X							X	X		
T-8040	X	X	X							X	X		
T-8050	X	X	X							X	X		

Table 9: Threats and Vulnerabilities (2/2)

6 Service Robotics Use Case: Risk assessment

In order to build a secure BRAIN-IoT system, security requirements need to be defined according to the security level targeted for each use case. The following section implements the methodology described in Section 4 in order to define the most appropriate security requirements for the Service Robotics that should be implemented in the architecture.

6.1 Asset Identification (Software and Hardware)

As described in Section 4.2, the first step for security requirement definition is the critical asset identification. For this early stage, the assets identified in the service robotics use case are presented in the Table 10 following the template described in Table 1.

A-1010	RB-1 Mobile Robot: Embedded Computer
A-1011	RB-1 Mobile Robot: Motion Control (motor driver)
A-1012	RB-1 Mobile Robot: Sensor 1, RGBD Camera
A-1013	RB-1 Mobile Robot: Sensor 2, Lidar
A-1014	RB-1 Mobile Robot: Sensor 3, IMU
A-1015	RB-1 Mobile Robot: Lift Mechanism
A-1016	RB-1 Mobile Robot: Battery (LiFePo)
A-1017	RB-1 Mobile Robot: Network (Router)
A-1020	FMS: Central Computer
A-1021	FMS: Network (Router and infrastructure)
A-1022	FMS: Mission Command (Outwards)
A-1023	FMS: Robot State (Inwards)
A-1030	Lift PLC
A-1031	PLC WiFi Gateway
A-1032	PLC: Opening order (Inwards)
A-1033	Factory External Sensor Signal (Tag, Switch, Bumpers)
A-1034	Factory External Actuator (Conveyor)
A-1040	Operator HMI

Table 10: Robotic case study assets list

6.2 Threats and Vulnerabilities

As described in Section 4.3, threats need to be identified for each asset. This "mapping" helps to define the security requirements needed to secure the system. According to the threats list presented in Table 2, the assets identified in this use case are related to them according to the matrix shown in Table 11.

Assets Threats	A-1010	A-1011	A-1012	A-1013	A-1014	A-1015	A-1016	A-1017	A-1020	A-1021	A-1022	A-1023	A-1030	A-1031	A-1032	A-1033	A-1034	A-1040
T-1010	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-1020	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-1030	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-1040	X	X	X	X	X	X	X	X	X	X			X	X			X	

T-1050	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-2010	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-2020	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-2030	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-2040	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-2050	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-3010	X	X							X				X				X	
T-3020	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-3030	X							X		X	X	X		X	X	X	X	X
T-4010								X		X	X	X		X	X	X	X	X
T-4020	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-4030	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-5010										X	X	X		X	X	X	X	X
T-5020			X														X	X
T-5030	X							X		X	X	X		X	X	X		
T-5040													X	X			X	
T-5050	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-5060																		X
T-5070																		X
T-5080	X											X				X		X
T-5090	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-5100	X	X							X		X		X	X	X			X
T-5110				X	X											X		
T-6010	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-6020	X	X	X	X	X	X	X	X	X	X			X	X			X	
T-6030	X														X		X	X
T-6040	X								X									X
T-6050	X								X				X					X
T-7010	X								X									X
T-7020	X								X				X					X
T-7030	X								X				X					X
T-7040	X							X	X	X			X	X				X
T-7050	X		X					X	X	X			X	X				X
T-8010	X							X	X	X			X	X				X
T-8020	X							X	X	X			X	X				X
T-8030	X							X	X	X			X	X				X
T-8040	X								X				X					X
T-8050	X								X				X					X

Table 11: Threats and Vulnerabilities

7 Conclusions

Thisdeliverable prsents a security assessment methodology for BRAIN-IoT solutions and provides a first implementation of this methodology on the project use cases, namely the Water Criticalinfrastructure and the Service robotics. More precisely, this delivrable is focused on identifying the critical assets of the use cases and the potential threats and vulnerabilities that might compromise them.

This version of the deliverable will be revised and further refined in the following versions which will include the security objectives and the associated technical requirements.

The proposed methodology together with the identified assets, threats and vulnerabilities are significant results that will be used as input to subsequent tasks of the project.

Acronyms

Acronym	Explanation
API	Application Program Interface
IoT	Internet of Things
IS	Information System
IT	Information Technology
PABX	Private Automatic Branch eXchange
RA	Risk Assessment
RM	Risk Management
SaaS	Software as a Service
SME	Small and Medium Entreprises
ISMS	Information Security Management System
ICS	Industrial Control Systems
SCADA	Supervisory Control and Data Acquisition
DCS	Distributed Control Systems
PLC	Programmable Logic Controllers
ISACA	Information System Audit and Control Association
OWASP	Open Web Application Security Project
COBIT	Control Objectives for Information and related Technology

List of figures

Figure 1 Risk assessment and relation with risk management process 6
Figure 2: Risk assessment methodology 16

List of tables

Table 1: Example of assets list 17
Table 2: EBIOS threat list....21
Table 3: Threat matrix 22
Table 4: security objectives list....22
Table 5: objectives traceability 23
Table 6: requirement list....23
Table 7: EMALCSA case study assets list 24
Table 8: Threats and Vulnerabilities (1/2) 26
Table 9: Threats and Vulnerabilities (2/2) 27
Table 10: Robotic case study assets list....28
Table 11: Threats and Vulnerabilities....29

References

[1] G.Stonebumer, A. Goguen, and A. Feringa, « Risk Management Guide for Information Technology Systems – Recommandations of the National Institute of Standards and Technology. » National Institute of Standards and Technology, Special Publication 800-30, 2002.

[2] J Rees, and J. Jaisingh, « Value at Risk : A Methodology for Information Security Risk Assessment. » CERIAS Technical Report 2001-127.

[3] ISO/IEC 27002:2013, « Information Technology – Security Techniques – Code of Practice for Information Security Controls. » ISO & IEC, 2013 (Previous ISO17799:2005).

[4] ISO/IEC 27001:2013 « Information Technology – Security Techniques – Information Security Management Systems – Requirements." ISO & IEC, 2013 (Previous ISO/IEC27001:2005, BS7799).

[5] Palisade Corporation, "@RISK: A Hands-On Tutorial." 2011.

[6] ISO/IEC 27000:2014, "Information Technology – Security Techniques – Information Security Management Systems- Overview and Vocabulary." ISO & IEC, 2014.

[7] ENISA, "Risk Assessment and Risk Management Methods: Information Packages for Small and Medium sized Enterprises (SMEs)." 2006.

[8] German BSI. Bsi standards 100-1, 100-2, 100-3, 100-4. https:/www.bsi.bund.de/EN/Publications/BSIStandards/standards.html

[9] Angelika Jaschob and Lydia Tsintsifa. It-grundschultz : Two-tier risk assessment for higher efficiency in IT security management. In ISSE 2006 – Securing Electronic Business Orocesses, pp 95-101. Viewweg, 2006.

[10] J. Kouns and Minoli. Information Technology Risk Management in Entreprise Environments : A Review of Industry Practices and a Practical Guide to Risk Management Teams. Wiley, 2010.

[11] Agence Nationale de la Sécurité des Systèmes d'Information. EBIOS 2010 - Expression of Needs and Identification of Security objectives. http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-188/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html, 2010.

[12] European Network and Information Security Agency. Inventory of risk management/ risk assessment methods. http://rm-inv.enisa.europe.eu/methods, February 3013.

[13] European Network and Information Security Agency. Inventory of risk management/ risk assessment methods. http://rm-inv.enisa.europe.eu/tools , February 3013.

[14] National Institute of Standards and Technology (NIST): NIST Cloud Computing Standards Roadmap, Special Publication 500-292, January 2014 (not available as PDF download but as book ISBN-13-978-1495323461)

[15] National Institute of Standards and Technology (NIST): US Government Cloud Computing Technology Roadmap, Volume I, release 1.0 (Draft), Special Publication 500-293, draft, November 2011, retrieved 2016-09-02 https://www.nist.gov/sites/default/files/documents/itl/cloud/SP_500_293_volumeI-2.pdf

[16] National Institute of Standards and Technology (NIST): Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, 2013 April, retrieved 2016-09-02 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[17] International Organization for Standardization: ISO 27000:2016: Information technology—Security technique—Information security management systems—Overview and vocabulary, 2016, retrieved 2016-09-02 http://www.iso.org/iso/catalogue_detail?csnumber=66435

[18] International Organization for Standardization: ISO 27036-4: Information technology—Security technique—Information security for supplier relationships—Part 1: Overview and concepts, 2014, retrieved 2014-09-26 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=59648

[19] National Institute of Standards and Technology (NIST): NIST Cloud Computing Standards Roadmap, Special Publication 500-291, version 2, July 2013, retrieved 2016-09-02

https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

[20] National Institute of Standards and Technology (NIST): Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144, December 2011, retrieved 2016-09-02 http://dx.doi.org/10.6028/NIST.SP.800-144

[21] National Institute of Standards and Technology (NIST): Cloud Computing Synopsis and Recommendations, Special Publication 800-161, May 2012, retrieved 2016-09-02 http://dx.doi.org/10.6028/NIST.SP.800-161

[22] The OWASP Foundation. The owasp risk rating methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[23] International Organization for Standardization: ISO 27001:2013: Information technology—Security technique—Information security management systems—Requirements, 2013, retrieved 2016-09-02 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

[24] International Organization for Standardization: ISO/IEC 27018:2014: Information technology—Security technique—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, 2014, retrieved 2016-09-05 http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

[25] IEEE Standards Association: 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, retrieved 2016-09-05 https://standards.ieee.org/findstds/standard/1686-2013.html

[26] Cloud Security Alliance (CSA): SAFEcode/CSA: Practices for Secure Development of Cloud Applications, December 2013, retrieved 2016-09-05 https://downloads.cloudsecurityalliance.org/initiatives/collaborate/safecode/SAFECode-CSA-Cloud-White-Paper.pdf from https://cloudsecurityalliance.org/group/security-guidance/

[27] Cloud Security Alliance (CSA): CSA Security Guidance Version 3, 11/14/2011, retrieved 2016-09-05 https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/ from https://cloudsecurityalliance.org/download/safecode-csa-whitepaper/