SPEAR

Secure and PrivaTE smArt gRid

(Grant Agreement No 787011)

D2.4 – Public Version of User, Security and Privacy Requirements

2019-01-31

Version 1.0

Published by the SPEAR Consortium

Dissemination Level: Public

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No 787011

Document Control Page

Document Details

Document Version	**1.0**
Document Owner	LUH
Contributors	UOWM, 8BL, SURREY, ENEL, ED, SCHN, PIMEE, VETS, TUS, TEC
Work Package	WP 2 - Use Case Preparation, Architecture, Security & Privacy Requirements
Deliverable Type	[PU]
Task	Task 2.4 – Public Version of User, Security and Privacy Requirements
Document Status	Final
Dissemination Level	Public

Document History

Version	Author(s)	Date	Summary of changes
0.1	Iheanyi Nwankwo, Marc Stauch (LUH)	2018-09-01	Table of Contents
0.2	Francisco Ramos, David Pierre (SCHN)	2018-12-26	Chapter 4.
0.3	Alkiviadis Giannakoulias (ED)	2019-01-07	Chapters 6 and 7.
0.4	Odysseas Nikolis, Vakakis Nikolaos (CERTH)	2019-01-14	Chapter 4.
0.5	Solon Athanasopoulos (PPC)	2019-01-11	Chapter 4.
0.6	Anton Hristov (VETS)	2019-01-15	Chapter 4.
0.7	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-01-16	Compilation and structure review
0.8	Igor Kotsiuba (PIMEE)	2019-01-17	Chapter 6
0.9	Francisco Ramos, David Pierre (SCHN)	2019-01-18	Chapter 4
0.91	Eider Iturbe Zamalloa, Erkuden Rios Velasco (TEC)	2019-01-18	Structure review
0.92	Solon Athanasopoulos (PPC)	2019-01-19	Chapter 4

0.93	Odysseas Nikolis, Vakakis Nikolaos (CERTH)	2019-01-22	Chapter 4
0.94	Anton Hristov (VETS)	2019-01-22	Chapter 4.
0.95	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-01-22	Structure review and compilation
0.96	Tina Krügel	2019-01-28	Review
0.97	Alkiviadis Giannakoulias (ED)	2019-01-29	Review
0.98	Eider Iturbe Zamalloa (TEC)	2019-01-30	Review
0.99	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-01-30	Review and compilation
1.0	Iheanyi Nwankwo, Marc Stauch (LUH)	2019-01-31	Final draft

Internal Review History

Reviewed By	**Date**	**Summary of Comments**
Dimitrios Tzovaras and Dimosthenis Ioannidis (CERTH)	2019-01-28	The content of the current version in general covers the essence of the document. Some amendments were suggested: - Executive Summary needs to outline clearly the tasks this report will provide inputs / outputs and can be extended to 1-page for providing full summary of the achievements of the report (i.e. number of UR, Privacy & Security defined, etc).
Emmanouil Panaousis (SURREY)	2019-01-28	The deliverable is acceptable. Some few aspects relating to security need to be modified.

Legal Notice

The information in this document is subject to change without notice.

The Members of the SPEAR Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

The Members of the SPEAR Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Possible inaccuracies of information are under the responsibility of the project. This report reflects only the author's view and that the Agency and the Commission are not responsible for any use that may be made of the information it contains.

Table of Contents

Acronyms

Acronym	Explanation
AEPD	Agencia Española de Protección de Datos
AMI	Advanced Metering Infrastructure
BDAC	Big Data Analytics Component
CERTH	Centre for Research and Technology Hellas CERTH
CJEU	Court of Justice of the European Union
CNIL	Commission nationale de l'informatique et des libertés
D	Deliverable
DDOS	Distributed Denial of Service
DoS	Denial of Service
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operators
DSP	Digital Service Providers
EC	European Commission
EEA	European Economic Area
ENEL	Ente Nazionale per l'Energia eLettrica
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
ER	Ethical Requirements
EU	European Union
FDPA	French Data Protection Act
GDPR	General Data Protection Regulation
GTM	Grid Trusted Module
HAN	Home Area Networks
HMI	Human Machine Interface
HPP	Hydro Power Plant
IAN	Industrial Area Networks
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IP	Internet Protocol
IoT	Internet of Things
ISA	International Sociological Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSP	Information System Security Policy

LUH	Gottfried Wilhelm Leibniz Universität Hannover
MTU	Master Terminal Units
MQTT	Message Queuing Telemetry Transport
NIS	Network and Information Security
NISD	Network and Information Security Directive
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services
OSSIM	Open Source Security Information Management
PIMEE	G.E. Pukhov Institute for Modeling in Energy Engineering of the National Academy of Sciences of Ukraine
PPC	Public Power Company
PLC	Programmable Logic Controller
PR	Privacy Requirements
RTU	Remote Terminal Units
RBAC	Role-Based Access Control
SC	Scenario Case
SCADA	Supervisory Control And Data Acquisition
SCHN	Schneider Electric France SAS
SIEM	Security Information and Event Management
SPEAR	Secure and PrivaTE smArt gRid
SPEAR-CHF	SPEAR Cyber Hygiene Framework
SPEAR-FRF	SPEAR Forensic Readiness Framework
SPEAR-RI	SPEAR Repository of Incidents
SR	Security Requirements
SSO	Single-Sign-On
TCP	Transmission Control Protocol
TRSC	Testing, Research and Standards Centre
TSO	Transmission System Operators
UC	Use Case
UDP	User Datagram Protocol
UOWM	University of Western Macedonia
UR	User Requirements
US	United States
VIDS	Visual-aided Intrusion Detection System
VETS	VETS Lenishta OOD

List of Figures

List of Tables

1. Executive Summary

One of the primary goals of this report is to identify the user, security and privacy requirements of the proposed SPEAR platform. The core tasks reported here were carried out in close collaboration with all project partners using several methods: teleconference, questionnaires, meetings, emails, etc., which resulted in elicitation of the requirements contained in this deliverable. Some of the partners that represent the potential end-users of the SPEAR tools identified specific business needs of the energy operators which translate into user requirements, elaborating on some of the requirements already identified in the Grant Agreement. Various core business requirements were identified from the questionnaire completed by these end-users, some of which were concretised in the use case scenarios described in the earlier part of this report:

- Quick time of detection and response
- Detection of known attacks
- Availability
- Secure transmission of data
- Visualisation of different anomalies/attacks timeframes
- A visual-added IDS with a central panel with option on specific IP devices or severity of events
- Remote notification
- Information sharing of threat intelligence
- Common form of timestamps
- Comply with relevant best practices, standards and laws
- Maintain privacy of personal data
- Reliability of tool
- Differentiation of attacks.

The privacy and security requirements followed suit as identified from the user needs and regulatory framework upon which the platform will operate. These requirements are summarised and presented in tabular form, at the end of the relevant section that analysed their source, and thereafter further collated in Annex V to this Deliverable. Together they aim to address both the need of the end-users as well as SPEAR system compliant with EU law on data protection and security. In addition, several ethical considerations relating to the use of honeypot for investigative research in the project were identified.

In essence, both the functional and non-functional requirements identified in this report will be reflected in the design of the system as documented in Deliverable D2.2— System Specification & Architecture where applicable. They will also guide the further development of the project by providing input to D2.3— Evaluation Strategy, WPs 3, 4, 5, 6 and 7.

2. Introduction

The energy sector and its infrastructure have significantly improved with the integration of information technologies, which has increased the efficiency of generation, transmission and distribution of electricity services. Various use cases of the digitalization have been highlighted [1], indicating a more advanced, data-driven energy system. Smart cities and homes are also emerging where IoT is integrated with the energy provisioning. However, these advances also have their downside. The probability of attacks on the smart grid has increased [2], [3], [9]. These attacks also put at risk personal data that may be associated with these smart technologies, including the Internet Protocol (IP) addresses and smart meters used to reach individual consumers.

The tools proposed by SPEAR aim to provide effective detection, response and countermeasures against advanced cyber threats and attacks targeted at the smart grids. Such tools are important from a user perspective, as the ability to detect different kinds of attacks concerning confidentiality, integrity and availability, as well as timely detection of these attacks are key to their business model. As noted by one respondent of the questionnaire, if the settings of the smart grid are "manipulated with malicious intent, it can pose a serious threat to the business operations, plant equipment and grid equipment, safety of power plant personnel as well as safety of the local population" [61]. This poses a threat of significant concern, requiring a thorough understanding of the needs of the energy operators in designing the proposed tools.

Privacy and security requirements applicable to SPEAR arise not only from the user needs but also from regulatory compliance. Although the proposed SPEAR platform does not fall under the definition of 'electricity undertaking' under Article 2 (35) of Directive 2009/72/EC concerning common rules for the internal market in electricity [4], it is nevertheless, important for SPEAR to reflect the requirements of the Network and Information Security (NIS) Directive [5], as best possible because it will impact the ability of the users of the tool to be compliant with this Directive. The General Data Protection Regulation (GDPR) [6] provides rules for systems used for processing personal data, and therefore applicable to SPEAR. There is also sector-specific requirements such as the use of data protection impact assessment (DPIA) template for the smart grid sector, which could serve as a reference for the SPEAR framework [7].

In all, this deliverable highlights the specific requirements methodologies of the SPEAR software requirements—the process of determining the potential users' needs, the requirements to ensure that the requisite privacy and security controls are embedded into the architecture of the system to be developed using "data protection and security by design" approach.

2.1 Contextual Reference: Overview of the SPEAR Project

The SPEAR project aims to support energy operators with a tool that could be deployed for detecting, responding and taking countermeasures against advanced cyber threats and attacks targeted at modern smart grids. This platform is proposed as a three-tier system, where each part has a different yet complementary role: the first tier builds an advanced all-in-one, open source Security Information and Event Management (SIEM) tool (SPEAR SIEM). This is designed for timeously detecting threats and attacks in smart environments. The second tier provides a rigorous forensic framework (SPEAR Forensic Readiness Framework (SPEAR-FRF), aiming to assure forensic readiness in the sense that the applied network forensic strategies are deployed before a cyber-attack incident takes place. Innovative techniques employed in this tier include an Advanced Metering Infrastructure (AMI), and honeypots for attracting attackers and capturing the necessary attacks traces for forensic procedures that will secure a detailed and complete report of the launched attack for legal purposes. The third tier is designed in line with two major requirements of all security-oriented organisations: increasing the trust between smart grid operators and facilitating EU consensus towards confronting cyber-attacks. In this respect, SPEAR not only proposes standalone solutions but goes beyond by inaugurating an anonymous and secure communication channel between all energy operators in the EU. To this end, all SPEAR SIEM tools are interconnected via a common and distributed incident database, called SPEAR Repository of Incidents (SPEAR-RI), where updates, patches and best practices are anonymously exchanged, in real time, without risking an organisation's reputation or exposing weak parts of the grid.

Figure 1 below represents the architectural description of the SPEAR platform showing its various components. D2.2—System Specifications and Architecture, contains a description of the components and data they will process. From these descriptions, potential personal data is identified and mapped for data protection purposes as shown in Chapter 4 below, thus providing the context for certain privacy and security requirements of SPEAR.

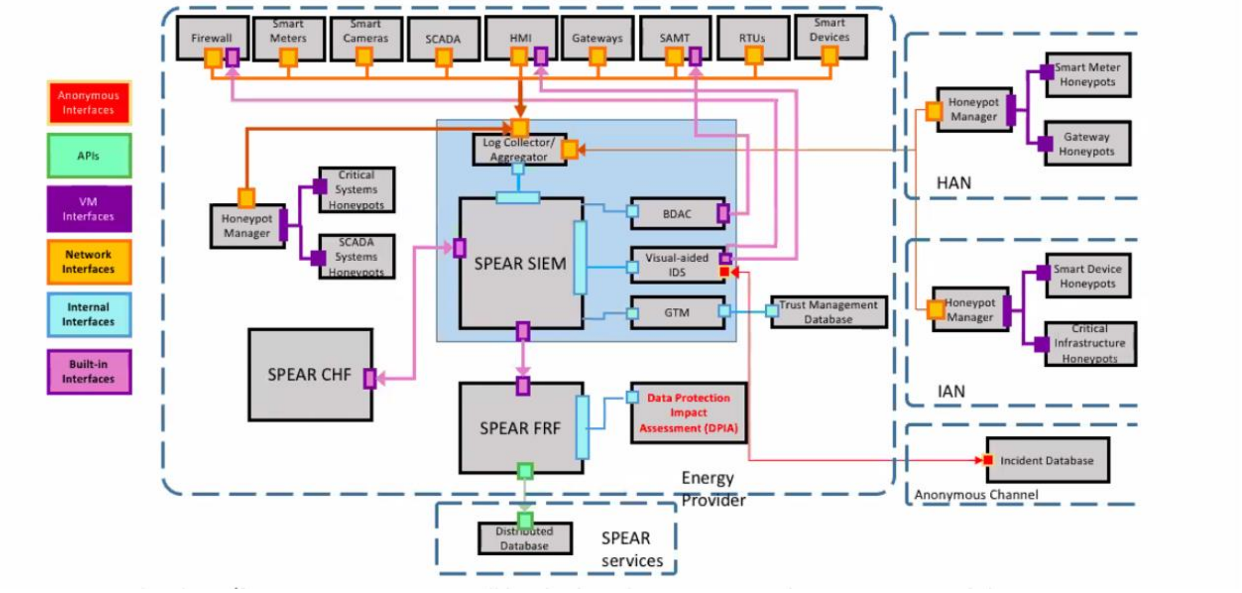

Figure 1: The SPEAR platform diagram

2.2 Structure of the deliverable

This deliverable is broadly divided into three parts which represent the user, privacy, and security requirements. At the end of each part, a table of the identified requirement is placed for easy reference. The chapters are structured as follows:

- Chapter 1 is the executive summary.
- Chapter 2 gives an introduction to the subject matter and provides an overview of the SPEAR platform and the methodology used in completing this report.
- Chapter 3 identifies the user requirements and gives an overview of the use cases.
- Chapter 4 discusses privacy and ethical requirements with a particular focus on the regulatory aspect.
- Chapter 5 focuses on security requirements.
- Chapter 6 concludes the deliverable.

2.3 Methodology

The objective of this task is to capture the user, privacy protection, and data security requirements of the SPEAR platform given the project's objectives. In general, the design of the SPEAR project is based on the ARCADE methodology framework [8]. For the tasks described in this report, desktop research, questionnaires and consultations with relevant project partners have been utilised to complete them. According to the common rules for the internal market in electricity, entities engaging in "electricity undertaking" include any natural or legal person carrying out at least one of the following functions: generation, transmission, distribution, supply, or purchase of electricity. This assisted in identifying and defining the SPEAR end-users, including consumers.

2.3.1 User requirements investigation

This section describes only the user requirement investigation based on the viewpoint requirement extraction of the ARCADE framework. Three complementary methods were applied in parallel in order to achieve better results in the collection of the SPEAR user requirements. As follows, these methods are quantitative and qualitative methods:

1. **Observation and field visit:** These are types of correlational methods in which an analysis team observes users (i.e., energy providers) as they work and takes notes of the activities that occur during the execution of their job tasks. In the SPEAR project, each use case partner and end-user partner conducted this user observation and field visit in its own premises in order to collect and extract user requirements. Some academic partners (e.g. UOWM) more familiar with the concept of Quality Assurance and Project Management technics visited the use case partners (e.g., VETS) premises as the analysis team.
2. **Interview:** This is the most common technique for gathering requirements. The users are interviewed by the requirements analysis team, to receive information about their needs and requirements in relation to the new system. In the SPEAR project, the interviews were conducted in a form of teleconferences among the use case partners, the end-users in order to understand and detect user requirements.
3. **Questionnaires**: A set of written questions to a sample population of users is given. Questionnaires can help determine the needs of users, current work practices and attitudes to the new system ideas and concept. The following SPEAR partners completed the questionnaires—PPC (representing generators and distributors), VETS (representing generators), SCHN and ENEL (representing distributors), CERTH (representing consumers).

2.3.2 Privacy and security requirements investigation

The privacy and security requirements investigation comprise both the identified requirements of the users, as well as the general system requirements of SPEAR (during the system's development and actual use in a real environment). The users' aspect was obtained with the method above. For the system in general, the following methods were used:

1. **Questionnaire:** To identify whether personal data will be processed in the development and actual use of the SPEAR platform, a questionnaire was also sent by LUH to all the other project partners to describe the nature of the data they intend to process in the project. The questionnaire introduces the meaning of personal data as well as records the intention of the partners to collect and process personal data within the scope of SPEAR.
2. **System architecture analysis:** The description of the SPEAR system's input and output data (as indicated in the Grant Agreement, deliverables D1.4 - Data Management Plan, D2.2 - System Specifications and Architecture) was analysed to obtain the privacy and security requirements for the system. Privacy and security experts in the project collaborated in this task of which the use case scenarios afforded the opportunity to imagine some of the input and output data of the system.

3. **Desktop research:** The legal and ethical framework—laws, guidelines, standards, etc., relevant for privacy and security in the smart energy systems was investigated through desktop research and analysed using a doctrinal approach.

2.3.3 Requirements specification model and link with the system's specification and architecture

From the above sources, a list of the user, security and privacy requirements for the SPEAR platform was made using the ARCADE requirement specification form. In the ARCADE framework, the requirement view documents uniquely identifiable and testable requirements. The objective is to identify, document, or specify requirements related to any concerns to the target system. Requirements shall be testable and shall be used to verify that the target system is able to perform its intended tasks.

For SPEAR, this viewpoint represents the user business requirements and compliance requirements in terms of privacy and security. Each requirement is documented as a separate entity and may concern any aspect of the architecture description. The requirement model used for documentation here is the textual description. Requirement identifiers are unique and remain constant during the full development process of the environmental information platform. A specification adopted for SPEAR include:

Table 1: SPEAR user, security and privacy requirements identifiers

Requirement identifiers	Meaning
UR	User Requirements
PR	Privacy Requirements
ER	Ethical Requirements
SR	Security Requirements

The requirement specification list is placed at the end of each division as indicated earlier and compiled as Annex II.

The output of this deliverable will be used in D2.2 which focuses on the System Specification and Architecture. D2.1 is incorporated as the "requirement viewpoint" in D2.2. To overcome the hurdle that both D2.1 and D2.2 were due at the same time, both reports were shared in their draft among the project partners.

3. User Requirements Definition

3.1 User requirements elicitation

As mentioned earlier, a user-oriented approach [62] has been adopted to identify the SPEAR user requirements. In their responses to the questionnaire circulated by LUH asking for requirements, the SPEAR end-users represented by the Use Case partners (VETS, Schneider/Enel, PPC, and CERTH) highlighted a number of key aspects, even though some of them are beyond the scope of SPEAR. First, these users stressed the need for a quick response time, in which the SIEM would detect and allow responses to cyber-attacks, preferably near real-time; the time interval for the forensic analysis to be ready was seen as less critical, with 3-7 days suggested by one respondent as a reasonable margin. Second, as regards the type of threat users regarded as most requiring protection against, this varied to some extent according to the nature of their enterprise. Thus VETS, in the context of running its hydro-electrical power station, flagged as critical the risk a cyber-intruder might gain access to the main control unit and manipulate the parameters or settings of the unit; this could involve direct physical means (malware on a USB stick). In the Smart Home scenario, CERTH noted the specific added risk of eavesdropping and extortion attacks that aim to steal information from the occupants as a basis for committing fraud or even extortion against the latter.

For their part, Schneider/ENEL, and PPC from the perspective of large utility providers, stressed the need for their Smart Grid to be safeguarded from DDOS attacks. However, they also flagged as important that the SIEM send an alert (including by email or SMS to key offsite personnel) in case a cyber-attacker seeks to take over remote control of devices and communications: this presupposed that the SIEM would be able to identify attacker behaviour that deliberately mimics the real behaviour of the system. PPC identified the IAN and HAN scenarios in its Testing, Research and Standards Centre as especially central to its security needs.

A further suggestion of VETS was that the system could allow for the disconnection of elements under attack, while maintaining just the most critical components for the essential plant functioning It was also deemed important that, in visually presenting attack information, the Visual-based IDS should employ a chronological dimension that allows the user quickly to understand the way different incidents unfold and relate to each other across time. Ideally, this information should be layered, with the user able to click on a given incident to see further details for it presented in an ‘expert mode’. In relation to cyber-hygiene issues, the partners identified the need for the SPEAR system to reflect and support information security standards and frameworks, such as the ISO 27000 specifications, IEC 62351 and IEC 62443, as well as the data protection requirements of the GDPR as best as possible to assist them in achieving them.

It is important to highlight that in the analysis of their full responses to the questions in the Questionnaire appended in Annexes 1-4 to this Deliverable, only the requirements that are within the scope of SPEAR were reflected. The list of the user requirements is presented further below in the table in Section 3.3.

3.2 The use cases

To support verification and validation of the user requirements, four use cases have been relied upon in the SPEAR project. The description, definition and user stories in this section were developed by the partners that completed the questionnaire.

3.2.1 Use Case 1: The Hydro Power Plant Scenario

3.2.1.1 Description of the Hydro Power Plant use case

Hydro power is an essential part of the electricity mix and is the biggest contributor to the renewable energy production worldwide, constituting more than 50% of the global RES production [64]. Hydro power plants vary in size and technology and have a different impact on the local or regional grid.

The hydro power plant scenario includes real testing of the developed SPEAR tools and components in an operational electricity production facility. HPP Lenishta is located in the mountain area of Bulgaria (near the city of Razlog) and has an installed capacity of 500kW. The plant is connected to the distribution grid via 370 meters long 20 kV transmission line. The SPEAR components will be running to detect attacks. Types of attacks will vary in order to confirm the SPEAR ability to differentiate between a cyber-attack and anomalies caused by extreme weather conditions.

Figure 2 below represents the hydro power plant scenario:

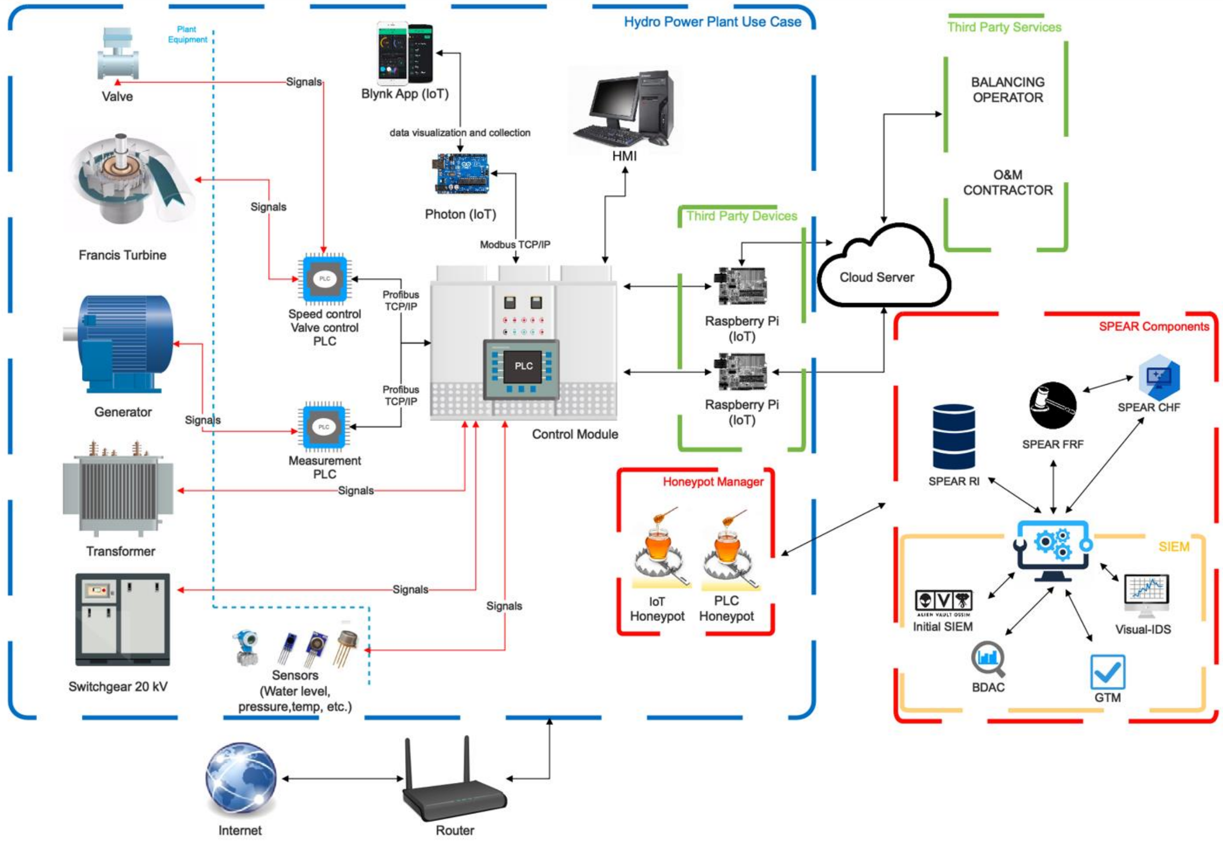

Figure 2: The Hydro power plant scenario architecture diagram

3.2.1.2 Components and related data for the Hydro Power Plant scenario

The components existing in the Hydro Power Plant are as follows:

- **Plant equipment** – (valve, turbine, generator, transformer, switchgear, sensors) - all power plant components generate signals and communicate them to the PLC units. A set of sensors perform measurements of pressure, temperatures, water levels and other critical parameters for operation.
- **Control Module PLC** – gathers data from the plant equipment either directly, or through additional PLC units and makes decisions about the plant operation based on the received values and the preset limits.
- **HMI**– visualizes information from the control module and allows for monitoring and operating the power plant. This can also be done through remote control of the HMI.
- **Particle Photon (IoT)** – an open source product, which communicates through Modbus TCP/IP with the Control module and collects data, which it then visualizes on an IoT application. The Blynk application is used for remote monitoring of the PLC visualization module. Currently, control functions are also being developed.
- **Raspberry Pi (IoT)** – two separate devices that collect data about the plant performance from the Control module. The first one sends data to the balancing operator which is necessary for correct forecasting of production and grid stability. The other one collects information about operational data and sends it to the O&M operator for continuous monitoring of the power plant status and enables timely preventive maintenance measures.

The potential SPEAR components to be integrated and the required functionalities from them are the following:

- **SPEAR SIEM** – the detection tool with its related components will detect and warn about any suspicious activities, which may constitute a cyber-attack. The platform will use state of the art analytics tools, graphical-aided visualisation techniques and trust management mechanisms in order to detect anomalies and disruptions in the data traffic and alert about it in real time.
- **Honeypots** – that simulate the vulnerable hydro power plant PLCs and IoT devices, and capture as much information about the attack and attacker, including IP addresses, timestamp, access ports and communication protocols and other.

Data collected during the deployment of the use case and the lifespan of the project:

- **Communication Data** – data communication between the plant equipment, PLC and smart devices includes strictly industrial measurement data regarding operational readiness. Metrics like equipment temperatures, water levels, voltage and other hydro power related measures do not include any personal information.
- **Data from the Honeypots** - Honeypots simulating the PLC controller and the IoT devices will collect detailed information regarding the attack and attacker which may include personal data.

Outputs:

- **Visual-based IDS** shall provide a visual representation of the SPEAR SIEM functionalities in the hydro power plant architecture.
- **PLC Honeypot** shall store logs and generated network traffic.

3.2.1.3 Hydro Power Plant use case scenario definition

Table 2 describes the Hydro Power Plant scenarios while figure 3 shows the roles of the actors identified for this use case.

Table 2: The Hydro power plant scenario definition

Use case	Scenario ID and Title	Priority level	Related requirements
UC1. Hydro Power Plant	SC1.1. Detection and reaction to cyber-attack on the PLC controller in the hydro power plant	High	UR-01, UR-02
	SC1.2 Detection and reaction to cyber-attack on the IoT devices in the hydro power plant	High	UR-01, UR-02
	SC1.3. Differentiation between cyber-attack and anomalies caused by extreme weather conditions	Medium	UR-13
	SC1.4. Honeypots operation in the hydro power plant	High	UR-12, ER-02

- **SPEAR Security Engineer** – a person responsible for installation, monitoring and operation of the SPEAR platform in the hydro power plant. Since the Lenishta power plant is fully automated and does not require human presence full time, the security engineer would be accessing the plant and SPEAR software remotely. He is responsible for receiving notifications from the platform and taking the necessary measures to react to the cyber-attack.
- **Hydro power plant operator** – a person with technical and operational knowledge of the plant, who when necessary physically controls the facilities through the control module or the HMI inside the control room.
- **Cyber-attacker** – a person conducting the cyber-attack either remotely or by physically connecting a hard drive with malicious software to the control module or HMI

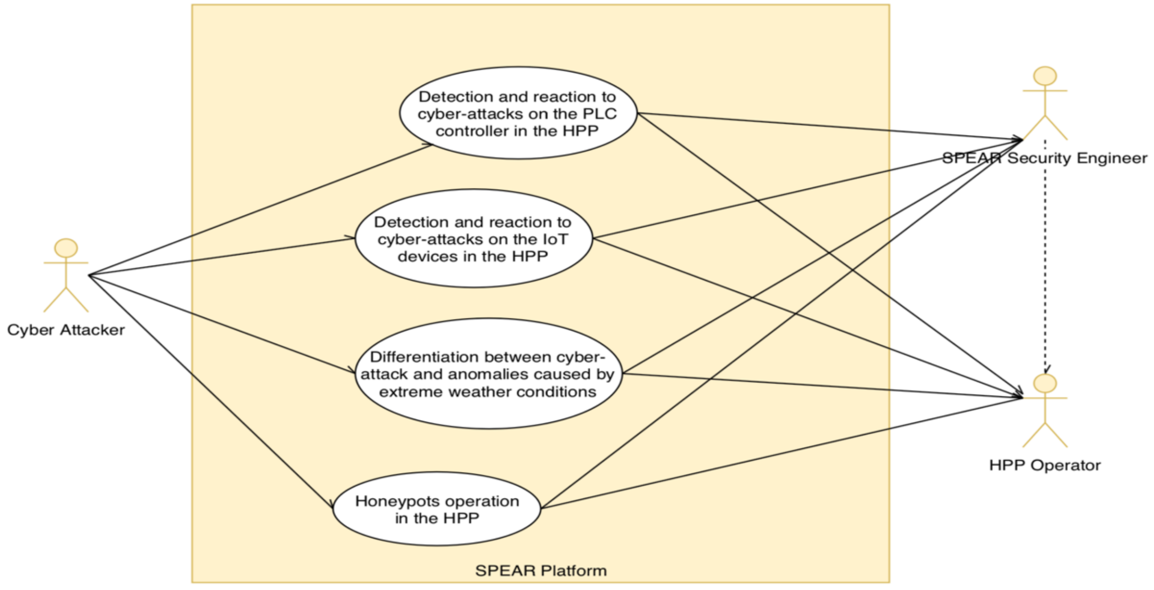
Detection and reaction to cyber-attacks on the PLC controller in the HPP
Detection and reaction to cyber-attacks on the IoT devices in the HPP
Differentiation between cyber-attack and anomalies caused by extreme weather conditions
Honeypots operation in the HPP
SPEAR Platform
Cyber Attacker
SPEAR Security Engineer
HPP Operator

Figure 3: High-level description of the Hydro power plant use case roles in the use case scenarios

3.2.1.4 Scenarios description

Tables 3, 4, 5 and 6 describe the use case scenarios for the Hydro-Power Plant in Bulgaria. These tables showcase what each scenario of the use case is targeted at as well as the evaluation criteria.

Table 3: Detection and reaction to cyber-attack on the PLC controller in the hydro power plant

Scenario Name	SC1.1. Detection and reaction to cyber-attack on the PLC controller in the hydro power plant
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	The automated hydro power plant has a PLC Control module connected to the internet, which monitors all operational parameters and takes decisions regarding the behaviour of the plant. This is the most critical component to protect in this use case, since it manages all aspects of the power plant and poses a threat to plant and grid equipment, but also third party property damage and physical health. This scenario showcases how the SPEAR platform detects and reacts to a cyber-attack on the most critical plant device.
Challenges	1. Ability to detect a breach in the security of the PLC as quickly as possible 2. Short alert and response time
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The security engineer is monitoring the system remotely via the visual IDS.
Goal (Successful End Condition)	The attack has been successfully identified by the output of the SPEAR SIEM tool, the BDAC, or the Visual IDS or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart Grid Database, the reputation of the attacked node is being updated in the GTM and the attack has been recorded in the SPEAR-RI.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Cyber attacker
Scenario Initiation	An attacker launches an attack against the Profibus TCP/IP protocol used by the PLC devices.
Main Flow	1. The attacker launches a (D)DoS attack against the controller and inundates it with traffic. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the security engineer monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the inverters/chargers is updated in GTM component. The incident is being recorded in SPEAR-RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 4: Detection and reaction to cyber-attack on the IoT devices in the Hydro Power Plant

Scenario Name	SC1.2 Detection and reaction to cyber-attack on the IoT devices in the hydro power plant
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	The hydro power plant equipment includes 3 IoT devices. A Photon Particle, which sends data to a mobile application for monitoring and 2 Raspberry Pi's, which send data to a cloud service to be accessed by third parties. This scenario showcases how the SPEAR system reacts to a cyber-attack against the IoT devices.
Challenges	1. Ability to detect anomalies in the data transfer from the IoT devices. 2. Timely detection of the anomalies.
Assumptions & Pre-Conditions	1. The IoT devices are functioning properly and sending adequate data. 2. The SPEAR system is up and running. 3. The security engineer is monitoring the system remotely via the visual IDS.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool or SPEAR BDAC or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM and the attack has been recorded in the SPEAR-RI.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Cyber attacker
Scenario Initiation	An attacker launches an attack against the Modbus TCP/IP protocol used by the IoT devices
Main Flow	1. The attacker sends TCP packets exceeding the maximum length to the Modbus client and server trying to succeed a buffer overflow attack. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the security engineer monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the inverters/chargers is updated in GTM component. The incident is being recorded in SPEAR-RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer, allowing him to take appropriate remedial actions.

Table 5: Differentiation between cyber-attack and anomalies caused by extreme weather conditions

Scenario Name	SC1.3. Differentiation between cyber-attack and anomalies caused by extreme weather conditions
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	The hydro power plant may experience anomalies in traffic and communication with the grid or between devices due to extreme weather conditions. Such incidents may include lack of internet connectivity caused by the provider's equipment or absence of electrical power to the router. This scenario showcases the ability of SPEAR components to differentiate between a cyber-attack and a naturally caused anomaly.
Challenges	1. Ability to differentiate the cause of the detected anomaly
Assumptions & Pre-Conditions	1. All plant components are working properly before the extreme weather event 2. The SPEAR system is up and running. 3. The security engineer is monitoring the system remotely via the visual IDS.
Goal (Successful End Condition)	The anomaly has been successfully identified by the SPEAR SIEM tool or the SPEAR BDAC or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM and the anomaly has been recorded in the SPEAR-RI.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Weather conditions
Scenario Initiation	Extreme weather causes anomalies in the communication between the plant components and smart devices.
Main Flow	1. The communication between the plant components and devices is disrupted. 2. The SPEAR BDAC anomaly detection algorithms identify the incident as not-malicious and caused by a cyber-attack or the security engineer monitoring the system notices the internet connection or the power is down. 3. System logs and network packets are securely stored in the Smart grid Database for a non-malicious example. 4. The incident is being recorded in the SPEAR-RI without the need to protect personal information.
Evaluation Criteria	SPEAR detects the anomaly and notifies the security engineer allowing him to take appropriate remedial actions.

Table 6: Honeypots operation in the hydro power plant

Scenario Name	SC1.4. Honeypots operation in the hydro power plant
Related Use Case	UC1. Hydro Power Plant
Scenario Description	
Brief Description	Honeypots are a cyber-security system which acts as a decoy for attackers and captures information about the attacker and the incident. This scenario showcases how the SPEAR honeypots operate and record data from cyber-attacks on the PLC and IoT devices in the power plant.
Challenges	1. Honeypots should mimic the PLC or IoT devices realistically to attract the attacker and hide the original device 2. SPEAR SIEM should be able to detect anti-honeypot techniques and overcome them
Assumptions & Pre-Conditions	1. Honeypots are installed and connected to the Local Area Network of the hydro power plant 2. Honeypots will simulate a PLC controller and an IoT device
Goal (Successful End Condition)	The execution of this scenario is considered successful when the honeypot has attracted a simulated cyber-attack on the simulated devices and has recorded information regarding attacker and incident.
Involved Actors	1. Hydro power plant operator 2. SPEAR security engineer 3. Cyber attacker
Scenario Initiation	An attacker launches an attack against the Modbus TCP/IP protocol used by the IoT devices
Main Flow	1. Initialize and start the execution of the honeypot software. 2. Verify that the honeypot records the cyber-attacker actions. 3. Execute the steps of a cyber-attack against the simulated Hydro power equipment or service. 4. Collect system logs and network packets. Interpretation and assignment of the registered information in the log-files with the cyber-attack actions.
Evaluation Criteria	SPEAR honeypot records the attack and notifies the security engineer allowing him to take appropriate remedial actions.

3.2.1.5 User Stories for the Hydro power plant use case

I. Using SPEAR-SIEM in the hydro power plant to detect cyber-attacks against PLCs

The SE goes on his usual daily routine and periodically checks the system remotely for any anomalies detected by the SPEAR BDAC or the SPEAR SIEM tools and reported back in the dashboard of visual-aided IDS. He receives an alert for a suspicious event and goes into more detail with the help of the visual-based IDS and the dashboard from the SPEAR SIEM tool. The results of his examination point him to the type of attack and he takes measures to ensure the HPP system is protected and safe from outside influence or control. The SPEAR SIEM component registers all attack details (systems logs and network packets) to the smart grid database while the SPEAR GTM component updates the reputation score of the respective attacked devices.

II. Using the SPEAR-SIEM to differentiate between cyber-attack and anomalies caused by extreme weather conditions

The SE goes on his usual daily routine and periodically checks the system remotely for anomalies detected by the SPEAR SIEM. He receives an alert for a suspicious event and goes into more detail with the help of the visual-based IDS. The SPEAR-SIEM signalled that there was a sudden stop in communication traffic, or sent an alert that the SIEM stopped operating. After a physical visit to the power plant, the SE notices that the traffic anomaly was related to a temporary loss of internet connectivity caused by bad weather conditions. In this case, the monitoring devices were not working properly, however, the power plant was still operating and could be monitored and controlled manually on site from the touch panel of the PLC controller.

III. Using the SPEAR honeypot in the hydro power plant environment.

Honeypots are used by the HPP SPEAR Security Engineer (SE) to collect information about cyber-attacks against the HPP equipment, network and protocols. By mimicking the PLCs, IoT devices and other network components, the honeypots prevent the attacker from accessing the infrastructure and eliminate the risk of irreversible consequences by the attack. The SE analyses the information sent to log files and whenever he notices anything out of the ordinary, takes responsive measures. These typically include assurance of the range of attack, investigation of the logs, and any subsequent response necessary.

3.2.2 Use Case 2: The Substation Scenario

3.2.2.1 Description of the Substation Scenario Use Case

The electrical network is defined a critical infrastructure [10], and one of the main elements of the Electrical Distribution Network is the Substation Automation Systems that control and monitor the electrical infrastructure. These control systems are composed of advanced Remote Terminal Units (RTU) and Intelligent Electronic Devices (IED) which enclose serial and Ethernet communications, data logging capabilities, analogue and digital inputs/outputs, etc. Currently, new vulnerabilities and threats have emerged to these types of assets so their protection to avoid cyber-attacks is a primary concern.

The challenge now is to improve the security of the Substation Automation Systems to protect the electrical network. In this context, the use case is based on Substation Automation Systems. Schneider Electric will provide a suitable experimental scenario that will be used in the evaluation and validation activities under realistic conditions at the laboratory level. The aim will be to simulate a real Substation Automation System of the Electrical Distribution Network.

3.2.2.2 Components and related data for the scenario

The components existing in the Substation are as follows:

- **Security Server and Configuration tool** are companion products to be used with Intelligent Electronic Devices (like RTU) that integrate the library of functions allowing compliance to cybersecurity standards IEC 62443, IEC62351.
- **Configuration tool** is used for configuring the security policy (authentication/authorization with RBAC, local user management).
- **Security Server** is a security server allowing security management at system level (aggregation of security logs from any Syslog compliant device, centralized authentication/authorization AD/Radius).
- **Remote Terminal Unit (RTU)** is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA by transmitting telemetry data to the system, and by using messages from the supervisory.

The potential SPEAR components to be integrated and the required functionalities from them are the following:

- **RTU Honeypot** is a virtual component that simulates the behaviour of a real RTU.
- **SPEAR Security Information and Event Management (SIEM),** including its components. This component supports the detection of threats, anomalies and cyber-attacks in smart grid environments. It enables the collection of information from several architectural levels of the smart grid system by using multiple distributed security probes (called sensors in the SPEAR context), to perform a sophisticated correlation analysis of attack patterns in order to detect cyber-attack incidents. It also provides a visual-aided dashboard where visualisations could significantly assist the security administrator to globally inspect the smart grid infrastructure in near real time. It integrates existing top open-source SIEM tool capabilities such as AlientVault's OSSIM's together with innovative technologies based on advanced analytics, graphical-aided visualisation techniques and trust management mechanisms.

Concerning the data, both personal and non-personal data are processed in this use case are as follows:

- **Configuration tool**: storing into a database the role-based access control (definition of users, roles, and permissions and assignment of roles to users) and security policies (like the address of the Syslog Server). Personal information on user: name, telephone number, email.
- **Security Server:** record userID and collect Syslog from the device which is stored in a database. Security Server is using Syslog (RFC5424) that includes a mandatory field for "peerID", as a result when a user performs an action the action is recorded, the log contains the userID inside the peerID field.
- **RTU** is producing a real-time database according with commands coming from distributed control system or SCADA which generates digital and analogue outputs and with the information produced by the sensors that are, digital and analogue inputs. Inputs initially generated by sensor which are capture by acquisition RTU and then sent to front end RTU using industrial protocols, such IEC104, DNP3 and IEC61850, generating network traffic between both devices. In addition, RTU will generate system-logs which includes information about the RTU software versions, warnings and possible errors during the RTU power on and the operating period and security warnings.
- **RTU Honeypot** will simulate the behaviour of the RTU and will generate the same kind of data. Honeypot will collect attackers' network traffic data **(**normally anonymized by TOR**).**

Outputs:

- **Configuration tool:** shall provide role-based access control (RBAC) information. Stored in Configuration tool.
- **Security Server:** shall provide userID and Syslogs. Stored in Security Server.
- **RTU:** shall provide digital, analogue inputs and outputs and Syslog. Stored in RTU.
- **RTU Honeypot**: shall provide digital, analogue inputs and outputs and Syslog, and attackers' network traffic data stored at Honeypot level.

3.2.2.3 Substation use case scenario definition

Table 7 describes the Substation scenarios while Figure 4 shows the roles of the actors identified for this use case.

Table 7: The Substation scenario definition

Use case	Scenario ID and Title	Priority level	Related requirements
UC2. Substation	SC2.1. Detection and reaction to cyber-attack on the smart-grid equipment of the Substation.	High	UR-01, UR-02
	SC2.2. Detection and reaction to cyber-attack on the RTUs in the Substation.	High	UR-01; UR-02
	SC2.3. Detection and reaction to cyber-attack on the gateways in the Substation.	High	UR-01, UR-02
	SC2.4. Detection and reaction to cyber-attack on the RTUs and Security	High	UR-01, UR-02

Use case	Scenario ID and Title	Priority level	Related requirements
	Server/Configuration tool in the Substation Scenario		
	SC2.5. Honeypot operation in the Substation Scenario	High	UR-12, ER-02

Figure 4 visualizes the Substation Use Case Roles, and the modules and components used during the execution of the use case scenarios. There are three roles:

- **Substation security administrator**: This user is responsible to use, monitor and maintain the SPEAR installation in the Substation. This is the most important user of the SPEAR system in this use case.
- **Substation end-user engineer:** This user is a user of the Substation RTU and Security Server/Configuration tool system. The behaviour of this user has an indirect effect on the SPEAR system. This user is aware of the SPEAR system and the provided security services but he/she has limited or no access to the SPEAR system.
- **Substation cyber-attacker:** This user is the cyber-attacker against the Substation infrastructure.

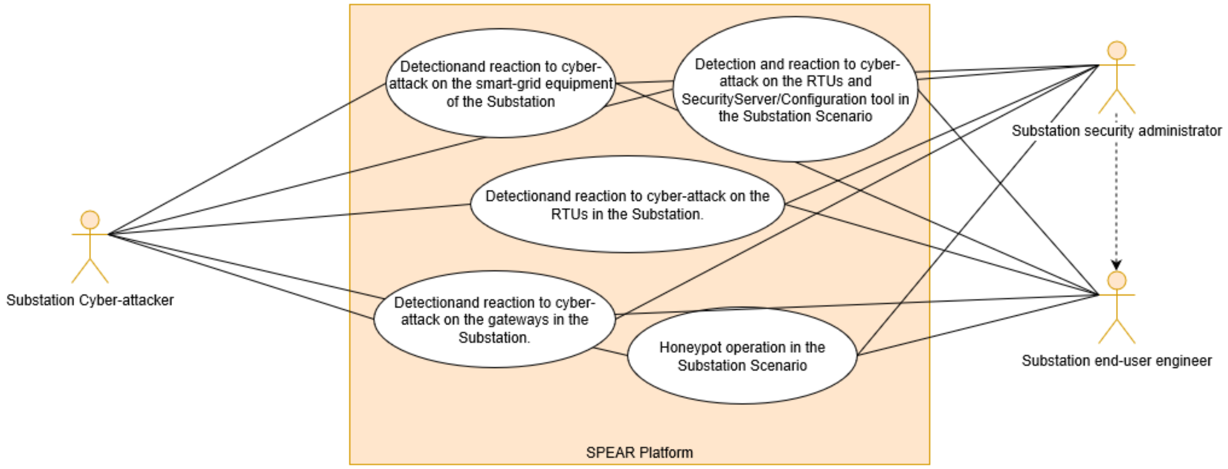
Detectionand reaction to cyber-attack on the smart-grid equipment of the Substation
Detection and reaction to cyber-attack on the RTUs and SecurityServer/Configuration tool in the Substation Scenario
Detectionand reaction to cyber-attack on the RTUs in the Substation.
Detectionand reaction to cyber-attack on the gateways in the Substation.
Honeypot operation in the Substation Scenario
SPEAR Platform
Substation Cyber-attacker
Substation security administrator
Substation end-user engineer

Figure 4: High-Level Description of the Substation Use Case Roles in the use case scenarios

3.2.2.4 Scenarios description

Tables 8, 9, 10, 11 and 12 describe the use case scenarios for the Substation in France and Spain. These tables showcase what each scenario of the use case is targeted at, as well as the evaluation criteria.

Table 8: Detection and reaction to cyber-attack on the smart-grid equipment of the Substation

Scenario Name	SC2.1. Detection and reaction to cyber-attack on the smart-grid equipment of the Substation.

Related Use Case	UC2. Substation
Scenario Description	
Brief Description	The Substation has a System of Control of Supervision and the Acquisition of Information (SCADA). Smart-grid services such as remotely manage the elements manoeuvres on the electrical substations that allow to transport and to distribute the electric power of the network. This scenario showcases how the SPEAR system detects a cyber-attack on the smart-grid equipment and services.
Challenges	1. Ability to detect different kinds of attacks concerning confidentiality, integrity and availability. 2. Timely detection of the attack.
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The security engineer is monitoring the system via the visual IDS and the SPEAR SIEM dashboard.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM.
Involved Actors	1. Substation security administrator: 2. Substation end-user engineer 3. Substation Cyber attacker.
Scenario Initiation	The cyber-attacker launches an attack against the SCADA with the objective to get the unauthorized remote control of the system.
Main Flow	1. The attacker sends TCP/IP packets changing the IP trying the host answers receive the TCP/IP packets to the false IP. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the security engineer monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the inverters/chargers is updated in GTM component.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 9: Detection and reaction to cyber-attack on the RTUs in the Substation

Scenario Name	SC2.2. Detection and reaction to cyber-attack on the RTUs in the Substation.
Related Use Case	UC2. Substation
Scenario Description	
Brief Description	In the Substation, there are some RTUs responsible to execute the commands coming from the Control Centres. This scenario showcases how the SPEAR system deploys security operations against a cyber-attack on the RTUs and the services they support.

Challenges	1. Ability to detect different kinds of attacks concerning confidentiality, integrity and availability. 2. Timely detection of the attack
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The security engineer is monitoring the system via the visual IDS and the SPEAR SIEM dashboard.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM.
Involved Actors	1. Substation security administrator: 2. Substation end-user engineer 3. Substation Cyber attacker.
Scenario Initiation	The cyber-attacker launches a malware against the RTUs
Main Flow	1. Simulating a physical attack against the substation devices, the cyber-attacker installs a malware in a RTU with a pen drive. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the security engineer monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the energy meters that have been attacked is updated in the GTM component.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 10: Detection and reaction to cyber-attack on the gateways in the Substation

Scenario Name	SC2.3. Detection and reaction to cyber-attack on the gateways in the Substation.
Related Use Case	UC2 Substation
Scenario Description	
Brief Description	In the Substation, there are various gateways supporting multi-sensor devices and end-user services. This scenario investigates how the SPEAR system deploys security operations against a cyber-attack on the gateways and the services they support.
Challenges	1. A major challenge in this scenario is the research and detection of active vulnerabilities and specific exploits that apply in the Substation equipment. 2. A big challenge for this scenario is the reset of the Substation equipment after the execution of the cyber-attack and the restore of the system back to normal operation.
Assumptions & Pre-Conditions	It is assumed that in the beginning of the experiment the gateways are operating normally and no other cyber-attack or malfunction is applied on the equipment. The normal operation of the gateways before the application of the cyber-attack is very important to

	determine the effect of the attack against the Substation devices and services.
Goal (Successful End Condition)	The SPEAR SIEM detects and reports the applied cyber-attacks or abnormal events against the gateways in the Substation.
Involved Actors	1. Substation security administrator. 2. Substation end-user engineer. 3. Substation Cyber attacker.
Scenario Initiation	The hardware and software of the gateways is updated and the equipment is working in normal operation supporting the Substation services.
Main Flow	In this scenario, different experiments and cyber-attacks will be investigated against the gateways of the Substation. The most important vulnerabilities will be exploited in order to reveal the weaknesses on the gateways of the Substation. The main flow of the execution of the experiments is described here by the application of a SQL false data injection attack on a local server-gateway of the Substation. A similar main flow can be applied for other attacks also. 1. Initiate the gateways and the connected devices under attack. 2. Launch the cyber-attack against the Substation gateway. 3. Verify the response of the SPEAR-SIEM tool at the cyber-attack. 4. Register and report the results. 5. Restart the system under attack and bring it back in normal operation. Regarding the gateways the available vulnerabilities are defined by the current version of hardware, firmware/software, the communication protocols, the network architecture and the preservation of the security properties (confidentiality, integrity, non-repudiation, availability).
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 11: Detection and reaction to cyber-attack on the on the RTUs and Security Server/Configuration tool in the Substation Scenario

Scenario Name	SC2.4. Detection and reaction to cyber-attack on the on the RTUs and Security Server/Configuration tool in the Substation Scenario
Related Use Case	UC2. Substation
Scenario Description	
Brief Description	RTUs devices are the key element of Substation Automation Systems. The RTUs as central part of the control and monitoring system of the electric Substation can be a target to cyber-attackers. Security Server/Configuration tool systems are already in place to improve security in the scenario. This scenario will investigate how the SPEAR system deploys security operations against a cyber-attack on the RTUs and Security Server/Configuration tool.

Challenges	1. Ability to detect different kinds of attacks concerning confidentiality, integrity and availability. 2. Timely detection of the attack.
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The security engineer is monitoring the system via the visual IDS and the SPEAR SIEM dashboard.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool or by the security engineer, all needed information for the SPEAR-FRF has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM.
Involved Actors	1. Substation security administrator. 2. Substation end-user engineer. 3. Substation Cyber attacker.
Scenario Initiation	The cyber-attacker launches an attack against the industrial protocols such as IEC104, DNP3, Modbus protocols or IEC61850 protocols used by RTUs.
Main Flow	1. Attack to the TCP/IP protocols such as DoS, SYN Flooding, Defeating the Network Security, Man-in-the-middle, etc. 2. The SPEAR SIEM or the security engineer monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, identify the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the inverters/chargers is updated in GTM component.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 12: Honeypot operation in the Substation Scenario

Scenario Name	SC2.5. Honeypot operation in the Substation Scenario
Related Use Case	UC2. Substation
Scenario Description	
Brief Description	The honeypots are cyber-security systems which try to capture and track the attack vector against the Substation. This scenario investigates how the SPEAR honeypot works in a Substation and describes the recorded action of a cyber-attacker targeting smart-devices and the services they support.
Challenges	A major challenge in this scenario is the research and detection of active vulnerabilities and specific exploits that apply in the RTUs.
Assumptions & Pre-Conditions	The honeypot behaves as real RTUs and are installed and connected to the network.
Goal (Successful End Condition)	The execution of this scenario is considered successful when the honeypot records the behaviour of a cyber-attacker executing a pre-defined cyber-attack against the simulated equipment.
Involved Actors	1. Substation security administrator.

	2. Substation end-user engineer. 3. Substation Cyber attacker.
Scenario Initiation	The honeypot is installed and configured to record in log files the behaviour of a cyber-attacker on a public IP accessible from outside.
Main Flow	In the main flow of this scenario the following steps present an execution 1. Initialize and start the execution of the honeypot software. 2. Verify that the honeypot records the cyber-attacker actions. 3. The cyber-attacker executes the steps of a cyber-attack against the simulated Substation RTUs. 4. Collect the log-files and all activity related to the attack. 5. Interpretation and assignment of the registered information in the log-files with the cyber-attack actions by the SPEAR SIEM.
Evaluation Criteria	SPEAR honeypot records the attack and notifies the security engineer allowing him to take appropriate remedial actions.

3.2.2.5 User Stories for the Substation use case

I. Using SPEAR-SIEM in Substation environment to detect cyber-attacks against smartgrid equipment

Charles, the Substation end-user engineer is colleague of Peter, the Substation security administrator.

Charles makes continuous testing cases in the smart-grid equipment in order to ensure all the infrastructures under his responsibility are working correctly. When Charles discovers any device in the Smart grid is behaving strangely, he informs to Peter.

Peter works in the security department; SPEAR platform is the main tool he has to detect attacks on the smart grids. He is always monitoring cybersecurity and working with a 24/7 hours services team in charge of the SPEAR platform.

When Peter realizes that there is an attack, he informs to Charles. In this way they are permanently aligned in order to detect a possible threat quickly.

Today, Peter has received an alert notification from SPEAR platform about an unknown attack. When he calls Charles, the end-user engineer confirms the SCADA is not working correctly and is being remotely managed by a non-authorized person. Immediately, Charles shuts down the SCADA, waiting until the incident has been solved.

II. Using SPEAR-SIEM in Substation environment to detect cyber-attacks against RTUs

Charles, the Substation end-user engineer, as usual is testing the Smart grid devices to guarantee that all the devices are working correctly. In a testing environment, he is simulating some commands in the RTUs and verifying the expected results. Once Charles detects something is working wrongly, he informs Peter, the Substation security administrator, who investigates if the SPEAR platform can identify any cybersecurity alert. After some minutes of analysing with his cybersecurity team, they find a malware running in an RTU. Peter could fix the infected RTU before working in production. Due to their close working relationship, Peter and Charles detect on a testing behaviour a strong threat that could be of significant consequences in the energy supply of several citizens.

III. Using SPEAR-SIEM in Substation environment to detect cyber-attacks against gateways

Peter, the Substation security administrator wants to test the SPEAR-SIEM tool and its ability to timeously detect a cyber-attack against Substation gateways. He speaks with Charles, the Substation end-user engineer, in order to prepare a test environment. Peter wants to introduce a false data injection in the database of the Substation server-gateway. Once the attack is performed, Charles realizes that the Substation devices do not work correctly. Peter sees the SPEAR-SIEM platform detected the attack with an unusual traffic and analysed all the information detected as well as sending the corresponding notification. The test has been a successful case.

IV. Using SPEAR-SIEM in Substation to detect cyber-attacks against the infrastructure

Peter the Substation security administrator, as usual is monitoring the system to find any suspicious event that could lead to a security breach in the Substation. Peter uses the SPEAR-SIEM for identifying anomalies in the Substation’s network traffic. At some point Peter receives a notification from SPEAR, warning him for a severe security event. The anomaly detection algorithms have identified unusual network traffic behaviour. Peter uses the visual-based IDS in order to investigate the event in more depth by observing different aspects of the network data and notices a large amount of received TCP packets, concerning specific RTUs for a time-period. He understands that the RTUs are under a DDOS attack and he immediately takes counter-measures to confront the attack and assure the integrity of energy meters. Attack information, needed by the SPEAR-FRF (system logs and network packets), has been securely stored in the Smart grid Database, in order to form evidence for the court while the GTM component updates the reputation score of the RTUs that have been attacked.

V. Using the SPEAR honeypot in the Substation.

Peter, the Substation SPEAR security administrator is using honeypots for two main reasons. One reason is to record and study the behaviour of the cyber-attackers against the Substation infrastructure. The other reason is to prevent the cyber-attackers from exploiting or damaging valuable Substation infrastructure by imitating the critical infrastructure with the use of the honeypots. Peter has installed and launched a honeypot in the network. He is checking the log-files constantly in order to detect and understand suspicious operations against the Substation through the SPEAR SIEM. When Peter detects a suspicious behaviour, he reviews the information in the log-files and at the same time he uses the SPEAR SIEM to see if other infrastructure is under a cyber-attack or experiencing abnormal events.

3.2.3 Use Case 3: The combined IAN and HAN scenario

3.2.3.1 Description of the combined IAN and HAN use case

The combined use case that is deployed by the Public Power Company (PPC) consists of two scenarios that aim to evaluate and validate the SPEAR platform’s ability to detect and respond to cyberattacks in combined scenarios, where both Industrial Area Networks (IAN) and Home Area Networks (HAN) exist.

The architecture of the combined IAN and HAN scenario is depicted in Figure 5 which is deployed on both the Testing, Research and Standards Centre (TRSC) laboratory of PPC, located in Athens, Greece, and the Lavrio Unit No 5 power plant of PPC that is located in Lavrio, Greece. The IAN network consists of various industrial equipment and PLCs that acquire signals and data from that equipment and make them available to Master Terminal Units (MTUs) and the Human Machine Interface (HMI). On the other hand, the HAN network contains smart meters that retain data from various Intelligent Electronic Devices (IEDs) that are placed at offices and non-industrial environments and forwards them to the headend and the HMI.

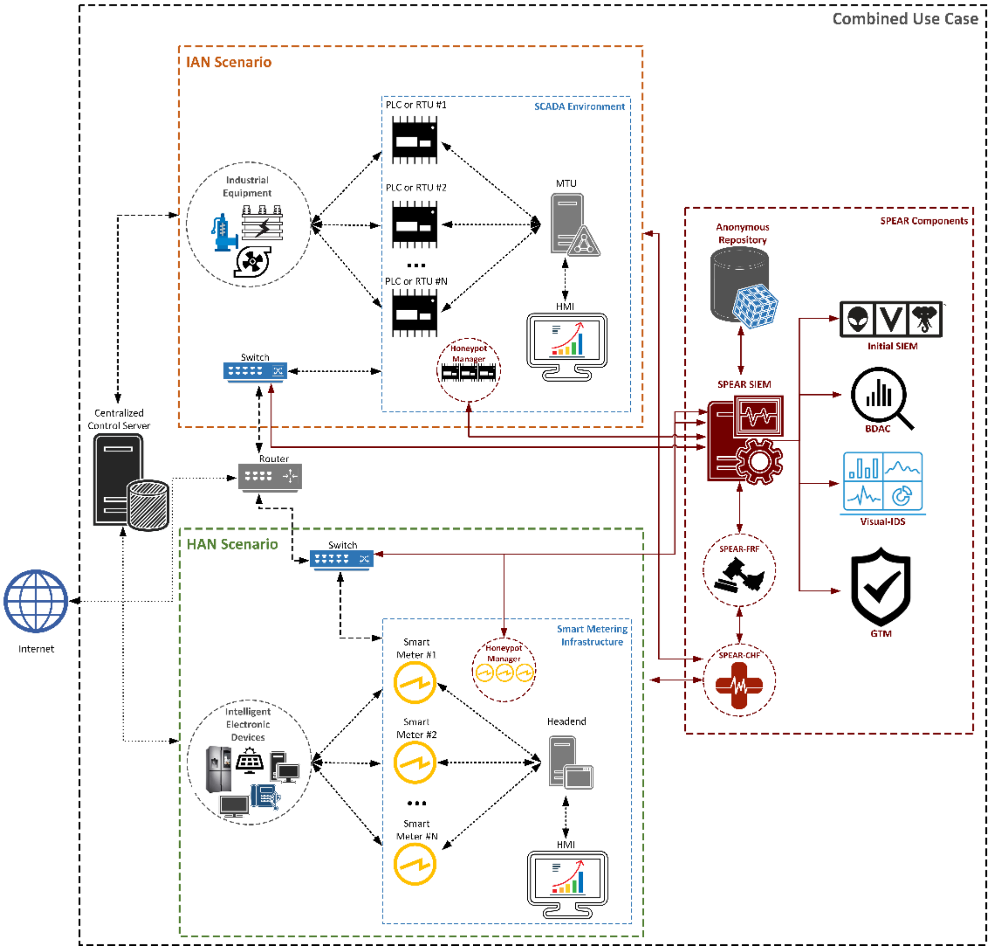

Figure 5: The Combined IAN and HAN Scenario architecture diagram

A second combined scenario will be deployed in Lavrio and will test the SPEAR platform in a larger scale. This scenario will be deployed in the new unit of the Lavrio 378 MV combined cycle natural gas thermal power plant and involves a greater variety of industrial equipment, compared to the TRSC scenario, that feeds with signals and data the rest of the Lavrio scenario infrastructure, in a similar way with the combined scenario of TRSC

3.2.3.2 Components and related data for the scenario

Components existing in the combined use case are the followings:

- **Industrial equipment**, like power generators, turbines, water/oil pumps and wastewater treatment plants generate signals and data like power generation or consumption, voltage, current and power metrics.

- **Non-industrial equipment** that includes end devices, like personal computers and printers, as well as intermediate devices, like router and switches.

- **PLCs**, that interface non-TCP/IP physical devices to the SCADA system and the rest of the control infrastructure as well as MTUs that acquire data from PLCs. Smart meters are used in the HAN scenarios in order to acquire data from non-industrial equipment.

The potential SPEAR components to be integrated and the required functionalities from them are the following:

- **The SPEAR SIEM** tool that includes the AlienVault OSSIM, the Big Data Analytics Component (BDAC), the Visual-aided Intrusion Detection System (Visual-aided IDS) and the Grid Trusted Module (GTM). The SIEM collects data in a distributed way, using sensors, and performs sophisticated analysis that aims to detect cyber-attack attempts. The incidents are illustrated on a visual-aided dashboard in near-real time. The SIEM tool is the component that integrate all innovative technologies that SPEAR uses like advanced analytics, graphical-aided visualisation techniques and trust management mechanisms.

- **The Honeypot Manager** that hosts Honeypot VMs, which emulate real PLCs and protocols.

Regarding the data that is collected during the deployment of the combined use case and the project's lifespan, the following are recognized:

- **Industrial devices**, PLCs and smart meters exchange real-time data that include commands addressed from control units as well as acquired data, like electrical metrics (voltage, current, power consumption) and logs that contain firmware version, warnings and errors that occur.

- **Honeypots** that simulate the behaviour of PLCs and record detailed logs regarding the network traffic that they receive from potential attackers.

Outputs

- **The visual-based IDS** of the SPEAR SIEM will provide visualised output of the communications and security incidents in the smart grid.

- **Honeypot**s will store in log files input commands and application-layer payload of incoming network traffic data. These logs are stored in honeypots and transferred to the SPEAR SIEM for further processing.

3.2.3.3 Combined IAN and HAN use case scenarios definition

Table 13 describes the combined IAN and HAN scenarios while figure 8 shows the roles of the actors identified for this use case.

Table 13: The Combined IAN and HAN scenario definition

Use case	Scenario ID and Title	Priority level	Related requirements
UC3. Combined	SC3.1. Detection and reaction to cyber-attack in the combined IAN and HAN of TRSC.	High	UR-01, UR-02
	SC3.2. Detection and reaction to cyber-attack in the large-scale IAN of Lavrio unit.	High	UR-01, UR-02
	SC3.3. Detection and reaction to cyber-attack in the HAN of TRSC.	High	UR-01, UR-02
	SC3.4. Honeypots operation in the combined IAN and HAN.	High	UR-12, ER-02

Figure 6 illustrates a high-level diagram of the combined use cases, that relates actors and use cases scenarios with the SPEAR components. More specifically, in the combined use case, the following actors are identified:

- **SPEAR Security Engineer:** Is the person that installs, operates, maintains and monitors the SPEAR platform in the combined use case scenarios. This person is considered to have technical expertise and has elevated privileges over the control of the SPEAR platform. This person also monitors the security status of the system through the SPEAR’s visual-aided IDS and receives notifications from the SPEAR SIEM in case of any security incident or breach.
- **IAN operator:** Is the person that has some technical expertise and interacts with the industrial equipment, installs and maintains PLCs, MTUs and the HMI. This person has knowledge of the SPEAR tool and their interactions has indirect effect on the SPEAR outputs.
- **HAN user:** Is the person, a simple user with probably no technical background, that operates electronic devices, which, in turn, feed smart meters with data. Similar to the IAN operator, this person has knowledge of the SPEAR tool and their interactions have indirect effect on the SPEAR outputs.
- **Cyber-attacker:** Is the person that performs cyber-attacks against PLCs and smart meters, or against honeypots.

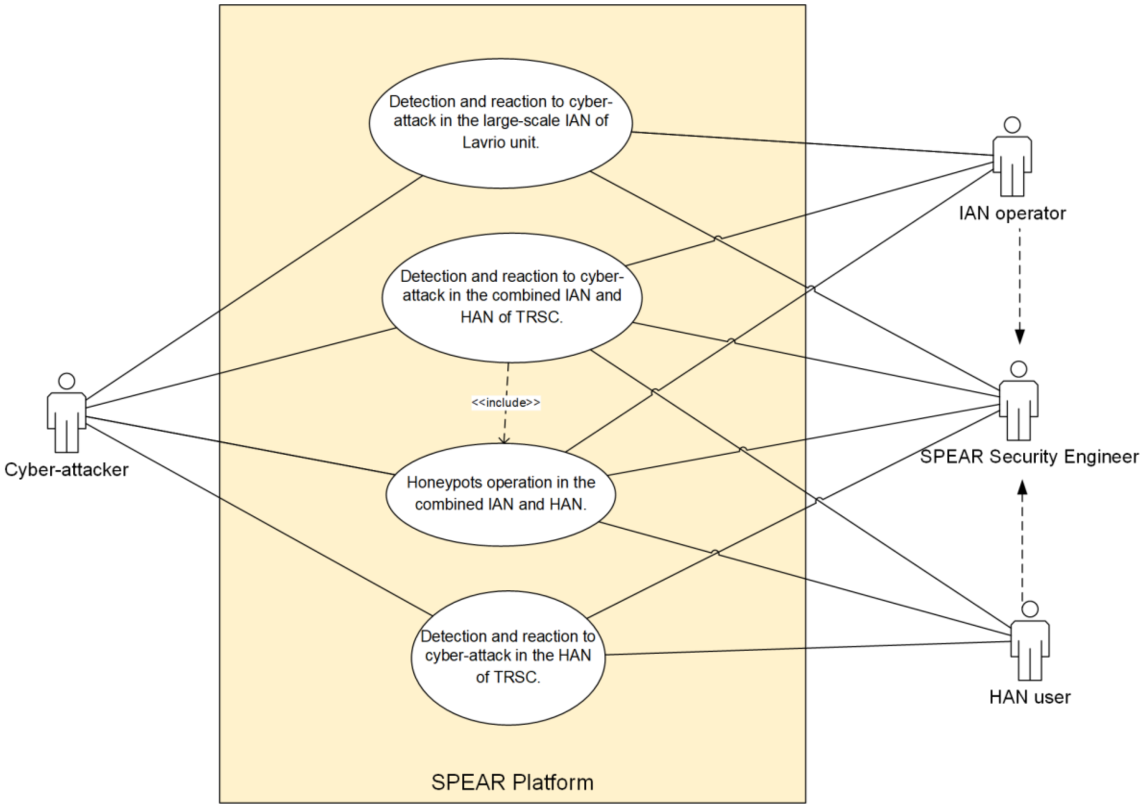
Detection and reaction to cyber-attack in the large-scale IAN of Lavrio unit.
Detection and reaction to cyber-attack in the combined IAN and HAN of TRSC.
<<include>>
Honeypots operation in the combined IAN and HAN.
Detection and reaction to cyber-attack in the HAN of TRSC.
SPEAR Platform
Cyber-attacker
IAN operator
SPEAR Security Engineer
HAN user

Figure 6: High-Level description of the Combined IAN and HAN use case scenarios, roles and components

3.2.3.4 Scenarios description

Tables 14, 15, 16 and 17 describe the use case scenarios for the Combined IAN and HAN in Greece. These tables showcase what each scenario of the use case is targeted at as well as the evaluation criteria.

Table 14: Detection and reaction to cyber-attack in the combined IAN and HAN of TRSC

Scenario Name	SC3.1. Detection and reaction to cyber-attack in the combined IAN and HAN of TRSC.
Related Use Case	UC3. Combined
Scenario description	
Brief Description	This scenario showcases how SPEAR performs in a mixed smart grid environment, which is located in TRSC premises and consists of an IAN that hosts industrial devices, like PLCs, and a HAN that hosts non-industrial equipment, like smart meters.
Challenges	1. Ability to detect various kind of attacks against both PLCs and smart meters and can cause service disruption or data leaks. 2. Early detection of each kind of attack.
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The SPEAR security engineer monitors the system through the visual-aided IDS.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool and/or by the security engineer, all needed information for the SPEAR FRF (system logs and network packets), has been securely

	stored in the Smart grid Database, the reputation of the attacked node has been updated in the GTM and the attack has been reported to the SPEAR RI.
Involved Actors	1. IAN operator 2. HAN user 3. SPEAR security engineer 4. Cyber-attacker
Scenario Initiation	An attacker launches an attack against a PLC or a smart meter of TRSC
Main Flow	1. The attacker launches a DDoS attack against both PLCs and smart meters of TRSC. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious and notifies the security engineer, or the security engineer notices the unusual traffic through the visual-aided IDS and the SPEAR SIEM dashboard, and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the devices under attack are updated in the GTM component. 5. The incident is being recorded in SPEAR RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 15: Detection and reaction to cyber-attack on in the large-scale IAN of Lavrio unit

Scenario Name	SC3.2. Detection and reaction to cyber-attack on in the large-scale IAN of Lavrio unit.
Related Use Case	UC3. Combined
Scenario description	
Brief Description	This scenario showcases how SPEAR performs in a large-scale Industrial Area Network in the PPC's power plant in Lavrio Unit No.5. This scenario includes PLCs that acquire signals and data from the industrial equipment and make them available to MTUs and the HMI.
Challenges	1. Ability to detect various kind of attacks against PLCs that can cause service disruption. 2. Early detection of each kind of attack.
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The SPEAR security engineer monitors the system through the visual-aided IDS.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool and/or by the security engineer, all needed information for the SPEAR FRF (system logs and network packets), has been securely stored in the Smart grid Database, the reputation of the attacked node has been updated in the GTM and the attack has been recorded in the SPEAR RI.
Involved Actors	1. IAN operator 2. SPEAR security engineer

	3. Cyber-attacker
Scenario Initiation	An attacker launches an attack against a PLC of the Lavrio unit
Main Flow	1. An attacker launches a DoS attack against a PLC of the Lavrio unit. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious and notifies the security engineer, or the security engineer notices the unusual traffic through the visual-aided IDS and the SPEAR SIEM dashboard, and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The PLC's reputation is updated in the GTM component. 5. The incident is being recorded in SPEAR RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 16: Detection and reaction to cyber-attack in the HAN of TRSC

Scenario Name	SC3.3. Detection and reaction to cyber-attack in the HAN of TRSC.
Related Use Case	UC3. Combined
Scenario description	
Brief Description	This scenario showcases how SPEAR performs in a Home Area Network, which contains smart meters that retain data from various Intelligent Electronic Devices (IEDs). Those devices are placed at offices and non-industrial environments of the TRSC lab.
Challenges	1. Ability to detect various kind of attacks that aim smart meters and can cause service disruption or privacy violations. 2. Early detection of each kind of attack.
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The SPEAR security engineer monitors the system through the visual-aided IDS.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool and/or by the security engineer, all needed information for the SPEAR FRF (system logs and network packets), has been securely stored in the Smart grid Database, the reputation of the attacked node has been updated in the GTM and the attack has been recorded in the SPEAR RI.
Involved Actors	1. HAN user. 2. SPEAR security engineer. 3. Cyber-attacker.
Scenario Initiation	The attacker launches a DoS attack against a smart meter of TRSC
Main Flow	1. The attacker launches a DoS attack against a smart meter of TRSC. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious and notifies the security engineer, or the security engineer notices the unusual traffic

	through the visual-aided IDS and the SPEAR SIEM dashboard, and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The smart meter's reputation is updated in the GTM component. 5. The incident is being recorded in SPEAR-RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 17: Honeypots operation in the combined IAN and HAN

Scenario Name	SC3.4. Honeypots operation in the combined IAN and HAN.
Related Use Case	UC3. Combined
Scenario description	
Brief Description	Honeypots are security devices that aim to attract and capture traces from cyber-attackers. This scenario investigates how well the SPEAR honeypots perform in a combined scenario, where both industrial and home networks exists.
Challenges	• Honeypots should simulate device and protocols that are in the combined scenario, in a realistic way. • Honeypots should capture all the activity of the attackers. • The SPEAR Platform should analyse the data captured by the honeypots and study for new attack patterns.
Assumptions & Pre-Conditions	Honeypots are installed and connected to the local network as part of the SPEAR Platform. It is assumed that the honeypots will simulate AMI devices of the system such as PLCs, smart meters and industrial protocols that those devices use to communicate with the rest of the topology.
Goal (Successful End Condition)	The execution of this scenario is considered successful when the SPEAR Platform collects the syslogs and traffic from the honeypots, by using anti-honeypot strategies in order to attract the attackers to the honeypots.
Involved Actors	1. HAN user. 2. IAN operator. 3. SPEAR security engineer. 4. Cyber attacker.
Scenario Initiation	An attacker launches a DoS attack against the honeypot VMs of TRSC.
Main Flow	1. The SPEAR platform applies the game theory model to attract the attacker to the honeypot, to avoid that the attacker targets a real smart grid device in operation. 2. An attacker launches a DoS attack against the honeypot of TRSC. 3. The honeypot records logs of the incoming traffic and forwards them to the SPEAR SIEM. 4. The SPEAR BDAC anomaly detection algorithms identify an attack by analysing the incoming logs and, therefore, notifies the security engineer, or the security engineer

	notices the attack through the visual-aided IDS and the SPEAR SIEM dashboard.
Evaluation Criteria	The SPEAR SIEM has received logs and traffic from honeypots and it has analysed all the data in order to detect new attack patterns.

3.2.3.5 User stories for the combined use case

I. The SPEAR-SIEM in a combined network infrastructure to detect cyber-attacks against smart meters or PLCs.

Jane, the SPEAR security engineer, has deployed and activated the SPEAR SIEM platform in the TRSC lab, in order to monitor the HAN and IAN networks that host industrial equipment, PLCs, smart meters and IEDs. Jane uses the SPEAR SIEM to early detect attack attempts and to take immediate actions that protect the lab's property from availability, integrity or any data leak. Jane checks periodically the visual-aided IDS of the SPEAR SIEM in order to be aware of the network's security status. At some point, suspicious packets are received by devices in the networks. The SPEAR BDAC anomaly detection algorithms realise that there is an ongoing attack and therefore notifies Jane, who in turn acts promptly in order to protect the lab's equipment. At the same time attack information, needed by the SPEAR-FRF (system logs and network packets), has been securely stored in the Smart grid Database, in order to form evidence at the court, whilst the SPEAR RI is informed about the incident and the GTM component updates the reputation score of the devices that have been attacked.

II. Using the SPEAR honeypots to identify cyber-attackers

Alongside with the SPEAR SIEM, Jane has deployed a honeypot manager, a software that hosts and orchestrates Virtual Machines (VMs). Each VM represents a honeypot that imitates PLCs or smart meters that are located in HAN and IAN networks and could be targets of attacks. Jane uses honeypots for two main reasons, firstly to identify attackers and record valuable information about them and their attack strategies and, secondly, to protect the real infrastructure from being harmed or exploited. Jane has launched some honeypots and she checks regularly the visual-aided IDS for events that are generated by those honeypots. When an attack takes place, Jane receives near real time notifications about the security event and, concurrently, the SPEAR platform investigates the situation and, if it is necessary, attempts to orchestrate honeypot VMs through the Honeypot Manager, in order to counteract the attack. While the threat is confronted, attack information, needed by the SPEAR-FRF (system logs and network packets), is securely stored in the Smart grid Database, in order to form evidence for the court, the SPEAR RI is updated with the incident and the GTM component is updated accordingly.

III. Testing and evaluating the SPEAR SIEM

Jane wants to test the SPEAR SIEM tool and its ability to timeously detect a cyber-attack in the combined infrastructure. Therefore, she decides to simulate a DDoS attack against the devices in the combined internetwork. To achieve this attack, Jane writes a computer script that spans a number of "zombies" hosts that flood network devices with packets, thus causing a Denial of Service. Shortly after launching the attack, Jane receives a notification from the SPEAR SIEM about the detected unusual traffic which indicates an attack. By receiving this notification, Jane verifies the effectiveness of the anomaly detection algorithms of the SPEAR BDAC.

3.2.4 Use Case 4: The Smart Home Scenario

3.2.4.1 Description of the Smart Home use case

The Smart Home is a near-Zero Energy Building, based on state of the art construction materials (insulations, windows, etc.) with smart technologies that provide various ICT research topics like energy efficiency and automation in Renewable Energy Resources. The Smart House is equipped with a multi-sensorial network and smart appliances that measure in real-time almost every challenging aspect of a modern house/work place (energy, occupancy, use of grey water collected, net metering, etc.).

3.2.4.2 Components and related data for the Smart Home scenario

The components existing in the Smart Home are explained below:

- **The PV installation is a Photo-Voltaic system of 10kW for energy production and storage.** It is connected with the electric grid of the Public Power Corporation. It is also connected on the Smart-Home network for data measurement acquisition, management and control. The smart-inverter collects energy measurement and status data for the PV-installation through the Smart-Home network. Additionally, the smart-inverters has a command and control functionality to control the status of the smart-grid equipment.

- **The smart devices** are split in two categories, those using gateways and those connected straight on the Smart-Home network. Most of the smart devices, sensors and actuators are connected on the network through the gateways. The gateways collect and forward messages in both directions between the servers and the smart devices. These messages transfer different types of data related with people counting in the rooms of Smart-Home, control data for the use of home-appliances, multi-sensorial measurement data (temperature, humidity, etc.) and water consumption data.

- **The Smart-Home network** is a centralized IoT architecture. It is based on a central server which collects all the measurements from distributed nodes.

The potential SPEAR components to be integrated and the required functionalities from them are the following:

- **SPEAR Security Information and Event Management (SIEM)** system with its related components, namely big data analytics, visual-aided intrusion detection system (IDS), and grid trusted module (GTM). The data that will be collected for the development of big data analytics and visual-aided IDS components are related to the incoming/outgoing network traffic of the Smart-Home. This traffic includes packets and messages from all the smart devices connected in the Smart Home and is collected by utilizing the port mirroring functionality.

- **A honeypot** imitating a smart device will be used to attract adversaries and gather information for the attacks against the Smart-Home network.

Outputs:

- **Visual-based IDS**: After the deployment of SPEAR SIEM, the visualization tool will give as output an overview of the communications between Smart Home's nodes and the energy consumption, and notifications about security incidents.
- **GTM**: The GTM component will keep database records concerning the reputation of Smart Home's nodes such as reputation metrics, number of intrusions, location of the intrusion (i.e. room, device) etc.

3.2.4.3 Smart Home use case scenarios definition

Table 18 describes the Smart Home scenarios while Figure 10 shows the roles of the actors identified for this use case.

Table 18: The Smart Home scenarios

Use case	Scenario ID and Title	Priority level	Related requirements
UC4. Smart Home	SC4.1. Detection and notification about cyber-attacks against the smart-grid equipment of the Smart-Home.	High	UR-01, UR-02
	SC4.2. Detection and notification about cyber-attacks against the smart-devices in the Smart-Home.	High	UR-01, UR-02
	SC4.3. Detection and notification about cyber-attacks against the gateways in the Smart-Home.	High	UR-01,UR-02
	SC4.4. Honeypot operation in Smart-Home.	Medium	UR-12, ER-02

Figure 7 visualizes the Smart-Home Use Case Roles and their connection with the use case scenarios. There are three roles,

- **Facility manager:** This user is responsible for using, monitoring and maintaining the SPEAR installation in the Smart-Home. This is the most important user of the SPEAR system in this use case.
- **Smart-Home End-User:** This user is a simple user of the Smart-Home network and equipment. The behaviour of this user has an indirect effect on the SPEAR system. This user is aware of the SPEAR system and the provided security services but he/she has limited or no access to the SPEAR system.
- **Smart-Home cyber-attacker:** This user is the cyber-attacker against the Smart-Home infrastructure.

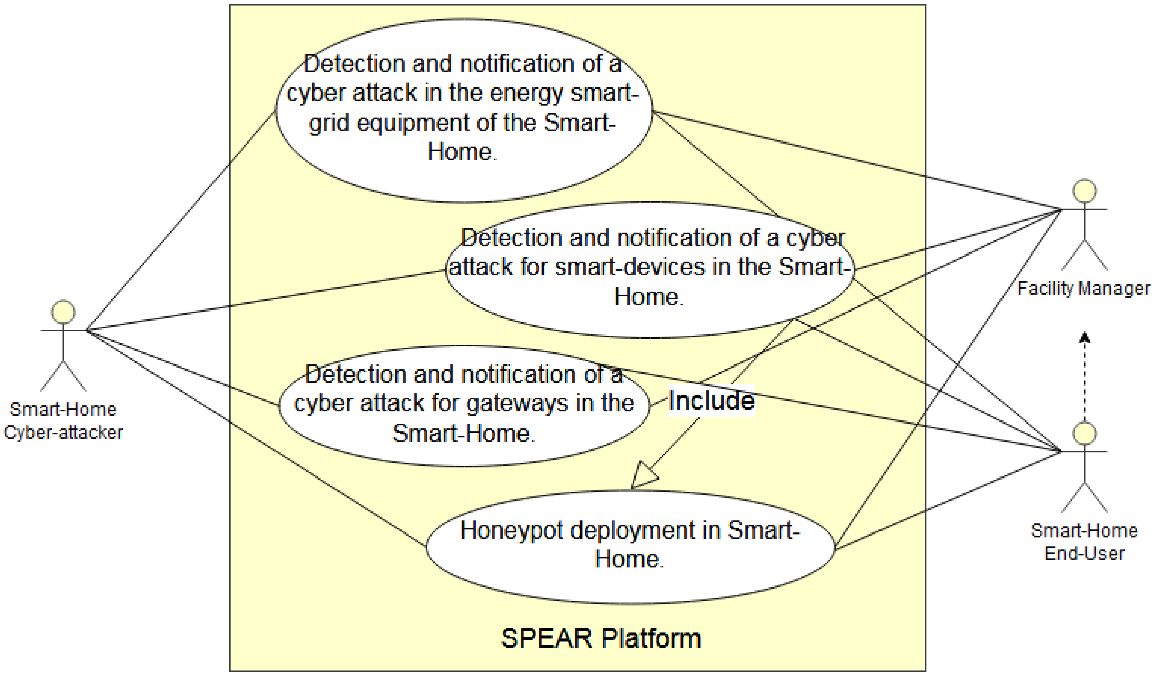
Detection and notification of a cyber attack in the energy smart-grid equipment of the Smart-Home.
Detection and notification of a cyber attack for smart-devices in the Smart-Home.
Detection and notification of a cyber attack for gateways in the Smart-Home.
Include
Honeypot deployment in Smart-Home.
SPEAR Platform
Smart-Home Cyber-attacker
Facility Manager
Smart-Home End-User

Figure 7: High-Level Description of the Smart-Home Use Case Roles in the use case scenarios

3.2.4.4 Scenarios description

Tables 19, 20, 21 and 22 describe the use case scenarios for the Smart Home in France. These tables showcase what each scenario of the use case is targeted at as well as the evaluation criteria.

Table 19: Detection and notification about a cyber-attack against the smart-grid equipment of the Smart-Home

Name	SC4.1. Detection and notification about cyber-attacks against the smart-grid equipment of the Smart-Home.
Related Use Case	UC4. Smart Home
Scenario Description	
Brief Description	The Smart-Home has a PV-installation and smart-meters which are key elements of the future smart-grids. Smart-grid services such as monitoring the power consumption/production and controlling of the inverters of a PV-installation can be a target to cyber-attackers. This scenario showcases how the SPEAR system detects attacks on the smart-grid equipment and services.
Challenges	1. Ability to detect different kinds of attacks concerning confidentiality, integrity and availability. 2. Timely detection of the attack.
Assumptions & Pre-Conditions	1. The SPEAR system is up and running. 2. The facility manager is monitoring the system via the visual IDS and the SPEAR SIEM dashboard.
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool or by the facility manager, all needed information for the SPEAR-FRF

	(system logs and network packets), has been securely stored in the Smart grid Database, the reputation of the attacked node is updated in the GTM and the attack has been recorded in the SPEAR-RI.
Involved Actors	1. Smart-Home end-user 2. Smart-Home facility manager 3. Cyber attacker.
Scenario Initiation	An attacker launches an attack against the Modbus TCP/IP protocol.
Main Flow	1. The attacker sends TCP packets exceeding the maximum length to the Modbus client and server trying to succeed with a buffer overflow attack. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the facility manager monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the inverters/chargers is updated in GTM component. 5. The incident is being recorded in SPEAR-RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions.

Table 20: Detection and notification about cyber-attacks against the smart-devices in the Smart-Home

Scenario Name	SC4.2. Detection and notification about cyber-attacks against the smart-devices in the Smart-Home.
Related Use Case	UC4. Smart Home
Scenario Description	
Brief Description	The Smart-Home includes various smart devices supporting different services. This scenario showcases how the SPEAR system detects attacks on the smart-devices and the services they support.
Challenges	1. Ability to detect different kinds of attacks concerning confidentiality, integrity and availability. 2. Timely detection of the attack
Assumptions & Pre-Conditions	3. The SPEAR system is up and running 4. The security engineer is monitoring the system via the visual IDS
Goal (Successful End Condition)	The attack has been successfully identified by the SPEAR SIEM tool or by the facility manager, all needed information for the SPEAR-FRF (system logs and network packets), has been securely stored in the Smart grid Database, the reputation of the attacked node is being updated in the GTM and the attack has been recorded in the SPEAR-RI.
Involved Actors	1. Smart-Home end-user 2. Smart-Home facility manager 3. Cyber attacker.
Scenario Initiation	An attacker launches a DDOS attack against the energy meters

Main Flow	1. The attacker injects a large amount of false requests. 2. The SPEAR BDAC anomaly detection algorithms identify the incoming traffic as malicious or the facility manager monitoring the system via the visual IDS component and the SPEAR SIEM dashboard, notices the unusual traffic and identifies the attack. 3. System logs and network packets are securely stored in the Smart grid Database. 4. The reputation of the energy meters that have been attacked is updated in the GTM component. 5. The incident is being recorded in SPEAR-RI without revealing any private information.
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions

Table 21: Detection and notification about cyber-attacks against the gateways in the Smart-Home

Name	SC4.3. Detection and notification about cyber-attacks against the gateways in the Smart-Home.
Related Use Case	UC4. Smart Home
Scenario Description	
Brief Description	In the Smart-Home, there are various gateways supporting multi-sensor devices and end-user services. This scenario showcases how the SPEAR system detects a cyber-attack on the gateways and the services they support.
Challenges	1. A major challenge in this scenario is the research and detection of active vulnerabilities and specific exploits that apply in the Smart-Home equipment. 2. A big challenge for this scenario is the reset of the Smart-Home equipment after the execution of the cyber-attack and the restoring of the system back to normal operation.
Assumptions & Pre-Conditions	It is assumed that in the beginning of the experiment the gateways are operating normally and no other cyber-attack or malfunction is applied on the equipment.
Goal (Successful End Condition)	The SPEAR SIEM detects and reports the applied cyber-attacks or abnormal events against the gateways in the Smart-Home.
Involved Actors	1. Smart-Home end-user 2. Smart-Home facility manager 3. Cyber attacker.
Scenario Initiation	The hardware and software of the gateways is updated and the equipment is working in normal operation supporting the Smart-Home services.
Main Flow	In this scenario, different experiments and cyber-attacks will be investigated against the gateways of the Smart-Home. In particular the most important vulnerabilities will be exploited in order to reveal the weaknesses on the gateways of the Smart-Home.

	The main flow of the execution of the experiments is described here by the application of a DoS cyber-attack against a Smart-Home gateway. A similar main flow can be applied for other attacks also. 1. Initiate the gateways and the connected devices under attack. 2. Prepare the tools (software, scripts, hardware, etc) to apply the cyber-attack or emulate an abnormal event against the infrastructure. 3. Launch the cyber-attack against the Smart-Home infrastructure. 4. Verify the expected effect of the cyber-attack on an infrastructure level. 5. Verify the response of the SPEAR-SIEM tool at the cyber-attack. 6. Register and report the results. 7. Restart the system under attack and bring it back into normal operation. Regarding the gateways the available vulnerabilities are defined by the current version of hardware, firmware/software, the communication protocols, the network architecture and the preservation of the security properties (confidentiality, integrity, non-repudiation, availability).
Evaluation Criteria	SPEAR detects the attack and notifies the security engineer allowing him to take appropriate remedial actions

Table 22: Honeypot operation in Smart-Home

Scenario Name	SC4.4. Honeypot operation in Smart-Home.
Related Use Case	UC4. Smart Home
Scenario Description	
Brief Description	The honeypots are cyber-security systems which try to capture and track the behaviour of a cyber-attacker against the Smart-Home network. This scenario showcases how the SPEAR honeypot works in a Smart-Home and describes the recorded action of a cyber-attacker targeting smart-devices and the services they support.
Challenges	A major challenge in this scenario is the research and detection of active vulnerabilities and specific exploits that apply in the Smart-Home equipment.
Assumptions & Pre-Conditions	The honeypot is installed and connected in the Smart-Home network. It is assumed that the honeypot will simulate a Smart-Home equipment or service (smart-device, protocols, etc).
Goal (Successful End Condition)	The execution of this scenario is considered successful when the honeypot records the behaviour of a cyber-attacker executing a pre-defined cyber-attack against the simulated equipment.
Involved Actors	1. Smart-Home end-user 2. Smart-Home facility manager 3. Cyber attacker.

Scenario Initiation	The honeypot is installed and configured to record in log files the behaviour of a cyber-attacker on a public IP visible from outside of the Smart-Home equipment.
Main Flow	In the main flow of this scenario the following steps present an execution script, 1. Initialize and start the execution of the honeypot software. 2. Verify that the honeypot records the cyber-attacker actions. 3. Execute the steps of a cyber-attack against the emulated Smart-Home equipment or service. 4. Collect the log-files. 5. Interpretation and assignment of the registered information in the log-files with the cyber-attack actions.
Evaluation Criteria	The attack is successfully recorded by the SPEAR honeypot and the facility manager takes the appropriate remediation actions.

3.2.4.5 User stories for the Smart home use case

I. Using the SPEAR honeypot in Smart-Home environment.

John, the Smart-Home facility manager is using honeypots for two main reasons. One reason is to record and study the behaviour of the cyber-attackers against the Smart-Home equipment, network and protocols. The other reason is to prevent the cyber-attackers from exploiting or damaging valuable Smart-Home infrastructure by imitating critical infrastructure in the Smart-Home with the use of the honeypots. John, has installed and launched a honeypot in the Smart-Home network. He is checking the log-files on a constant base in order to detect and understand suspicious operations against the Smart-Home infrastructure and services. When John, detects a suspicious behaviour he investigates the steps in the log-files and at the same time he is using the SPEAR SIEM to see if other infrastructure is under a cyber-attack or experiencing abnormal events.

II. Using SPEAR-SIEM in Smart-Home environment to detect cyber-attacks against smart devices

John the Smart-Home facility manager, as usual is monitoring the system to find any suspicious event that could lead to a security breach in the Smart-Home. John uses the SPEAR tool for identifying anomalies in the Smart-Home's network traffic. At some point John receives a notification from SPEAR, warning him of a severe security event. The anomaly detection algorithms have identified unusual network traffic behaviour. John uses the visual-based IDS in order to investigate the event in more depth by observing different aspects of the network data and notices a large amount of received TCP packets, concerning specific smart energy meters for a time-period. He understands that the energy meters are under a DDOS attack and he immediately takes counter-measures to confront the attack and assure the availability of energy meters. Also attack information, needed by the SPEAR-FRF (system logs and network packets), is securely stored in the Smart grid Database, in order to form evidence for the court while the GTM component updates the reputation score of the smart meters that have been attacked.

III. Using SPEAR-SIEM in Smart-Home environment to detect cyber-attacks against gateways

This time John wants to test the SPEAR-SIEM tool and its ability to timeously detect a cyber-attack against Smart Home's gateways, so he decides to simulate an attack himself on a server and see how SPEAR responds. To achieve this, he writes an attack script to make a "zombie" device launch a DoS attack against the server. Shortly after launching the attack, John receives a notification from SPEAR that warns him about the unusual traffic detected by the SPEAR-SIEM which indicates an attack. John verifies the effectiveness of the anomaly detection mechanism of SPEAR-SIEM, restores the system to normal operation and is ready to prepare more tests to detect any vulnerabilities concerning the Smart-Home equipment and further test detection capabilities of SPEAR-SIEM.

3.3 User Requirements Specification list

From the sections 3.1 and 3.2, the following user requirements have been identified. To achieve agreement with the system developers, teleconferences were organised and documents shared and reviewed among relevant partners.

Table 23: User requirements specification list

Req. id	Req. Title	Req. Description	Priority High I medium I Low}
UR-01	**Quick time of detection and response**	The SPEAR solution must be able to quickly detect and respond to cyber-attacks in a reasonable timeframe	High
UR-02	**Detection of known attacks**	The SPEAR solution must be able to detect attacks such as DoS, DDoS, brute force, man in the middle, SQL attacks, breach inside LAN	High
UR-03	**Availability**	• The security engineer must be able to access the SPEAR system 24/7; • The Smart-Home end-users must be able to have collected data on request according to the GDPR	High Medium
UR-04	**Secure transmission of data**	The SPEAR system must be able to ensure protection of data in transit.	High
UR-05	**Visualisation of different anomalies/attacks timeframes**	The security engineer must be able to visualises and filters different anomalies/attacks in different timeframes	High
UR-06	**A visual-added IDS with a central panel with option on specific IP devices or severity of events**	The security engineer must be able to assess a security event indicated by SPEAR-SIEM depending on the severity of the event	Medium
UR-07	**Remote notification**	The SPEAR solution must be able to support the offsite security engineers to receive a notification as soon as an anomaly has been identified by the SPEAR-SIEM through email notification	High
UR-08	**Information sharing of threat intelligence**	The SPEAR solution must be able to support gathering, sharing, storing and correlation of indicators of compromise of targeted	High

		attacks, threat intelligence and vulnerability information in a secure manner	
UR-09	**Common form of timestamps**	The SPEAR solution must be able to indicate unified timestamps across plant devices	High
UR-10	**Comply with relevant best practices, standards and laws**	The SPEAR Platform must support the smart grid system to be compliant to the data protection and security standards related to the functionalities offered (such as monitoring, or forensic auditing, or PIA).	High
UR-11	**Maintain privacy of personal data**	Personal data must be processed in compliance with data protection law	High
UR-12	**Reliability of tool**	The tool shall be able to add value to the business model of users	High
UR-13	**Differentiation of attacks**	The SPEAR system must be capable of differentiating cyber-attack from other anomalies caused by e.g., extreme weather conditions	High

4. Privacy Requirements Definition

Chapter 4 indicates that end-users consider privacy as key in their business operations and that overall, personal data shall be processed during the project development phase (e.g., network data from the honey pot, including IP address) which triggers the rules of personal data processing under EU law. In the second phase as well, that is, in real-life usage of the SPEAR tool, personal data shall certainly be processed by SPEAR components, for example, the SPEAR SIEM and SPEAR FRF. All these indicate the need to design the SPEAR system in compliance with extant data protection law. This will be discussed in the next sections.

4.1 Overview of privacy and personal data protection in European Law

From a regulatory point of view, the processing of personal data triggers compliance requirements with privacy and data protection law. Privacy and data protection are different but interrelated concepts that centre, among other things, on the ability of the data subjects to control the use of their data [63]. Both terms are interchangeable in this report. These requirements for privacy protection stems from the right to respect for private life and the right to personal data protection, which are closely related fundamental rights under European law [11], [12], [13]. Both international law and European law provide for these rights [16], [18]. The GDPR is currently the main overarching secondary law instrument within the EU on the right to data protection, and is the most appropriate secondary instrument applicable to the SPEAR platform and will be the focus of subsequent analysis. Other sector-specific instruments operate side-by-side with the GDPR where necessary [14]. It is notable that EU Member States have transposed various data protection laws into their domestic law including the GDPR. Only the relevant national frameworks will be analysed for the purposes of the SPEAR use cases.

According to Article 4 (1) of the GDPR, personal data means:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* [6].

This is a broad definition covering all information which may be linked to a person. These could be instances where a person is directly identified or where certain information may be combined before identifying a person. The Article 29 Working Party identified four closely intertwined elements or building blocks in the definition of personal data [19]. They are: first, "any information" which must be interpreted widely to accommodate information from the points of view of its nature, content or format. Second, "relating to" which focuses on when the content of information is about an individual, or if the purpose is to assess an individual or if its result will impact on the individual's rights and interests. Third, "identified or identifiable", in which a person counts as identified if he/she can be distinguished from a group of persons, and identifiable if his/her identification is possible through the aid of identifiers that relate to the individual, such as name, date of birth, address, IP address, etc. Here, account should be taken of all the means reasonably likely to be used to identify a person. As such, "personal data that has been de-identified, encrypted or pseudonymised, but can be used to re-identify a person remains personal data and falls within the scope of the law." By contrast, where personal data has been rendered anonymous in such a way that the individual is not or no longer identifiable, it is no longer considered personal data. That is, the anonymization must be irreversible. Finally, the fourth element, "natural person" operates as a limiting condition, by indicating that only living human beings are the subject of the rights protected under the GDPR.

It is worth emphasizing here that the Court of Justice of the European Union (CJEU) has ruled that IP address is personal data [20], [21]. In *Breyer v Bundesrepublik Deutschland*, the Court held that "a dynamic

IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data […], in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person" [20].

It is incumbent on information system developers to design their systems to comply with data protection principles and requirements, which has been captured succinctly by the principle of data protection by design [15]. These principles and obligations will be analysed in detail in the subsequent sections.

4.2 Key concepts, principles and obligations with respect to processing personal data

4.2.1 Processing of personal data

An important factor related to the definition of personal data is what amounts to the "processing" of such data. According to Article 4 (2) the GDPR, **processing** means:

> *Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* [6].

This is also a broad definition indicating that the data protection rules apply once personal data is processed (subject to certain exemptions) regardless of the means or technology used in the processing. In this regard, where the SPEAR platform processes IP addresses, or any other data that falls within the definition above, such data must be treated and protected as personal data. This means that the principles of data protection must be observed, in particular, there must be a legal basis for such processing.

4.2.2 Data protection principles

The GDPR contains basic principles for safeguarding the rights of data subjects [22]. These principles, enumerated in Article 5, represent general rules that express the fundamental obligations and limitations on processing personal data. Without explicitly imposing the manner in which these principles should be observed by data controllers and processors, these principles are:

1. **Lawfulness, fairness and transparency:** Article 5 (1)(a) requires that processing of personal data must be done lawfully, fairly and in a transparent manner in relation to the data subject. This principle comprises three in one: *Lawfulness* implies that data controllers must have legitimate grounds for processing personal data, and not use the data in ways that have unjustified adverse effects on the individuals concerned. The GDPR provides certain legal bases one of which the data controller could rely upon—consent, performance of contract, compliance with legal obligation, protection of the vital interest of the subject or another natural person, performance of public interest task, and legitimate interest of the controller or third party (art. 6). *Fairness* implies that personal data must be processed fairly and by implication, adhering to the other principles is an indication that the processing is fair. *Transparency* according to the Working Party is an overarching obligation applying to three central areas under the GDPR: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights; and (3) how data controllers facilitate the exercise of the data subjects' rights [23].

2. **Purpose limitation:** Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes according to Article 5 (1)(b). The principle of purpose limitation has two cornerstones: first, personal data must be collected for "specified, explicit and legitimate" purposes (purpose specification) and second, not be "further processed in a way incompatible" with those purposes (compatible use). This means that the purpose must be determined before commencing the data processing.

   However, the further use of data for compatible purposes is allowed on the ground of the initial legal basis in certain cases. Article 5(1)(b) provides instances of compatibility: "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes". Thus, further processing of retrospective data for compatible purposes (e.g., for scientific or historical research purposes or statistical purposes) is lawful, subject to implementation of appropriate safeguards such as pseudonymisation, anonymisation, encryption, etc., where necessary to protect the data subjects. This provision is relevant both for the development phase of SPEAR and the subsequent real-life use.

3. **Data minimization:** Data minimization is an important principle of data protection that must be taken into consideration when collecting data. As stipulated in Article 5(1)(c), personal data shall be adequate, relevant and limited to what is necessary for the purposes for which it is processed. Although the GDPR does not define "adequate and relevant" data, in effect, it means collecting and processing only the minimum amount of personal data needed to fulfil a certain purpose. Data that is no longer needed must be deleted.

4. **Accuracy:** Article 5 (1) (d) requires that that personal data processed shall be accurate and, where necessary, kept up to date. This implies that the data controller shall use every reasonable step to ensure that personal data that is inaccurate is erased or rectified.

5. **Storage limitation:** Personal data must not be kept in a form which permits identification of data subjects longer than is necessary for the purposes it is processed according to Article 5 (1) (e). This principle is meant to prevent the unlimited retention of personal data in a form which permits identification of data subjects. Data must be deleted or anonymised to comply with this principle. Personal data may, however, be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

6. **Integrity and confidentiality:** Personal data must be processed in a manner that ensures appropriate security of the data according to Article 5(1)(f). This includes protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures. This principle goes to the heart of data security, and introduces an obligation for proactive risk assessment of personal data undergoing processing. Some appropriate technical and organisational measure to secure such data have been suggested in Article 32 including pseudonymisation, encryption, regular risk assessment, logical and physical access controls, etc.

7. **Accountability:** The accountability principle requires the data controllers and processors to show how they comply with the principles and obligations imposed by the GDPR (Art. 5(2). They could demonstrate compliance in various ways depending on the complexity and nature of their data processing. These may include conducting a data protection impact assessment; documenting and creating a personal data inventory; implementing data protection by design and by default; developing a data privacy governance structure which may include appointing a Data Protection Officer; etc.

The implications of the above principles for the SPEAR platform are multifold. First, there must be a lawful basis for any processing of personal data in the platform. Second, the architecture must be designed with a focus on data protection: personal data processed in the platform must be for specific purposes, only the minimum amount of personal data necessary for fulfilling the identified purposed must be processed; personal data must not be stored for a period longer than necessary to fulfil the purpose of collection; as far as possible, only accurate data shall be processed. Third, personal data processed in the platform must be secured. Moreover, the platform must demonstrate that it processes personal data transparently and in compliance with the GDPR. This further implies complying with data controller obligations as will be elaborated below.

4.2.3 Data controller's obligations

The GDPR places various obligations on data controllers. These include:

- Observing the data protection principles, particularly, having a lawful basis for data processing (Art. 5);
- Implementing appropriate technical and organisational measures to ensure compliance (Art. 24);
- Implementing data protection by design and by default (Art. 25);
- For joint controllers, they must by means of an "arrangement" between them, apportion data protection compliance responsibilities between themselves (Arts. 4(7), 26); cf liability (Art. 26(3);
- Appointment of representatives by controllers outside the EU (Art. 27);
- Obligations related to appointment of processors (Art. 28);
- Keep a record of processing activities (Art. 30);
- Cooperate with the supervisory authorities (Art. 31);
- Ensure data security (Art. 32);
- Data breach notification (Arts. 33, 34);
- Carry out a Data Protection Impact Assessment (Art. 35);
- Enabling the rights of the data subjects (Art. 12);
- Data transfers to non-EU states (Arts 44 ff)

Below, some of these obligations that are immediately relevant for the SPEAR system design are highlighted.

4.2.3.1 Lawful processing basis

As noted above, under Article 5(1)(a) of the GDPR, lawful processing of personal data must be based on a legitimate basis. Article 6 of the GDPR provides an exhaustive list of these lawful bases as follows:

a) the data subject's specific consent;
b) processing is necessary for contract purposes;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject.

With respect to SPEAR, possible legal bases that could be identified from the list above largely depend on the purposes and actors involved in the use of the SPEAR platform. The table below shows these potential purposes and corresponding legal bases.

Table 24: Potential purposes and legal bases for processing data in SPEAR

SN	Purpose of data processing	Possible legal bases	Remarks
1	During the research phase of the project	A) Consent of the data subject; B) Exemptions for scientific research C) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party	Informed consent is designed for the SMART Home scenario, Processing data from the honey pot could be based on legitimate interest.
2	During the actual use of the platform after development for cybersecurity purposes	A) Compliance with a legal obligation of the controller (eg, NIS Directive) B) For contract performance C) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party	Depending on who deploys the SPEAR tools, the obligation to implement appropriate technical and organisational security under the NIS Directive or the transposing national law could be a legal ground for data processing. However, other legal bases such as consent could be possible in cases where the individual consumers (e.g. the smart home end-user) consents or contracts that such cybersecurity is integrated into his/her home. The contract of employment of the security personal using the SPEAR tools could also be a ground for data processing Where sensitive data is processed, then Article 9 of the GDPR becomes relevant as it provides specific legal

			bases for processing such data

It is important to point out that a balancing test is required to justify reliance on the legitimate interest of the data controller against that of the data subject (point f above) for the processing of personal data such as the IP address with the honey pot during the research phase of the project. For SPEAR, an argument could be made that conducting scientific research in the area of the cybersecurity is legitimate to advance the knowledge of the research institution that processes the data. This also has a public benefit in finding a solution to the issue of cyber-attacks against critical infrastructure. While on the other hand the, not informing the attackers or seeking their consent would put them on notice regarding their privacy right, this would jeopardize the research purpose. To balance this conflict, certain safeguards have been put in place. This include that the data will only be used for research purpose and no further steps will be taken to identify the real persons attacking the honey pot (see GDPR, art. 11). Only observation of the patterns used for the attack is relevant for the research. Second, as soon as possible, any data that could be used to identify a person such as the IP address obtained from the honey pot shall be anonymized or deleted when no longer needed. More importantly, data shall not be shared for prosecution or with law enforcement as this is beyond the purpose of the project.

4.2.3.2 Data protection by design and by default

This point has been alluded to earlier, and means that personal data processing systems shall be designed so that the protection of such data shall be an integral part of the systems (also known as privacy by design and by default) [24]. Article 25 of the GDPR captures this obligation, and requires in essence that the data controller both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which implement the data protection principles in an effective manner and to integrate the necessary safeguards into the processing for the protection of the data subjects' rights. The European Data Protection Supervisor (EDPS) also notes that data protection by design complements the controller's responsibility in Article 24. Four dimensions of this obligation have been identified in [32] as follows: (1) consideration of safeguards both at the design and operational phase, and clearly identifying the protection of individuals and their data within the project requirements, (2) adoption of a risk management approach (3) implementing measures appropriately and effectively and (4) integrating the identified safeguards into the processing.

Various suggestions and approaches on how to operationalise privacy by design have been made [25], [26], [27], [28], [30]. However, there is no consensus on this issue. An example by the European Union Agency for Network and Information Security (ENISA) documents certain strategies and ways of implementing privacy by design. ENISA emphasizes six data protection goals that should be targeted in privacy by design—Confidentiality, Integrity, Availability, Unlinkability, Transparency and Intervenability, as well as eight privacy design strategies—Minimise, Separate, Abstract, Hide, Inform, Control, Enforce, and Demonstrate [28], [29], [31]. Data protection by default is closely associated with the design [26], [27]. The Irish Computer Society suggests that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user [33]. As such, whenever default settings are pre-configured, they must be carefully chosen so that only personal data which are necessary for each specific processing purpose are in fact processed. The approach shall continue throughout the life cycle of the data processing operations [34].

The approach adopted in SPEAR is to define requirements with a focus on data protection by design and by default and specify them in this report as best as possible (see Section 6 for a list). This not only translates the legal requirements into practical controls and appropriate safeguards but will ensure that the tools are ready to be used in a compliant manner within the EU single market once they are fully developed.

4.2.3.3 Data Protection Impact Assessment

Article 35 (1) of the GDPR requires that where data processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, assess the impact of the envisaged processing operations on the protection of personal data. The GDPR envisages that the process of DPIA should operate hand-in-hand with the data protection by design approach, and should cover all aspects of personal data processing, ranging from collection to disposal. DPIA is particularly required where data processing involves a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing; processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or a systematic monitoring of a publicly accessible area on a large scale (art.35 (3)). The Working Party 29 has elaborated on these three examples and developed nine criteria to be considered by the national supervisory authorities when establishing their lists of processing requiring a DPIA [35].

Looking at the nature of the data processing envisaged in the SPEAR project, that is, monitoring of the network for cyber incidents (potentially on a large scale), as well as the potential processing of data that could be used for future criminal prosecution, a DPIA is required (See Work Package 4). Several templates and guidelines for conducting a DPIA exist such as [35], [36]. Moreover, the Expert Group 2 of the Smart Grid Task Force has published a second version of a DPIA template which is relevant to the SPEAR environment [7].

4.2.3.4 Enabling the rights of the data subjects

Chapter III (Articles 12-22) of the GDPR sets out a number of key rights enjoyed by the data subject in relation to processing that occurs with their data. A major aspect relates to the data subject's right to information and access to the information processed about him, thereby contributing to transparency, and operates, together with lawfulness and fairness, as a key principle of data processing. These rights which data controllers and processor are obliged to enable the subjects in exercising include:

1. the right to information (Arts. 13, 14);
2. the right of access (Art. 15);
3. the right of rectification (Art. 5 (1)(d), 16);
4. the right to erasure (Art. 17);
5. the right to restrict processing (Art. 18);
6. the right of data portability (Art. 20);
7. the right to object to certain processing (Art 21); and
8. the rights in relation to automated decision making and profiling (Art 22).

However, the various rights are prima facie, not absolute in character, i.e. subject to potential derogations/exemptions in various situations. That is to say, the rights may be denied, or limited, if there are compelling countervailing reasons for doing so. Under the GDPR, one situation, where this may occur is where the unrestricted exercise of a given right may interfere with scientific research activity, e.g. by overly burdening researchers or putting the accuracy of the results at risk. Here the possibility to exemptions in the respective national law is provided for in Article 89(2) of the GDPR. The exemptions may be relevant for SPEAR during the research phase of the project. It will also be pertinent to the later consideration of the requirements for managing the SPEAR platform after the conclusion of the Project.

4.2.3.5 Data breach notification

A further obligation of the data controller is to notify the supervisory authority without undue delay and, where feasible, not later than 72 hours, after having become aware of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (art. 33). A reason shall be furnished where the notification is not made within 72 hours. Article 33 (3) enumerates what shall be included in the notification such as the nature of the data breach, the number of data subjects concerned, the likely consequence of the breach, etc.

Furthermore, where the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall notify the data subject in a plain language, about the nature of the breach without undue delay according to Article 34. However, notification to the data subject may not be required where the data controller has implemented appropriate technical and organisational protection measures on the affected data, in particular, those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption, or measures had been taken to make the high risk not materialize, or notifying the data subject would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The implication of this obligation will be significant once the SPEAR platform is deployed in practice. At this point, it should support the capability of notifying the competent supervisory authorities, data controller, and (in appropriate cases) data subjects should a breach occur.

4.2.3.6 Obligation to keep a record of processing activities

The GDPR also requires a data controller to maintain a record of processing activities under its responsibility. Article 30 contains a list of what shall be included in the record including: the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; etc. This record shall be in writing, including in electronic form, and shall be made available to the supervisory authority on request.

It is notable that this obligation does not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Given that the SPEAR platform could potentially process personal data later used to prosecute criminal activity, this may clearly impact on the rights and freedoms of the data subjects. Accordingly, the platform should support keeping records of these processing activities.

4.2.3.7 Data transfers to non-EU states

To ensure that personal data obtained within the EU enjoy the same level of protection when it leaves the jurisdiction of the EU, Article 45 of the GDPR provides that any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall be subject to certain legal basis and safeguards. These legal grounds include:

- transfers on the basis of a European Commission (EC) adequacy decision (art. 45);
- transfers subject to appropriate safeguards such as binding corporate rules, standard contractual agreements, use of approved code of conduct or certification, etc. (art. 46).

However, there are specific situations in which these requirements may be derogated from, specifically on the grounds listed in Article 49 such as where the data subject explicitly agrees to the transfer, or the performance of a contract, etc.

This obligation has implications for SPEAR in terms of using cloud computing, where the servers for processing personal data are located outside the EU/EEA and the access or processing of EU subjects data by partners who are non-EU and do not have adequacy finding by the EC. In this regard, SPEAR’s use of cloud has to be subject to this consideration in terms of restricting the location of the servers within the EU/EEA.

For access by project partners who are established outside the EU (such as PIMEE which is based in Ukraine), if it is determined that the partner will process personal data, then additional safeguard such as EC standard contractual agreement with the data controller(s) transferring the specific data has to be concluded before any data transfer or access to the SPEAR database with personal data. A further potential issue that may affect data processing in the development phase is the likely exit of the United Kingdom from the EU (Brexit). This may affect the data processing of the University of Surrey, UK, but as the final outcome of this exit is not clear now, this will be kept under review during the lifespan of the project.

4.3 Users of the SPEAR System and their Status Regarding Data Processing

In order to determine the nature of the obligations of the different entities involved in SPEAR in relation to the data protection duties, it is important to consider their status under the GDPR. As considered further below, the GDPR distinguishes different roles of parties depending on how much control they have in respect to the processing. These entities include:

I. Data Controller

An entity which alone or jointly with others determines the purpose and means of data processing (art. 4 (7). To assume this role, the factual element of the circumstances surrounding the data processing has to be taken into account, such as how far the entity determines the purpose of data collection, the technical and organisational means of data collection, etc. [37]. Where two or more entities are regarded as joint controllers, they must determine their respective responsibilities for compliance with the obligations under the regulation in an agreement. The main responsibilities under the GDPR rest with the data controllers, and they are accountable to both the data subjects and the supervisory authorities on how they process data.

II. Data Processor

Distinguished in the GDPR from the data controller is the data processor, which is an entity that processes data on behalf of the data controller (art. 4(8). The processor processes data solely according to the instructions of the data controller, as opposed to itself determining the purposes or means of such processing. However, under the GDPR, processors also have responsibilities such as implementing appropriate technical and organizational measures to protect the data, data breach notification to the controller, etc.

III. Data Subjects

The data subject is the individual whose personal data is processed by the data controller or processor. Legal personalities that are not natural persons such as a company is not considered as data subjects under the GDPR.

Following the above terminological clarification, the status of the SPEAR system, as well as the users of the system, will next be analysed. In the context of the ecosystem of the smart grid, typical actors could include Generators, Transmission System Operators (TSO), Distribution System Operators (DSOs), and consumers. It will be important to keep these actors under review, with respect to SPEAR as the project develops because how the SPEAR tools are deployed, in fact, will determine the status of the user regarding data protection compliance.

4.3.1.1 SPEAR System and the Consortium

It is important to note that although SPEAR consortium is made up of 16 research partners, it is not a legal person and therefore cannot as a whole be subject to obligations under the GDPR. Therefore, in the course of developing the SPEAR tools, each of these partners ideally determines the purpose and means of processing personal data that such partner requires to fulfil its task. As such, each partner would be regarded as a data controller in respect of the specific data it processes [38]. If the purpose and means of the data processing are determined in conjunction with other partners, those partners will assume the role of joint controllers.

In the second phase of the project when the SPEAR platform is fully developed and ready to be used in real-life scenarios to collect and process entirely new datasets, then the legal entity that operates the SPEAR platform (e.g, as service provider), as well as determines the purpose and means of data processing will assume the role of data controller (or joint controller, if done together with another). At this stage, a number of constellations regarding the status of this future entity may be possible. One scenario could be where the SPEAR platform provides a service and an energy operator acquires this service and integrates SPEAR tools into its system and determines the purpose and means (possibly jointly with the entity that administers the SPEAR service). There could also be another scenario where the SPEAR service provider represents only a data processor. Given that the configuration of this post-project phase is not entirely clear at this stage, an assessment will be made at the relevant stage of the project (e.g, towards the end of the project when the platform has been further developed).

4.3.1.2 Users as Energy Operators

Several entities involved in the smart grid chain as providers of energy services or operators could be potential users of the SPEAR platform. As explained above, the entity that acquires and installs the SPEAR tools or integrates it into its system, could either be a data controller or a joint controller, where such entity determines the means and purpose of data processing obtained with SPEAR tools or joint controller if done jointly with others.

For example, if on the one hand, the developed SPEAR platform has both open source tools that could be deployed as standalone tools, the energy operator that downloads and deploys these tools and uses them to process personal data will be regarded as the data controller. If on the other hand, a SPEAR service provider jointly determines the purpose and means of the data processing, then, both entities would be regarded as joint data controllers. Another possible scenario could be where an energy operator assumes controllership of the deployed SPEAR system and permits the SPEAR service provider to only process data on its behalf (as a data processor). The specific status will need to be assessed when concrete scenarios emerge in the future.

4.3.1.3 Users as Consumers

The consumers here refer to the individuals who use the smart grid electricity service (as end-user) and whose data will be processed using the SPEAR platform, for example, the smart home occupant. They are the data subjects and the object of protection under the GDPR.

However, apart from these energy consumers, other data subjects could be envisaged: for example, the security administrators who monitor the relevant system security using SPEAR (eg, credentials/authentication data), the third parties who interact with systems that SPEAR is monitoring (e.g., attackers, non-attackers). This distinction is important because different legal bases may be used for processing the various data of these subjects.

4.4 National frameworks for data protection

The GDPR, as a 'Regulation', is a directly applicable EU instrument, which is intended to apply directly and with consistent effect in all Member States. In this respect it contrasts with the 1995 Directive (which it replaced), which had required transposition in diverse national law at Member State level in order to be legally applicable, leading to inconsistent rules in some situations. Nonetheless, in practice the GDPR also leaves room for variation between Member States in some aspects of data protection law [40]. Indeed, there remain more than fifty areas where Member States are permitted to legislate in different ways (so-called 'opening clauses'); one area this is true for is in relation to the use of data for scientific research, where Member States are allowed, among other matters, to provide for exemptions from the rights otherwise accorded to data subjects, if they deem this necessary in the interests of the research (see also Section 5.2.3.4).

In order to implement the GDPR, and enact their individual rules where allowed for, the Member States have passed, or are in the process of passing new national data protection laws (updating their old laws that gave effect to the 1995 Directive). As noted, in some cases, rules – diverging from the general EU position – may be contained in such national law, which impact upon the processing of personal data for scientific research. In the context of the SPEAR Project, the Project partners responsible for the use cases, and which may have occasion to process such data in executing these, are located in Bulgaria, France, Greece, and Spain. In this regard, it will be important for those partners to take account of any special rules here that are implemented by their respective Member States: this is a matter on which advice from the relevant national supervisory authority should be sought as appropriate, as the GDPR implementation situation evolves.

As at January 2019, of the mentioned Member States, France has enacted relevant implementing law, in the form of a new French Data Protection Act (Law 2018-493 of 20 June 2018) ('FDPA') [41], which aims to fill out some of the rules where the GDPR has left discretion to Member States, while also providing that further such rules may be enacted in the future by Presidential decree. The FDPA permits data controllers to retain data after their initial processing, if this is required for archiving purposes in the public interest. It also contains safeguards in relation to automated processing that may result in a decision disadvantageous to an individual data subject. As regards data processing for scientific research, there is – subject again to suitable safeguards to protect the fundamental interests of data subjects - provision for exemptions from some of the rights of subject rights set out in Chapter III of the GDPR (see section 5.2.3.4); in particular, under Article 39 II of the FDPA, the rights of access, rectification, objection, restriction of processing, erasure and data portability where data is needed for research, provided mechanisms, such as secure de-identification of the data, are adopted to guarantee the data subject's interests by other means.

Recently, on 7 December 2019, Spain also passed the Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights to implement the GDPR in Spain, however, an English translation is not yet available. As regards Bulgaria and Greece, draft laws are presently passing through their respective legislative assemblies: in Bulgaria on 30.04.2018 a draft law amending and supplementing the Personal Data Protection Act was introduced on 30 April 2018 for public discussion [42]; in Greece, a Bill with a similar purpose was published on 20 February 2018 and submitted to public consultation [43]. However, as of January 2019, neither of these laws has been enacted.

In summary, the position as to any special rules at national level that impact upon data use in scientific research is not yet fully determined. As stated, even in France, while some such rules have been determined (in the FDPA of 20 June 2018), others may be added by Presidential Decree. This underlines the importance for the Project, and for the relevant partners, of keeping the situation under review, including by appropriate liaising with their national supervisory authorities. In Bulgaria, the responsible body is the Commission for Data Protection [44]; in France it is CNIL [45]; in Greece, the Hellenic Data Protection Authority [46]; and in Spain, the AEPD [47]. These contacts are also important given that, by the nature of things, it will be some time until national courts have interpreted and applied the often-complex provisions in particular cases. Until such time, the recommendations of the supervisory authorities will provide the best guidance on legally compliant processing practice in each Member State.

4.5 Data and Component Mapping for Privacy Protection

From the previous discussions, as well as analysis of D2.2, and the questionnaire completed by project partners detailing the nature of their data processing, the table below lists the personal data that have been identified in the project for privacy protection.

Table 25: A mapping of personal data identified in SPEAR

SN	Potential Personal Datasets	Components	Remarks
1	Network traffic data (eg., IP address)	SIEM, BDAC, Visual-based IDS, SPEAR FRF, any other component	Where data could be used to identify energy consumers including smart home occupants, or any other human subject including the attacker
2	Credential/Authentication data	SIEM, any other component	Where it is related to the system/security administrators
3	Data of the Smart Home occupant, including their devices	SIEM, SPEAR FRF, any other component	Applicable to the smart home use case
4	Other personally identifying data	SIEM, Security Server, SPEAR FRF, any other component	Where the log data from devices/systems, smart meter data, etc., could be linked to human owners, then they are regarded as personal data.

4.6 Privacy Requirements Specification list

Table 26 compiles the privacy requirements identified from the analysis in Chapter 4.

Table 26: Privacy requirements specification list

Req. id	Req. Title	Req. Description	Priority High I Medium I Low
PR-01	**Legal basis for data processing**	The SPEAR platform shall have a clear legal basis for processing personal data (stated in the privacy policy)	High
PR-02	**Data minimisation**	The SPEAR platform shall collect only a minimum personal data relevant for its purposes	High
PR-03	**Enablement of data subjects' rights**	The SPEAR platform shall support and	High

		enable a rights management capability for data subjects	
PR-04	**Data accuracy**	Personal data processed in the system shall be accurate	High
PR-05	**Storage limitation**	• Personal data stored in the SPEAR platform shall be retained only for a period necessary to fulfil its purpose (end of the project); • Personal data that is no longer needed must be properly disposed	High
PR-06	**DPIA compliance**	The platform shall incorporate a data protection impact assessment (DPIA) to ensure that appropriate protections are in place (See WP4)	High
PR-07	**Record of data processing**	The SPEAR platform shall support keeping a record of personal data processing within the platform	High
PR-08	**Transparency**	The SPEAR platform shall provide necessary information relating to data processing to the data subjects (to be included in the privacy policy)	High
PR-09	**Purpose limitation**	The SPEAR platform shall only process data for the specific purposes it was collected	High
PR-10	**Traceability of incidents**	The SPEAR platform shall support the logging of data to trace privacy and security incidents	High
PR-11	**Integrity, availability and confidentiality**	• The SPEAR platform shall use state of the art measures	High

		maintain the integrity, availability and confidentiality of personal data; • The system network communications must be protected from unauthorized information gathering and eavesdropping; • The system shall provide a data backup mechanism	
PR-12	**Strong authentication measures**	The system shall have strong authentication measures in place at all system gateways and entrance points	High
PR-13	**Secure location of data**	The SPEAR system shall use cloud systems subject to EU law	High

4.7 Key Ethical Considerations and Safeguards

Over the years, certain fundamental principles of ethics—human dignity, autonomy, necessity and proportionality and common good—have developed to tackle issues of ethical relevance, in particular, with respect to protecting the interests and concerns of human subjects. The GDPR emphasizes that the processing of personal data should be designed to serve mankind, which brings to the fore the ethical aspect of data processing. Advanced data processing mechanisms such as artificial intelligence, and the intended or unintended consequences of such processes have shown the need for ethical data and information management system [48]. For the SPEAR project, the following ethical issues have been considered.

4.7.1 The use of Honeypots and ethical issues

An important aspect of the SPEAR Project concerns the envisaged development and use of ‘honeypots’, as shown the Use Cases. In the computer security industry, honeypots are defined as a computer system implemented as a decoy network, which seeks to entice would-be attackers into exploiting the system with the various tools within their hacking toolkit. In doing so, the aim is not only to distract attention away from the real system as a target, but for the attackers’ interaction with the decoy to be monitored and recorded, and the results used to research and improve rules on Intrusion Detection Systems. Secondly, network traffic data captured from an attacker, such as the IP address of the device used in the attack, could later form the basis for a criminal investigation (this criminal investigation part is outside the scope of SPEAR). As identified by commentators [49], the use generally of ‘honeypots’ may raise three main sets of legal/ethical issues, namely in relation to:

(i) Surveillance and privacy aspects

(ii) Entrapment aspects
(iii) Liability for onward damage

Looking, first at the surveillance point, in SPEAR it is apparent that, when it monitors the behaviour of attackers within the honeypots, the Project is engaging in observational research for which it does not have the consent of the research subjects, i.e., the attackers. This is in contrast to the other key scenario where the Project may capture personal data of subjects, namely in relation to the (CERTH employee) occupants of the Smart Home in Use Case 4, where full informed consent will be obtained [39]. The difficulty with seeking consent in relation to the honeypots is indeed clear, namely that this would negate the object of the research: the intention is to observe attack strategies that the attackers would not reveal (or indeed they would not access the honeypot in the first place) if they were aware it was a honeypot.

Even so, it should be recognized that conducting research in this non-consensual, covert form is an exception to standard research practice, and that the onus of ethical justification is clearly upon the researcher. In this regard, the International Sociological Association's (ISA) *Code of Ethics*, for example, states that: "*The consent of research subjects and informants should be obtained in advance. Covert research should be avoided in principle, unless it is the only method by which information can be gathered* [50]. It is apparent that here the ethical position is stricter than the legal position under the GDPR, where we saw that other bases to justify data processing, such as the legitimate interests of the controller, may be invoked as equal alternatives to subject consent. At the same time, the ethical codes like the ISA one just cited admit the possibility of non-consensual research if this is the only way of obtaining the required research information.

As noted above, in relation to SPEAR, the argument is precisely that seeking research subject (attacker) consent to observe their actions would defeat the research purpose. Nevertheless, at this point, two further essential principles of research ethics need to be considered [51]. First, the research must be of sufficient inherent value to outweigh the downgrading of the subject's autonomy interest that is implicit in not seeking their consent. (Another way of expressing this is to say that, if a given piece of research is of a trivial nature, then – if it cannot be conducted on the basis of subject consent, it should better not be conducted at all.) On this aspect, though, it is apparent that the SPEAR research, seeking solutions to a serious threat – cyberattacks – to critical energy infrastructures, is clearly of sufficient value.

Secondly, however, performing the research must not expose the subject to an unreasonable risk of harm – here, given the lack of subject consent, it is generally agreed that 'unreasonable' means 'more than minimal' (by contrast, where consent is obtained, subjects may choose (as an aspect of their autonomy) to accept a somewhat higher risk of harm). In the context of SPEAR, this underscores the importance of having safeguards in place to protect the privacy of the research subjects such as encryption, anonymization, etc., where necessary.

In terms of the network traffic data, it is evident that it may be useful for the research purpose to be able to trace that the same attacker-machine was used at different time-points in different attacks; thus it might possibly be justified to store the data for a limited period (till the end of the SPEAR project) to analyse how the attack strategy varies in subsequent attacks. Moreover, to ensure risks to the research subject do not rise above minimal, there should be a short longstop - a short upper time-limit on the period for which the data should be kept for research analysis, prior to being anonymised or deleted. Secure protection mechanisms such as encryption, pseudonymisation or anonymization should be applied where appropriate to the network traffic data in question [52]. As discussed further below (under 'entrapment'), failure to take this measure could potentially expose the research subjects to significant risks.

As is implicit from the above the particular status of the research subjects as honeypot attackers (and thus putative cybercriminals) has no real ethical bearing on the above analysis. It is true that an argument might be made that the attacker has a lower expectation of privacy if he enters an area that is evidently off-limits: thus he may expect counter-measures to detect his presence. However, whether or not this may apply to real-life honeypot deployment, the argument has no weight in the research scenario of SPEAR. Leaving aside the point that a variety of different individuals may be caught in the honeypot, from novice hackers out for 'a bit of fun' to hardened black-hats and/or state-sponsored agents, the researcher has no justification for entering into this form of enquiry. The interests of the research subject should always be the researcher's paramount concern.

Looking, next, at the issue of entrapment, the latter was defined (in a leading US decision) as "…the conception and planning of an offense by a [state official], and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion, or fraud of the [official]" [53]. In the context of honeypots, this is arguably germane in that the attacker is in a sense lured into accessing the network due to it been made to appear of potential interest while incorporating deliberate design vulnerabilities [54]. Though it might be asserted in response that, if the honeypot had not existed, the attacker would have found another target, this cannot simply be assumed; moreover, in the case of some attackers, the only reason they succeed in accessing a closed-system (in this case the honeypot) will be due to the intentional vulnerabilities implanted by the designer. Here any criminal activity they engage in within such a closed-system would not otherwise occur.

An alternative argument that the use of honeypots does not involve entrapment points to the state-sponsored nature of the activity (as highlighted in the US authority cited above) [49]. However, while it is true that (as in the case of SPEAR) honeypots are frequently deployed by private actors, rather than the state, where used to gather forensic evidence to assist in the subsequent criminal prosecution of attackers, they closely ally themselves to the state function of law enforcement. Moreover, in the context of SPEAR, where the Use Case honeypot deployments are primarily for the purpose of research, it is suggested that disclosing attackers' data to the authorities would contravene the important duty not to harm the research subject. In SPEAR there is no suggestion that this would happen willingly: as discussed, the intention is for any identifying information associated with the attacker, such as network traffic data to be protected once it can serve the research purpose and deleted at the end of the project. At the same time, a problem may occur if a partner that captures such data is requested by a national or international law enforcement agency to divulge this.

Finally, thought should be given to a mechanism some commentators have put forward as a way of lessening entrapment concerns in relation to honeypots, namely the use of pop-up banners to warn those who access the system that their activities may be monitored [49]. Indeed, an advantage of this may be to deter novice hackers, and thus reduce resources needed for monitoring their – for the research - uninteresting activity. Even so, it would damage the research if the presence of the banner at the same time led experienced intruders to suspect they had accessed a honeypot: thus the banners used should plausibly mimic those found on real networks.

The third of the key issues noted earlier, liability, may be relevant in the event that an attacker, who gained access to a honeypot, were to use the honeypot system as a springboard for launching a 'downstream' attack on another party network. In such a case, there might even be the prospect of legal liability for negligence, if the vulnerabilities and other features of the honeypot made it readily foreseeable that it could be so used. However that may be, in terms of adhering to research ethical norms it is evident that the honeypots in SPEAR must be configured to as far as possible eliminate the risk that they could be misused in this way, in particular by properly securing its egress points to the internet [54] or by performing the tests in a lab environment.

Deployment of honeypots outside the research environment, that is, in a real-life situation is even more complex with respect to legal issues such as the establishing identity of the attacker, privacy and data protection, evidence management, etc. The legal aspects of network forensics relating to honeypots outside the lab will be addressed further in D4.1: Forensic Law and Regulations.

4.7.2 Ethical requirements specification list

Table 27 compiles the ethical requirements identified from the analysis in Section 4.7.

Table 27: Ethical requirements specification list

Req. id	**Req. Title**	**Req. Description**	**Priority** **High I medium I Low}**
ER-01	Research ethics adherence	The SPEAR platform shall adhere to accepted research ethical standards	High
ER-02	Safeguard research subject interests, including of cyber-attackers	The SPEAR platform shall treat honeypot attackers as research subjects, and take appropriate steps to safeguard them from harm or inconvenience, including measures to protect their data	High
ER-03	Assess constraints for use of honey pot in real-life	Real-life constraints to the use of honeypots shall be identified (Ref. WP 4)	High

5. Security Requirements Definition

The security requirements for the SPEAR system describe functional and non-functional requirements that need to be satisfied, in order to achieve the security attributes of the system required by end-users and legal regulations. Best practices and standards as identified by experts in the project, have also contributed in the elicitation of SPEAR security requirement.

5.1 End-user security requirements

Analysis of the end-user requirements responses indicates that the security of their systems is a key business critical factor in their operation. As such, they seek to secure not only their informational assets but also their equipment and staff safety. As noted in Section 4.1, end users seek protection from DDoS, DoS, unauthorised access, remote manipulation of the control system, etc. They also seek availability by different means, as well as compliance with relevant security standards. These needs translate the user requirements, taken into account, in the elicitation of the security requirements.

5.2 The regulatory framework of network and information security of critical infrastructure in the EU

The NIS Directive (EU) 2016/1148 lays down measures to achieve a high common level of NIS among operators providing essential services (OES) and digital service providers (DSP) in the EU. Under the Directive, EU Members States are obliged to ensure their implementation. OES are companies providing essential services in the energy, transport, banking, financial markets, health, drinking water and digital infrastructure sectors [5], [55]. OES in the energy sector and the electricity subsector have key obligations to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations (NISD, art 14). Those measures shall ensure a level of security of network and information systems appropriate to the risk posed, having regard to the state of the art. While it has been pointed at that the proposed SPEAR platform does not qualify as OES, it is important to note that to facilitate their adoption by end-users who are obligated to comply with the Directive, the requirements in the Directive need to be supported by SPEAR where possible. This implies that apart from the specific security requirements of the users identified in the survey, the SPEAR system security should reflect and support these regulatory requirements where necessary.

Recently, the NIS Cooperation Group published a “Reference document on security measures for Operators of Essential Services” [58]. This document concretises key measures that OES should implement to enhance their network and information security. For example, with respect to information system security governance and risk management, the document recommends regular risk assessment of the system as part of the Information System Security Risk Analysis, as well as to develop a procedure for information system security audit, among others. Regarding IT Security Architecture, the following are recommended:

1. **Systems Configuration:** Install only services and functionalities or connect equipment which is essential for the functioning and security of the information system.
2. **System Segregation:** Segregate the system in order to limit the propagation of IT security incident within the system or subsystem.
3. **Traffic Filtering:** Filter traffic flows circulating in the system and forbid traffic that is not needed for the system and that are likely to facilitate attacks
4. **Cryptography:** Establish and implement a policy and procedure related to cryptography.

Several other recommendations in the Reference document relate to:

- **IT Security Administration**: Administration Accounts and Administration Information Systems;
- **Identity and Access Management:** Authentication and Identification and Access Rights;

- **IT Security Maintenance:** IT Security Maintenance Procedure and Industrial Control Systems;
- **Physical And Environmental Security**;
- **Detection:** Detection, Logging, Logs Correlation and Analysis;
- **Computer Security Incident Management**: Information System Security Incident Response, Incident Report and Communication with Competent Authorities and CSIRTs;
- **Continuity of Operations**: Business Continuity Management and Disaster Recovery Management;
- **Crisis Management:** Crisis Management Organization and Crisis Management Process.

While this point has been emphasized that SPEAR needs to reflect these recommendations as part of the data security design of the system where appropriate, it is also important to note that the GDPR expatiates on data security requirements, indicating examples of what technical and organisational measures that may be applied.

- **Technical measures** include: pseudonymisation and encryption of personal data where appropriate; data minimisation, regular testing of the systems, ensuring confidentiality, integrity, availability and resilience of processing systems and services through back-ups, authentication, etc.; implementing data protection by design and by default, regular update of the systems where necessary, logical access control, etc.
- **Organisational measures** include appropriate data protection and security policies, conducting a risk assessment, transparency in presenting information about the data processing, enabling data subjects to enforce their rights, physical access control, staff training, ensuring that only data processors with appropriate technical and organisational measures are used, etc. [56], [57].

Furthermore, adherence to approved codes of conduct and certification mechanisms could be used to demonstrate compliance with the GDPR obligations. Examples of standards and certifications relevant to security of information systems include the ISO/IEC 27000 family of standards on information security management systems, ISO/IEC 15408, ETSI TS 102 165-1, ETSI TR 103 305, NIST, etc. [59]. Supporting these standards where appropriate will add value to the SPEAR platform and the end-users.

5.3 Security expert analysis

A key aspect of information security is to preserve the confidentiality, integrity and availability of an organisation's information. It is only with this information that it can engage in commercial activities. Loss of one or more of these attributes can threaten the continued existence of even the largest corporate entities:

- **Confidentiality**. Assurance that information is shared only among authorised persons or organisations.
- **Integrity**. Assurance that the information is authentic and complete.
- **Availability**. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

It is generally accepted to divide the interests of entities related to the information system into the following categories: availability, integrity, confidentiality of information resources and supporting infrastructure. All of these aspects are essential elements of an ICT used in the energy sector.

The damage caused by the failure to comply with the availability requirement is particularly evident in all sorts of management systems: generation, production, transportation, distribution. Compliance with the integrity requirement is of particular value if the information is a “guide to action,” for example, for the technological process. Confidentiality is the most developed aspect of information security. However, cryptographic methods of protection as a way to ensure confidentiality is limited at the national legislative levels.

Information security threats can also be classified according to abovementioned criteria:

- **Threats of confidentiality (illegal access to information)**

The threat of breach of confidentiality is that information becomes known to someone who does not have access to it. It occurs when access to information stored in a system or transmitted from one system to another. Such threats may arise as a result of the human factor, failures of software and hardware.

- **Threats to integrity (illegal data change).**

Threats of integrity violation are threats associated with the likelihood of modification of particular information stored in the information system. Violation of integrity can be caused by various factors - from intentional personnel actions to equipment failure.

- **Threat to availability**

The implementation of actions that make it impossible or difficult access to the resources of the information system.

In sum, there is no one-size-fits-all solution for data security. A popular view is to adopt a risk-based approach continuously reviewing the risks. Therefore, it is important for the design of the relevant parts of the SPEAR systems to embed these security requirements for compliance with relevant regulations, as well as satisfy the user needs.

5.4 Security requirement specification list

Table 28 compiles the security requirements identified from the analysis in all the Chapters.

Table 28: Security requirements specification list

Req. id	Req. Title	Req. Description	Priority High I medium I Low}
SR-01	**Maintain a high level of Confidentiality, Integrity and Availability of the system**	• The system shall use a security protocol to protect user data over the Internet; • Ensure secure authentication control to the SPEAR tool; • Ensure regular backups and that the restoration procedures work as expected	High
SR-02	**Database security**	All databases where personal data are stored in the SPEAR platform must be encrypted, access to them must be	High

		restricted and authentication required to access such data	
SR-03	**Systems Configuration**	The SPEAR system shall install only services and functionalities or connect equipment which is essential for the functioning and security of the system	High
SR-04	**Support compliance with regulations and standards in the smart grid sector**	The SPEAR system shall support compliance with relevant standards and laws on IT security where applicable	High
SR-05	**Continuous System Management**	The system shall apply security updates continuously	High
SR-06	**Interconnectivity security**	The SPEAR system shall ensure that the interaction between the different SPEAR components as well as between the SPEAR platform and other external systems shall be secure	High
SR-07	**Security of the honeypots**	The honeypot shall not compromise the security of the host network or machine.	High
SR-08	**Logging**	The SPEAR platform shall establish relevant logging system	High

6. Conclusion

This Deliverable has examined the user, security and privacy requirements pertaining to the SPEAR project, with reference to its objective of providing tools to promote detection, response and countermeasures against advanced cyber threats and attacks on smart energy grids. As discussed in Chapter 2, the tasks, described in this report, were undertaken using a number of methodologies, including desktop research, questionnaires and consultations with relevant project partners were utilised. Moreover, several different types of requirements were subsequently identified, which will inform the ongoing development of the tools and the manner in which they are configured and used in the SPEAR platform. Initially, Chapter 3 focused on the user needs as identified and recorded by questionnaires and face-to-face interaction with the use case project partners. A detailed analysis of the four use case scenarios is given , namely the hydro power plant, substation, combined (IAN and HAN), and smart-home, in order to present the key requirements that are deemed essential to making SPEAR an effective, responsive and functional system. To assist the tool-developer partners to better appreciate the practical contexts in which the different users would have recourse to the SPEAR tools, the user partners contributed narratives of the key cyber-security challenges each faces in practice and how they envisage deploying the tools for addressing the same.

Other categories of requirements applicable to the SPEAR project, in particular those relating to privacy and security, arise not only from the user needs but also from regulatory compliance. In particular, the project will involve the use of personal data, partly already in relation to the development of the tools (e.g. network traffic data, potentially including IP addresses, that are captured by the SPEAR honeypots), but especially once the SPEAR platform is ready for exploitation. In this respect, it is essential that the platform is architected to operate in full compliance with EU data protection norms, in particular as set out in the GDPR. The requirements on data controllers stemming from the GDPR were thus presented in Chapter 4, and their implications for the key actors in SPEAR assessed. Similarly, requirements of an ethical nature, especially those concerning the deployment of honeypots as a cyber-attack research method were investigated in the same Chapter. Lastly, Chapter 5 presented and discussed the major security requirements on the SPEAR infrastructure, both as an aspect of data protection law (and covered similarly by provisions of the GDPR) and under the EU Network Information Security Directive, which aims to achieve high level of information security among critical infrastructures.

A template for the SPEAR partners to use as a consistent point of reference, where the various requirements have been summarised and presented in tabular form, is provided at the end of the relevant section that analysed their source, and thereafter further collated in Annex II to this Deliverable. Along with the Work Package 2 deliverable D2.2 (system specification and architecture), this deliverable thereby serves to lay down parameters that will guide the partners in performing their future tasks in the project.

References

[1] P. Vingerhoet, M. Chebbo, and N Hatziargyriou, “The digital energy system 4.0,” Smartgrids project 2016. [Online]. Available: https://www.etip-snet.eu/wp-content/uploads/2017/04/ETP-SG-Digital-Energy-System-4.0-2016.pdf. [Accessed Jan. 13, 2019].

[2] Directorate General for Internal Policies, “Cyber Security Strategy for the Energy Sector”, October 2016. Available: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf. [Accessed Jan. 13, 2019].

[3] P. Paganini “Smart meters in Spain can be hacked to hit the National power network” Security Affairs, October 17, 2014. Available: http://securityaffairs.co/wordpress/29353/security/smart-meters-hacking. [Accessed Jan. 13, 2019].

[4] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[7] Smart Grid Task Force 2012-14, “Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems,” v. 2 of 13 September 2018. Available: https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf. [Accessed Jan. 10, 2019].

[8] E. Stav, S. Walderhaug, and U. Johansen, ARCADE - An Open Architectural Description Framework. December 2013, SINTEF ICT. Available at: http://www.arcade-framework.org/wp-content/uploads/2013/12/ARCADE-Handbook.pdf. [Accessed Jan. 10, 2019].

[9] C. Vallance, “Ukraine cyber-attacks 'could happen to UK',” *BBC News*, February 29, 2016. Available: https://www.bbc.com/news/technology-35686493. [Accessed Jan. 10, 2019].

[10] European Program for Critical Infrastructure Protection (EPCIP) "Protection of critical infrastructure." Available:https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure. [Accessed Jan. 17, 2019].

[11] The Charter of Fundamental Rights of the EU 2000, arts 7 and 8; t

[12] The European Convention on Human Rights 1950, art 8.

[13] FRA, *Handbook on European data protection law.* Luxembourg: Publication office of the EU, 2018.

[14] For example, the Network and Information Security Directive, art 15(4), provides that competent authority established under the directive shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.

[15] GDPR, art 25.

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) Available: https://rm.coe.int/1680078b37. [Accessed Jan. 13, 2019].

[17] ECtHR, "Guide on Article 8 of the European Convention on Human Rights," August 2018.

[18] The modernised Convention 108. Available: https://www.coe.int/en/web/data-protection/convention108/modernised. [Accessed Jan. 13, 2019].

[19] Article 29 Working Party Opinion 4/2007 on the concept of personal data [Adopted on 20th June 2007].

[20] *Patrick Breyer v Bundesrepublik Deutschland* (Case C-582/14).

[21] *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Case C-70/10).

[22] The origin of these principles could be traced to the US Department of Health Education and Welfare's 1973 Fair Information Practice Principles (HEW 1973).

[23] Article 29 Working Party Guidelines on transparency under Regulation 2016/679 [Adopted on 11 April 2018].

[24] A. Cavoukian, "Privacy by Design… Take the Challenge," 2009. Available: https://web.archive.org/web/20120119044635/http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf. [Accessed 13 Jan 13 2019].

[25] L. Bygrave, "Hardwiring Privacy" University of Oslo Faculty of Law Research Paper No. 2017-02.

[26] Ann Cavoukian 'Privacy by Design: The 7 Foundational Principles' (2009, revised 2011)

[27] Ann Cavoukian, Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices (Ontario 2012).

[28] ENISA, Privacy and Data Protection by Design – from policy to engineering (2014).

[29] ENISA, Privacy and Data Protection in Mobile Applications (2017);

[30] German DPA's Standard Data Protection Model, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf.

[31] ENISA, Handbook on Security of Personal Data (2018)

[32] EDPS, Opinion 5/2018 Preliminary Opinion on privacy by design [Adopted 31 May 2018] 6-7.

[33] ICS, 'What is Privacy by Design & Default? <https://www.ics.ie/news/what-is-privacy-by-design-a-default> accessed 13 January 2019.

[34] Lee Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements', Oslo Law Review, Vol. 4 No.2, 2017

[35] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) [Adopted 4 October 2017].

[36] CNIL PIA methodology <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf> accessed 13 January 2019.

[37] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" [Adopted on 16 February 2010].

[39] See also SPEAR D9.1 H-Requirement No.2.

[40] The reason for this, which admittedly renders the legal position between EU member states barely more consistent than under the Directive, is that the EU enjoys limited legislative competence in some of the areas, as well as political compromises required during the GDPR enactment process

[41] An English translation of the FDPA is available on the French data protection authority (CNIL) website, at: <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf> accessed 15 January 2019.

[42] DLA Piper, Data Protection Laws of the World - “Bulgaria”. Available: https://www.dlapiperdataprotection.com/index.html?t=law&c=BG> [Accessed Jan. 15, 2019].

[43] DLA Piper, Data Protection Laws of the World - “Greece” Available: https://www.dlapiperdataprotection.com/index.html?t=law&c=GR [Accessed Jan. 15, 2019].

[44] See: https://www.cpdp.bg/en/ [Accessed Jan. 15, 2019].

[45] See: https://www.cnil.fr/en/home [Accessed Jan. 15 2019].

[46] See: http://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL> accessed 15 January 2019.

[47] See: https://www.aepd.es/> accessed 15 January 2019 (Spanish language version only).

[48] Katherine O`Keefe and Daragh Brien, *Ethical data and information management,* (Kogan Page, 2018).

[49] R. Campbell, “The Legal and Ethical Issues of Deploying Honeypots” (University of South Africa, 2014).

[50] International Sociological Association, *Code of Ethics* (Madrid: International Sociological Association, 2001), available at: [http://www.isa-sociology.org/about/isa_code_of_ethics.htm].

[51] *European Textbook on Ethics in Research* (PEAK, Keele University, commissioned by the EC), available at: [https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf], especially case studies 2.3 and 4.1

[52] See e.g. the White Paper on Pseudonymisation drafted by the Data Protection Focus Group (2017)

[53] *Sorrells v. United States* (1932), per Roberts J.

[54] Spitzner, L. (2002). *Honeypots: Tracking Hackers.* Reading: Addison Wesley.

[55] Tanguy Van Overstraeten et al, ‘EU – The implementation of the “Cyber Security” Directive’, Linklater 27 September 2018.

[56] UK’s Information Commissioner’s Office Guide to the GDPR, “Security” <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/>;

[57] UK’s Information Commissioner’s Office Guide to the GDPR, “Encryption” <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/> accessed 13 January 2019.

[58] <https://circabc.europa.eu/sd/a/c5748d89-82a9-4a40-bd51-44292329ed99/reference_document_security_measures_OES.pdf> accessed 13 January 2019.

[59] ENISA, “Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy (version 1.0 November 2016)”. Available: https://www.enisa.europa.eu/publications/gaps-eu-standardisation [Accessed Jan. 13 2019].

[60] UK Information Commissioner’s Office, “Protecting Personal Data in Online Services: Learning from the mistakes of others”, May 2014.

[61] One of the respondents to the SPEAR user requirements’ questionnaire.

[62] J. Brackett, “Software Requirements” SEI Curriculum Module SEI-CM-19-1.2, January 1990.

[63] A. Westin, *Privacy and Freedom,* (Atheneum, 1967).

Appendix I

User Requirement Questionnaire

Dear Participant,

The purpose of this questionnaire is to define the user requirements of the SPEAR project. SPEAR aims to provide effective solutions in detecting, responding and taking countermeasures against advanced cyber threats and attacks targeted to modern smart grids. Briefly, SPEAR proposes an integrated platform of methods, processes, tools and supporting tools for:

(a) Timely detection of evolved security attacks such as APT, Denial of Service (DoS) and Distributed DoS (DDoS) attacks using big data analytics, advanced visual-aided anomaly detection and embedded smart node trust management.
(b) Developing an advanced forensic readiness framework, based on smart honeypot deployment, which will be able to collect attack traces and prepare the necessary legal evidence in court, preserving the same time user private information.
(c) Implementing an anonymous smart grid channel for mitigating the lack of trust in exchanging sensitive information about cyber-attack incidents.
(d) Performing risk analysis and awareness through cyber hygiene frameworks, while empowering EU-wide consensus by collaborating with European and global security organisations, standardisation bodies, industry groups and smart grid operators.
(e) Exploiting the research outcomes to more CIN domains and creating competitive business models for utilising the implemented security tools in smart grid operators and actors across Europe.

Analysis of the answers you provide will be used for the system specification. We would appreciate if you kindly answer the following questions to the best of your knowledge.

Performance and functionality

1. What do you consider critical in terms of:
   a) time interval for detecting anomaly incident or security attacks of your system?
   b) response time for an attack?
   c) time interval for the result of the forensic analysis to be ready?

2. Please explain the scenario that would be most critical during the demonstration of your use case to assess SPEAR functionality and usability?

3. What are the major attacks you would like your Smart Grid to be protected from by SPEAR?

4. What critical features would you need improved in the availability, integrity and confidentiality safeguards of your system?

5. What key attack/incident data visualization and analysis capabilities would you consider an improvement from your current system in terms of cybersecurity? How would you like to visualise attacks and analysis results?

6. What key features would you need or want to be improved in a forensic framework in terms of collecting attack traces?

7. What key cyber-hygiene features would you need to enhance situational awareness within your environment?

Regulatory compliance and Reputation

8. What minimum standard and regulation would you need your Smart Grid system to follow in terms of privacy and security?

9. What barriers do you have in exchanging sensitive information about cyber-attack incidents?

10. What feature would increase your trust for exchanging anonymous information about smart grid incidents within a closed group of energy operators?

Business and organisational

11. What key processes, policies, best practices on cybersecurity and cyber-hygiene in your organisation do you consider key for SPEAR to help you with?

12. What business aspects would you expect SPEAR solution have an impact on and help you with?

Other requirements

13. Assuming there are requirements that were not mentioned above, please use the table below to provide these requirements and the expected value you hope to derive from them.

SN	Additional requirements	Rationale - Value expected

Appendix II

User, Security and Privacy Requirements Specification List

User Requirements

Req. id	**Req. Title**	**Req. Description**	**Priority** **High I medium I Low}**
UR-01	**Quick time of detection and response**	The SPEAR solution must be able to quickly detect and respond to cyber-attacks in a reasonable timeframe	High
UR-02	**Detection of known attacks**	The SPEAR solution must be able to detect attacks such as DoS, DDoS, brute force, man in the middle, SQL attacks, breach inside LAN	High
UR-03	**Availability**	• The security engineer must be able to access the SPEAR system 24/7; • The Smart-Home end-users must be able to have collected data on request according to the GDPR	High Medium
UR-04	**Secure transmission of data**	The SPEAR system must be able to ensure protection of data in transit.	High
UR-05	**Visualisation of different anomalies/attacks timeframes**	The security engineer must be able to visualises and filters different anomalies/attacks in different timeframes	High
UR-06	**A visual-added IDS with a central panel with option on specific IP devices or severity of events**	The security engineer must be able to assess a security event indicated by SPEAR-SIEM depending on the severity of the event	Medium
UR-07	**Remote notification**	The SPEAR solution must be able to support the offsite security engineers to receive a notification as soon as an anomaly has been identified by the SPEAR-SIEM through email notification	High
UR-08	**Information sharing of threat intelligence**	The SPEAR solution must be able to support gathering, sharing, storing and correlation of indicators of compromise of targeted attacks, threat intelligence	High

		and vulnerability information in a secure manner	
UR-09	**Common form of timestamps**	The SPEAR solution must be able to indicate unified timestamps across plant devices	High
UR-10	**Comply with relevant best practices, standards and laws**	The SPEAR Platform must support the smart grid system to be compliant to the data protection and security standards related to the functionalities offered (such as monitoring, or forensic auditing, or PIA).	High
UR-11	**Maintain privacy of personal data**	Personal data must be processed in compliance with data protection law	High
UR-12	**Reliability of tool**	The tool shall be able to add value to the business model of users	High
UR-13	**Differentiation of attacks**	The SPEAR system must be capable of differentiating cyber-attack from other anomalies caused by e.g., extreme weather conditions	High

Privacy Requirements

Req. id	Req. Title	Req. Description	Priority High I Medium I Low
PR-01	**Legal basis for data processing**	The SPEAR platform shall have a clear legal basis for processing personal data (stated in the privacy policy)	High
PR-02	**Data minimisation**	The SPEAR platform shall collect only a minimum personal data relevant for its purposes	High
PR-03	**Enablement of data subjects' rights**	The SPEAR platform shall support and enable a rights management capabilities for data subjects	High
PR-04	**Data accuracy**	Personal data processed in the system shall be accurate	High
PR-05	**Storage limitation**	• Personal data stored in the SPEAR platform shall be	High

		retained only for a period necessary to fulfil its purpose (end of the project); • Personal data that is no longer needed must be properly disposed	
PR-06	**DPIA compliance**	The platform shall incorporate a data protection impact assessment (DPIA) to ensure that appropriate protections are in place (See WP4)	High
PR-07	**Record of data processing**	The SPEAR platform shall support keeping a record of personal data processing within the platform	High
PR-08	**Transparency**	The SPEAR platform shall provide necessary information relating to data processing to the data subjects (to be included in the privacy policy)	High
PR-09	**Purpose limitation**	The SPEAR platform shall only process data for the specific purposes it was collected	High
PR-10	**Traceability of incidents**	The SPEAR platform shall support the logging of data to trace privacy and security incidents	High
PR-11	**Integrity, availability and confidentiality**	• The SPEAR platform shall use state of the art measures maintain the integrity, availability and confidentiality of personal data; • The system network communications must be protected from unauthorized	High

		information gathering and eavesdropping; - The system shall provide a data backup mechanism	
PR-12	**Strong authentication measures**	The system shall have strong authentication measures in place at all system gateways and entrance points	High
PR-13	**Secure location of data**	The SPEAR system shall use cloud systems subject to EU law	High

Ethical Requirements

Req. id	Req. Title	Req. Description	Priority High I medium I Low}
ER-01	Research ethics adherence	The SPEAR platform shall adhere to accepted research ethical standards.	High
ER-02	Safeguard research subject interests, including of cyber-attackers	The SPEAR platform shall treat honeypot attackers as research subjects, and take appropriate steps to safeguard them from harm or inconvenience, including measures to protect their data	High
ER-03	Assess constraints for use of honey pot in real-life	Real-life constraints to the use of honeypots shall be identified (Ref. WP 4)	High

Security Requirements

Req. id	Req. Title	Req. Description	Priority High I medium I Low}
SR-01	**Maintain a high level of Confidentiality, Integrity and Availability of the system**	• The system shall use a security protocol to protect user data over the Internet; • Ensure secure authentication control to the SPEAR tool; • Ensure regular backups and that the restoration procedures work as expected	High
SR-02	**Database security**	All databases where personal data are stored in the SPEAR platform must be encrypted, access to them must be restricted and authentication required to access such data	High
SR-03	**Systems Configuration**	The SPEAR system shall install only services and functionalities or connect equipment which is essential for the functioning and security of the system	High
SR-04	**Support compliance with regulations and standards in the smart grid sector**	The SPEAR system shall support compliance with relevant standards and laws on IT security where applicable	High
SR-05	**Continuous System Management**	The system shall apply security updates continuously	High
SR-06	**Interconnectivity security**	The SPEAR system shall ensure that the interaction between the different SPEAR components as well as between the SPEAR platform and other external systems shall be secure	High
SR-07	**Security of the honeypots**	The honeypot shall not compromise the security	High

		of the host network or machine.	
SR-08	**Logging**	The SPEAR platform shall establish relevant logging system	High