Secure and PrivaTE smArt gRid

(Grant Agreement No 787011)

D2.5 – System Specifications and Architecture

2019-08-31

Version 2.0

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	2.0
Document Owner	Eight Bells LTD (8BL)
Contributors	8BL, UOWM, SURREY, ENI, ED, SCHN, CERTH, LUH, TEC, PPC, VETS
Work Package	WP 2 - Use Case Preparation, Architecture, Security & Privacy Requirement
Deliverable Type	[PU]
Task	Task 2.2 – System Specification and Architecture
Document Status	Final
Dissemination Level	Public

Document History

Version	Author(s)	Date	Summary of changes
0.1	Ioannis Giannoulakis (8BL)	2019-01-09	ToC
0.2	Odysseas Nikolis, Nikos Vakakis, Dimos Ioannidis (CERTH)	2019-01-14	Contribution to Chapter 6
0.3	Pablo Gómez-Calvente Moreno (ENEL)	2019-01-15	Contribution to Chapter 5
0.4	Panagiotis Radoglou-Grammatikis (UOWM), Dimitrios Pliatsios (UOWM), Panagiotis Sarigiannidis (UOWM)	2019-01-16	Contribution to Chapters 3, 4 and 5
0.5	Emmanouil Panaousis, Muhammad Usman (SURR)	2019-01-16	Contribution to Chapter 1
0.51	Alkiviadis Giannakoulias (ED)		Contribution to Chapter 4 and 5
0.6	Vasilis Machamint (8BL)	2019-01-18	Contribution to Chapter 1 and Chapter 7
0.7	Eider Iturbe (TEC)	2019-01-21	Contribution to Chapter 5
0.8	Vasilis Machamint (8BL)	2019-01-29	Incorporation of reviewer's comments
0.81	Samuel Iheanyi Nwankwo (LUH)	2019-01-30	Comments on Deliverable Draft
0.9	Francisco Ramos (SCHN)	2019-01-30	Additions in Chapter 4

0.91	Vasilis Machamint (8BL), Panagiotis Radoglou-Grammatikis (UOWM), Dimitrios Pliatsios (UOWM), Panagiotis Sarigiannidis (UOWM), Muhammad Usman, Emmanouil Panaousis (SURREY), Odysseas Nikolis, Nikos Vakakis, Dimos Ioannidis (CERTH), Eider Iturbe (TEC)	2019-05-09	Revision of functional requirements based on the Project Officers guidelines
0.95	Vasilis Machamint (8BL) Panagiotis Radoglou-Grammatikis (UOWM), Dimitrios Pliatsios (UOWM), Panagiotis Sarigiannidis (UOWM), Muhammad Usman, Emmanouil Panaousis (SURREY), Odysseas Nikolis, Nikos Vakakis, Dimos Ioannidis (CERTH), Eider Iturbe (TEC)	2019-05-13	Final review of the functional and non-functional requirements
1.0	Vasilis Machamint (8BL)	2019-05-15	Final corrections on report. Finalization of Document: Acronyms, References and ToC
1.1	Vasilis Machamint (8BL), Panagiotis Radoglou-Gramattikis (UOWM), Dimitrios Pliatsios (UOWM), Panagiotis Sarigiannidis (UOWM), Odysseas Nikolis, Nikos Vakakis, Dimos Ioannidis (CERTH)	2019-07-01	Revised ToC based on the Project Review's comments
1.2	Alkiviadis Giannakoulias, Emmanouil Kaliorakis (ED)	2019-08-08	Additions in Chapter 5.2 in regards with the FRF components based on the Project Review's comments
1.3	Erkuden Rios Velasco, Eider Iturbe (TEC)	2019-08-15	Addition in Chapter 5.2 in regards with the RI components based on the Project Review's comments
1.4	Panagiotis Radoglou-Grammatikis (UOWM), Dimitrios Pliatsios (UOWM), Panagiotis Sarigiannidis (UOWM),	2019-08-16	Additions in Chapter 5.2 in regards with the SIEM components based on the Project Review's comments

	Emmanouil Panaousis (SURR) Erkuden Rios Velasco, Eider Iturbe (TEC)		
1.5	Vasilis Machamint (8BL) Panagiotis Radoglou-Grammatikis (UOWM), Dimitrios Pliatsios (UOWM), Panagiotis Sarigiannidis (UOWM), Erkuden Rios Velasco, Eider Iturbe (TEC) Emmanouil Panaousis (SURREY) Alkiviadis Giannakoulias, Emmanouil Kaliorakis (ED) Odysseas Nikolis, Nikos Vakakis, Dimos Ioannidis (CERTH)	2019-08-22	Based on reviewers' comments that the deliverable should be updated with technologies used, the technologies used for all the components of SIEM, FRF and RI have been introduced in Sections 5.2.1.3, 5.2.2.3, 5.2.3.3, 5.2.4.3, 5.2.5.3, **Error! Reference source not found.**, 5.2.6.3, 5.2.7.3 and 5.2.8.3
1.6	Panagiotis Radoglou-Grammatikis (UOWM), Dimitrios Pliatsios (UOWM), Panagiotis Sarigiannidis (UOWM), Erkuden Rios Velasco, Eider Iturbe (TEC) Emmanouil Panaousis (SURREY) Alkiviadis Giannakoulias, Emmanouil Kaliorakis (ED) Odysseas Nikolis, Nikos Vakakis, Dimos Ioannidis (CERTH)	2019-08-23	Based on reviewers' comments, the decomposition model of SPEAR has been introduced in a more detailed manner in Sections 5.2.1.2, 5.2.2.2, 5.2.3.2, 5.2.4.2, 5.2.5.2, **Error! Reference source not found.**, 5.2.6.2, 5.2.7.2 and 5.2.8.2
1.7	Panagiotis Radoglou-Grammatikis (UOWM) Erkuden Rios Velasco, Eider Iturbe (TEC) Emmanouil Panaousis (SURR) Alkiviadis Giannakoulias, Emmanouil Kaliorakis (ED) Odysseas Nikolis, Nikos Vakakis, Dimos Ioannidis (CERTH)	2019-08-26	Based on reviewer's comments, the information model of the SPEAR system has been updated in order to better clarify what gets communicated and how. Information flow of each component is presented in Sections 5.2.1.2, 5.2.2.2, 5.2.3.2, 5.2.4.2, 5.2.5.2, **Error! Reference source not found.**, 5.2.6.2, 5.2.7.2 and 5.2.8.2, .The interdependencies among the components are described in Sections 5.2.1.4, 5.2.2.4, 5.2.3.4, 5.2.4.4, 5.2.5.4, **Error! Reference source not found.**, 5.2.6.4, 5.2.7.4 and 5.2.8.4 Finally, the interfaces model in Section 5.3 has been updated
1.8	Panagiotis Radoglou-Grammatikis (UOWM)	2019-08-26	Enrichment of the Functional and Non-Functional Requirements in Section 4

	Erkuden Rios Velasco, Eider Iturbe (TEC) Emmanouil Panaousis (SURR) Alkiviadis Giannakoulias, Emmanouil Kaliorakis (ED) Vasilis Machamint (8BL)		
1.9	Panagiotis Radoglou-Grammatikis (UOWM) Vasilis Machamint (8BL)	2019-08-28	Final Review of Added Content
2.0	Vasilis Machamint (8BL)	2019-09-03	Final corrections on report. Report formatting. Finalization of Document: Acronyms, References and ToC

Internal Review History

Reviewed By	Date	Summary of Comments
Stamatia Bibi (UOWM)	2019-01-28	The quality of the deliverables is good. However, some comments attached inside the deliverable should be taken into account.
Erkuden Rios Velasco (TECN)	2019-01-28	The deliverable is acceptable. A few sections of the document need to be modified.
Dimosthenis Ioannidis (CERTH)	2019-09-02	The deliverable is acceptable. A few modifications on the functional requirements are suggested. Typographical errors should be corrected. An update on the document history should be provided
Panagiotis Sarigiannidis (UOWM)	2019-09-03	The deliverable is acceptable. A few revisions on the requirements are suggested. Some comments attached inside the deliverable should be taken into account.

Legal Notice

Table of Contents

Acronyms

Acronym	Explanation
ACC	Accuracy
AIS	Artificial Immune System
AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AUC	Area Under Curve
BDAC	Big Data Analytics Component
C&C	Command-and-Control
CCS	Centralized Control System
CIA	Central Intelligence Agency
CISO	Chief Information Security Officer
CPS	Cyber-Physical System
CSO	Chief Security Officer
DCS	Distributed Control System
DDoS	Distributed DoS
DF	Digital Forensic
DHS	Department of Homeland Security
DMS	Distribution Management System
DNS	Domain Name System
DoS	Denial of Service
DPO	Data Protection Officer
DR	Demand Response
DSM	Demand Side Management
EMS	Energy Management System
ENISA	European Network and Information Security Agency
EPCIP	European Program for Critical Infrastructure Protection
EU	European Union
FACTS	Flexible Alternating Current Transmission System
FP	False Positive
GDPR	General Data Protection Regulation
GIS	Geographic Information System
GLR	Generalized Likelihood Ratio
GOF	Grid OpenFlow Firewall
GTM	Grid Trusted Module
HAN	Home Area Network
HIDS	Host-based Intrusion Detection System
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
IAN	Industry Area Network
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communications Technology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers

IoT	Internet of Things
IPS	Intrusion Prevention System
LOED	Locally Optimum Estimated Direction
LOUD	Locally Optimum Unknown Direction
MBR	Master Boot Record
MOA	Massive Online Analysis
MTU	Master Terminal Unit
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
OKB	Ontology Knowledge Base
OSI	Open Systems Interconnection
OTS	One Time Signature
PC	Personal Computer
PET	Privacy-Enhancing Technology
PIA	Privacy Impact Assessment
PLC	Programmable Logic Controller
PPC	Public Power Corporation
QoS	Quality of Service
R2L	Remote to Local
RAM	Random Access Memory
RBAC	Role Based Access Control
RFC	the Request for Comment
RTU	Remote Terminal Unit
SAMT	Security Administration Modules and Tool
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SPEAR-CHF	SPEAR Cyber Hygiene Framework
SPEAR-FR	SPEAR Forensic Repository
SPEAR-FRF	SPEAR Forensic Readiness Framework
SPEAR-RI	SPEAR Repository of Incidents
SPEAR-SIEM	SPEAR Security Information and Event Management
SRAC	Smart Grid RbAC
STATCOM	Static Synchronous Compensator
SVC	Static VAR Compensator
SVM	Support Vector Machine
TNR	True Negative Rate
TPR	True Positive Rate
TRSC	Testing, Research and Standards Centre
U2R	User to Root
UML	Unified Modelling Language

List of Figures

List of Tables

Executive Summary

This Deliverable (D 2.5 System Specification and Architecture) provides a full description of the SPEAR project architecture. It is based on Task 2.2, which aims to output the System Specification and the SPEAR architecture. The Deliverable defines the SPEAR project architecture fed by the smart grid application requirements in security, privacy and information protection. Specifically, the identified requirements of Task 2.1 are analysed in order to determine a set of system specifications (technical, functional, non-functional) covering all the technological states of SPEAR project and thus affecting the development in WP3, WP4, WP5, as well as the longitudinal studies in WP6 and WP7.

The document is structured in 7 Chapters:

Chapter 1: An introduction regarding the scopes of the Deliverable, the definition of Smart Grid (SG) and the SPEAR Glossary.

Chapter 2: Description of the SPEAR Conceptual view and introduction of the methodology for the architecture description of the SPEAR project.

Chapter 3: Description of the Context Viewpoint of the SPEAR platform.

Chapter 4: Definition of the SPEAR functional and non-functional requirements.

Chapter 5: Decomposition of the SPEAR platform and description of the SPEAR system in terms of its components and information objects.

Chapter 6: The adoption of the SPEAR Platform in the four SPEAR use cases.

Chapter 7: Conclusions

1. Introduction

[space to be removed]The energy sector is at the beginning of the new era of the Smart Grids (SG) and is going through a major digital transformation, with an increase in the complexity of its technological environment and an escalation of interconnected equipment [1]. In modern SG networks, the traditional power grid is empowered by technological advances in sensing, measurement, and control devices as well as with two-way communications between the suppliers and consumers. The SG integration helps the power grid networks to be smarter, but it also increases the risk of attacks because of the existing obsolete cyber-infrastructure or that was not prepared to internet connectivity. Taking into account that the power grid is one of the most critical infrastructures, cybersecurity should be addressed not only at a technical point of view, but also from an operational and organisational one [2].

Over the last decade, cyberattacks have become increasingly sophisticated, stealthy, targeted and multi-faceted which may leverage zero-day exploits and highly creative interdisciplinary attack methods. Furthermore, due to the increasing connectivity of the SG and interdependency between systems and communication networks, there are many vulnerabilities that can be exploited. Securing the Grid against cyberattacks is an issue that is crucial for both the operation and the reliability of the SG. During the past years, operational SGs have been the target of criminals and could be easily affected by security threats because of their complexity and their cyber-physical connectivity.

The platform proposed by the SPEAR project aims to provide effective solutions in detecting, responding and taking countermeasures against advanced cyber threats and attacks targeted to modern SGs. SPEAR envisions to develop an integrated platform of methods, processes, and tools that will detect and respond to cyberattacks using innovative technologies and capabilities, and ultimately assure the resilient operation of the SG. This deliverable addresses the complexity of SG applications and describes thoroughly the SPEAR System Specifications. It defines the SPEAR platform architecture fed by the SPEAR use cases' requirements on security, privacy and information protection. The identified requirements of the Deliverable 2.1 are analysed in order to determine a set of system specifications (technical, functional, operational) covering all the technological aspects of the SPEAR platform.

1.1 Definition of Smart Grid

Over the past decades, electricity networks evolved from medium-scale grid networks to interconnected electric grids, which are based on generating stations that distribute power to major local centres and provide electricity to a large number of end-users. These stations, commonly referred to as power plants, were designed on a large scale for continuous operation and have generated most of the used electrical energy.

By the end of the 20th century, this old electricity network infrastructure was proven to be unreliable and inadequate with respect to modern challenges, such as alternative energy sources, electricity demand and energy saving policies. The SG is a concept that answers to the need for a new, environmentally friendly electricity network, which should be able to efficiently provide the desired energy at the desired time. The SG generally referred to as the next-generation power system, is an evolution of the current power grids. With the integration of advanced computing and communication technologies, the SG is expected to strengthen the reliability and enhance the resilience of the future renewable energy-based grid [3].

The term "SG" defines 'a self-healing network equipped with dynamic optimization techniques that use real-time measurements to minimize network losses, maintain voltage levels, increase reliability, and improve asset management. The operational data collected by the SG and its sub-systems will allow system operators to rapidly identify the best strategy to secure against attacks, vulnerability, and so on, caused by various contingencies' [4]. Based on performance measures, the working definition of the SG is the following: *The SG is an advanced digital two-way power flow power system capable of self-healing, and adaptive, resilient, and sustainable, with foresight for prediction under different uncertainties. It is equipped for interoperability with present and future standards of components, devices, and systems that are cyber-secured against malicious attack* [4].

SG development does not aim to replace the current electricity infrastructure. Instead, it aims to enhance the existing network by introducing novel services and features to the grid, while maintaining, when possible, the old physical infrastructure. [3]. The SG uses a two-way flow of information to create a high level of automation and a distributed energy

delivery network. Apart from the technical aspects, its successful and efficient implementation relies on accurate financial planning.

Compared with the traditional power systems, the SG is envisioned to fully integrate high-speed and two-way communication technologies into millions of power devices to establish a dynamic and interactive infrastructure with new energy management capabilities, such as Advanced Metering Infrastructure (AMI), Demand Response (DR) and Demand Side Management (DSM) [5]. However, the heavy dependence on information sharing exposes the SG to various vulnerabilities associated with telecommunications and network systems. This puts the reliable and secure operation of the grid at risk, which, nonetheless, is the ultimate objective of the SG. Network intrusion by attackers may lead to a variety of severe consequences in the grid, potentially resulting in exposure of private information, operation failures, blackouts or even destruction of infrastructures [5]. Thus, along with the silent features of the SG, cybersecurity emerges to be a critical issue as millions of electronic devices are interconnected via communication networks throughout critical power facilities, which has an immediate impact on the reliability of such a widespread infrastructure.

1.1.1 Assets of Smart Grid

The advent of SG adds more dimensions to the asset management problem of the utilities. Utilities will have to adapt and expand their asset models to integrate the innovations of the SG Systems and meet their needs. The software tools that have been used so far by the utilities are listed below [6]:

- Asset / Work Management Systems: These systems concentrate on recordkeeping and asset lifecycle tracking, including the work resources applied to construct and maintain the plant.
- Fixed Asset Accounting: Fixed asset systems manage the property records of the business from a financial value standpoint.
- Geographic Information System (GIS): These systems are used to layout (design) new facilities and model the relationships of assets to the electrical network.
- Planning Systems: Utilities use various software solutions to plan and model their network and predict its operation under normal and extreme conditions.
- SCADA Systems: These systems maintain sufficient asset information to enable dispatchers to operate the network in real-time.
- Distribution Management System (DMS): DMS combines the analytics of the planning systems with the real-time infrastructure of the SCADA systems. It allows utilities to optimize and automate their operations.

SG will integrate as a set of new technologies deployed over transmission and distribution systems, and its deployment will include new assets such as [7]:

- Advanced Interrupting Switches
- AMI
- Smart Meters
- Controllable/regulating Inverter s
- Customer Energy Management System (EMS)/Display/Portal
- Distribution Management System
- Enhanced Fault Detection Technology
- Flexible Alternating Current Transmission System (FACTS) Devices
- Microgrid Controllers
- Electric Vehicle Charging Stations
- Software - Advanced Analysis/Visualization
- Two-way Communications

Utilities need to adapt and develop plans to move towards an approach in which asset data and the processes to update that data must evolve [6]. These innovative asset models will enhance the functionality of the grid and help utilities operate in an augmented and largely interconnected environment.

1.2 Cyber-Physical Attacks Against Smart Grids

SG is a complex system of numerous constituting (sub)systems. It is one of the most heterogeneous Cyber-Physical Systems (CPSs) that are 'products' of the modern IoT industrial revolution 4.0 era. One of the key components of the power system operation and control is the control centre. The diversity and complexity, however, come with a wide range of security attacks [8]. A pictorial view of the cyber-physical attacks and threats in the SG realm is provided in Figure 1.

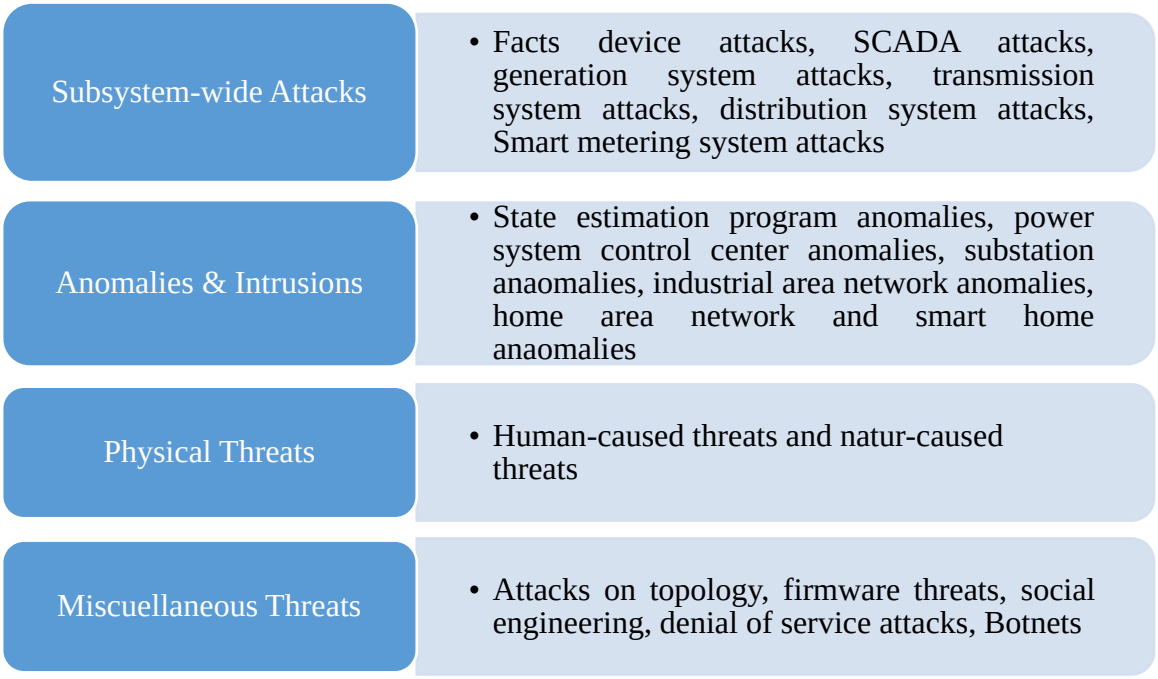


Figure 1: Cyber-Physical Attacks on SGs.

1.3 SPEAR Glossary

This subsection aims to clarify the glossary of the SPEAR project. It contains and explains the most common terms that will be used throughout the project design and implementation phases. This glossary can facilitate the understanding of the SPEAR key concepts and the standardization of the terms used in the project.

SPEAR-SIEM: The *SPEAR Security Information and Event Management (SPEAR SIEM)* tool is an advanced all-in-one, open-source tool which is designed for timely detecting threats and attacks in smart environments. It incorporates new technologies for detecting targeted attacks based on visual-aided techniques, advanced analytics and trust management. The SPEAR-SIEM tool will be able to aggregate log data collected from all SG systems. Novel technologies, such as big data analytics, will be used for the processing of the collected events and logs, allowing for quick cyberattack detection. The rationale behind the SPEAR point of view in detecting cyberattacks through SIEM tools is associated with an efficient all-in-one approach. The SPEAR SIEM tool will remove specific barriers of conventional SIEM tools, such as the limitations in capacity, in processing high volumes of data and in self-healing, when it is threatened by internal or external attacks.

SPEAR-FRF: The *SPEAR Forensic Readiness Framework (SPEAR-FRF)* intends to assure forensic readiness in the sense that the applied network forensic strategies are deployed before a cyberattack incident takes place. SPEAR-FRF will develop proactive forensic tools in line with three main methodologies, namely planning, implementation and assessment. Planning includes defining scenarios, storage and evidence handling. Implementation involves the pre-incident collection, pre-incident analysis and logging. Assessment involves the evaluation of the implementation processes and the subsequent results.

SPEAR-RI: SPEAR intends to contribute to improving the situational awareness by creating and maintaining a repository of SG incidents. The rationale behind the creation of this repository is to broadcast, inform and exchange critical information about cyberattack incidents in SGs across Europe. The SPEAR Repository of Incidents (SPEAR-RI) will develop the idea of utilising a network of trust where sensitive information is exchanged between institutes. It will form an anonymous repository using group signature and k-anonymity technology in sharing information. SG organisations across Europe will able to broadcast sensitive information in an anonymous way without exposing the reputation of the organisation. The advantages of the SPEAR-RI are the exchange of real-time security data and analysis, the circulation of best countermeasures practices, the comparison of various security solutions both from a technical and operational viewpoint and the ability to establish an open dialogue amongst anonymous peers who represent SG organisations (e.g., power plants) across Europe.

SPEAR-CHF: The *SPEAR Cyber Hygiene Framework (SPEAR-CHF)* is a set of safety protocols, recommendations and policies which will be defined, based on rigorous risk analysis and after intensive penetration tests in the end-users defence systems. Awareness-raising initiatives will be identified and integrated to such as manuals, guidelines, best practices and 'what to do in case of cyber-threats' guidelines based on the specific needs in SGs. Through cyber hygiene, SPEAR intends to increase society's resilience to significant threats.

BDAC: *Big Data Analytics Component (BDAC*) incorporates the *big data analytics capabilities* of the SPEAR SIEM system towards providing early anomaly detection. It extends the capabilities of SPEAR-SIEM by adopting big data analytics towards fact and accurate anomaly detection by applying correlation and machine learning decision-making to the logs received by the SPEAR-SIEM basis.

VIDS: *Visual-based Intrusion Detection System (VIDS)* brings dynamic visual-assisted analytics in the SPEAR SIEM system. VIDS will enable the usage of visual-based techniques in quickly detecting cyberattacks. The visual-based IDS system will offer a faster and more efficient way of observing and monitoring the whole smart grid subsystems using visual-assisted components.

GTM: *Grid Trusted Module (GTM)* is a component of the SPEAR SIEM system that is equipped with trust management algorithms and will apply node-centric reputation computation algorithms to all nodes (devices, meters, interfaces and gateways) connected to the SG ecosystem where each node may represent any smart device in the SG ecosystem. GTM will extend the capabilities of the SPEAR SIEM system by proactively addressing internal incidents such as accidental mistakes, hardware failures and malicious actions from inside.

AMI: *AMI* is an integrated system that enables two-way communication between utilities and IP-enabled smart metering devices. The system is able to monitor remotely power consumption on a real-time basis, connect and disconnect service of the device, etc. The need for communication and data transmission between consumers and utilities make AMI vulnerable to various cyberattacks.

APT: An Advanced Persistent Threat (*APT)* is a prolonged computer network attack in which a person or a group gains unauthorized access to a network and remains undetected for an extended period. The intention of APT attacks is to achieve and maintain continuous access to a targeted network rather than cause damage to the network.

IAN: *An Industry Area Network (IAN)* is a type of network that operates within an industrial environment. It connects sensors, controllers and building management systems into the network and it can be also used for the automation of processes.

HAN: *A Home Area Network (HAN)* is a type of network that operates within limited boundaries, i.e., a home or an office. It connects users' in-home devices, such as computers, peripheral devices, etc. into the network.

Honeypot: A honeypot is a mechanism aiming to imitate cyberattack targets. It is mainly used to distract attackers from the most crucial components of a network and issue early warnings for upcoming cyberattacks. Moreover, it can be used as a data source for gathering forensic information on the adversaries within a honeypot.

PLC: *Programmable Logic Controller (PLC)* is a digital computer mainly used for automation of electromechanical processes and industrial automation, i.e., assembly lines.

RTU: A Remote Terminal Unit (*RTU)* is a multi-purpose electronic device that interfaces objects in the physical world to a control system or SCADA system. It is typically deployed in an industrial environment and it can be used as a master controller for other devices in order to automate various processes.

SCADA: The *Supervisory Control and Data Acquisition (SCADA)* is a Centralised Control System (CCS) architecture that uses computers, networked data communications and a graphical user interface for high-level process supervisory management. It is a system of software and hardware elements that allows industrial organizations to:

- Control industrial processes locally or at remote locations.
- Monitor, gather, and process real-time data.
- Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software.
- Record events into log files

Smart Meter: It is an IP-enabled metering device that is capable of monitoring energy consumption in an automated way on a regular basis and/or in real-time. They enable two-way communication with the utilities and they are capable of providing necessary data for billing processes.

Threat actor: It is an individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. A threat actor is responsible for an incident that impacts – or has the potential to impact -- an organization's security.

Threat assessment: It is the practice of determining the credibility and seriousness of a potential threat, as well as the probability that the threat will become a reality. A threat assessment consists of a detailed evaluation of the characteristics of individual threats.

Vulnerability: It refers to a weakness of an IT system or component that renders it open to exploitation and attacks.

2. SPEAR Architecture

This section describes the SPEAR Conceptual view and introduces the methodology applied for the architecture description of the SPEAR project.

2.1 SPEAR Concept

The SPEAR platform relies on the basic concept that cybersecurity must be considered in all domains, components and subsystems of the smart grid and at all phases of the grid lifecycle. The transformation of the legacy power industry to the modern SG has led to a complex system that involves both IT and electricity operation and administration which apparently presents many and severe challenges in security, privacy and data protection. Timely detection becomes a necessity since traditional log collection and SIEM systems are unable to handle the huge number of smart devices, sensors and meters a modern smart grid composes. As illustrated in Figure 2, SPEAR brings an added value for addressing this backbreaking goal by introducing a second level of defence in the SIEM tools, where big data analytics in conjunction with visual-aided IDS will timely detect a stealth cyberattack, if it is missed by the basic SIEM tool due to lack of processing time. SPEAR efforts in anomaly detection employ the trust management concept by effectively controlling all nodes of the smart grid based on their (traffic) behaviour. Moreover, all SPEAR SIEM tools are essentially interconnected together by exchanging critical update information (patches, virus lists, black IP addresses list and malicious software fixes) using the common SPEAR-RI in an anonymous way. In this respect, SPEAR supports an enriched anomaly detection system, minimising the time needed for detecting sophisticated cyberattacks, and at the same time, advances the smart grid defence system to an EU-wide wall, where common experience and defence strategies are exchanged, against cyberattackers.

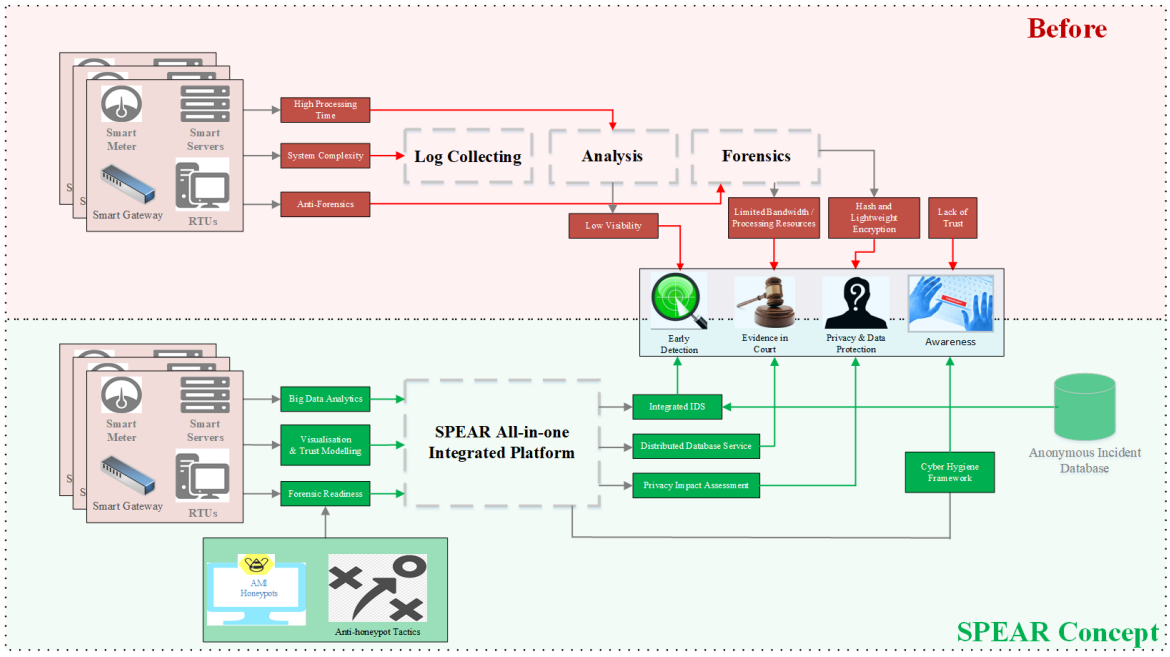


Figure 2: SPEAR concept against current view.

2.2 Methodology for Architecture Description

The SPEAR architecture has been completed by developing the viewpoints in the ARCADE framework [9]. This framework is an open architecture description framework influenced by IEEE 1471-2000, Recommended Practice for Architecture Description of Software-Intensive Systems [10].

The framework includes the following viewpoints to describe system architectures:

Context viewpoint:

The purpose of the context viewpoint (see Section 3) is to describe all aspects of the SPEAR platform's environment, including the interfaces between the SPEAR platform and its environment. This viewpoint enables understanding of all the interactions that SPEAR platform has with the external eco-system that it is a part of, thereby allowing a clear description of the interfaces. The context viewpoint describes the concepts (domain model) managed by SPEAR and the main stakeholders that interact with the SPEAR platform. In addition, this viewpoint also allows the definition of high-level work processes and the main information elements used by the stakeholders. Finally, the viewpoint describes the systems that can be found in the surroundings of the SPEAR platform interacting with it.

Requirement viewpoint:

The purpose of the requirement viewpoint (see Section 4) is to document all specific requirements related to the SPEAR platform from the end-user business perspective and regulatory compliance perspective for data protection and security. This viewpoint enables understanding of the end-user needs to enhance their business operation, as well as the legal framework that the SPEAR platform has to comply with for processing personal data such as the General Data Protection Regulation (GDPR). The security of the platform is considered under this viewpoint. Both functional and non-functional requirement emanating from these end-user and legal requirements are detailed in D2.4—User, Security and Privacy Requirements, and relevant aspects are reflected here in D2.5 in section 4.

Component viewpoint:

The purpose of the component viewpoint (see Section 5) is to describe the SPEAR system in terms of its subsystems, components and information objects. The viewpoint reports the way that information is processed by the SPEAR components and subsystems and describes their interconnections and interactions. The component viewpoint focuses on the structure of the SPEAR system. It describes the SPEAR architecture at a functional level and from a technology-independent perspective. As part of the component view, the models reported in this section are created with special focus on information, system decomposition, system collaboration, and interfaces specification.

The initial SPEAR framework specification, reported in this document, includes the description of the aforementioned three viewpoints defined by Arcade. Apart from these viewpoints, the ARCADE framework defines two more viewpoints, the Distribution viewpoint and the Realisation viewpoint. The purpose of the distribution viewpoint is to describe the logical distribution of software and hardware components. The distribution viewpoint shows how the components are "logically" placed and separated from each other. Furthermore, the purpose of the realisation viewpoint is to describe how the final system's components should be implemented and deployed into a real-life environment using real technology. The two latter viewpoints are more technology dependent and will be part of future deliverables of SPEAR technical Work Packages.

3. Context viewpoint

This section describes the context viewpoint of the SPEAR architecture. The context viewpoint describes the environment of the SPEAR system in terms of its business-related aspects, other involved technical systems and the mapping of business aspects to the target system.

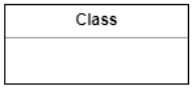
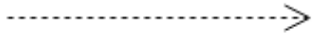
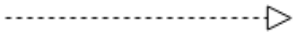
3.1 Domain model

The domain model presents the key concepts of SPEAR platform and their relations. Its purpose is to give an understanding of the scope of the project domain among the project participants as well as outsiders to the project. Figure 3 shows the SPEAR domain model as a Unified Modelling Language (UML) class diagram. The concepts found in yellow belong to the general domain of the SG system, and the concepts in green are related to the SPEAR objectives of ensuring data protection security and privacy to the SG domain.

With the aim to make the model more readable, only the key concepts and relations have been included in the figure.

The notation and colour coding used for the domain model elements are summarized in Table 1.

Table 1: Notation of domain model elements

	Class/Concept
	Dependency
	Aggregation
	Generalization
	Realization
	Smart Grid system related concept
	Cybersecurity related concept

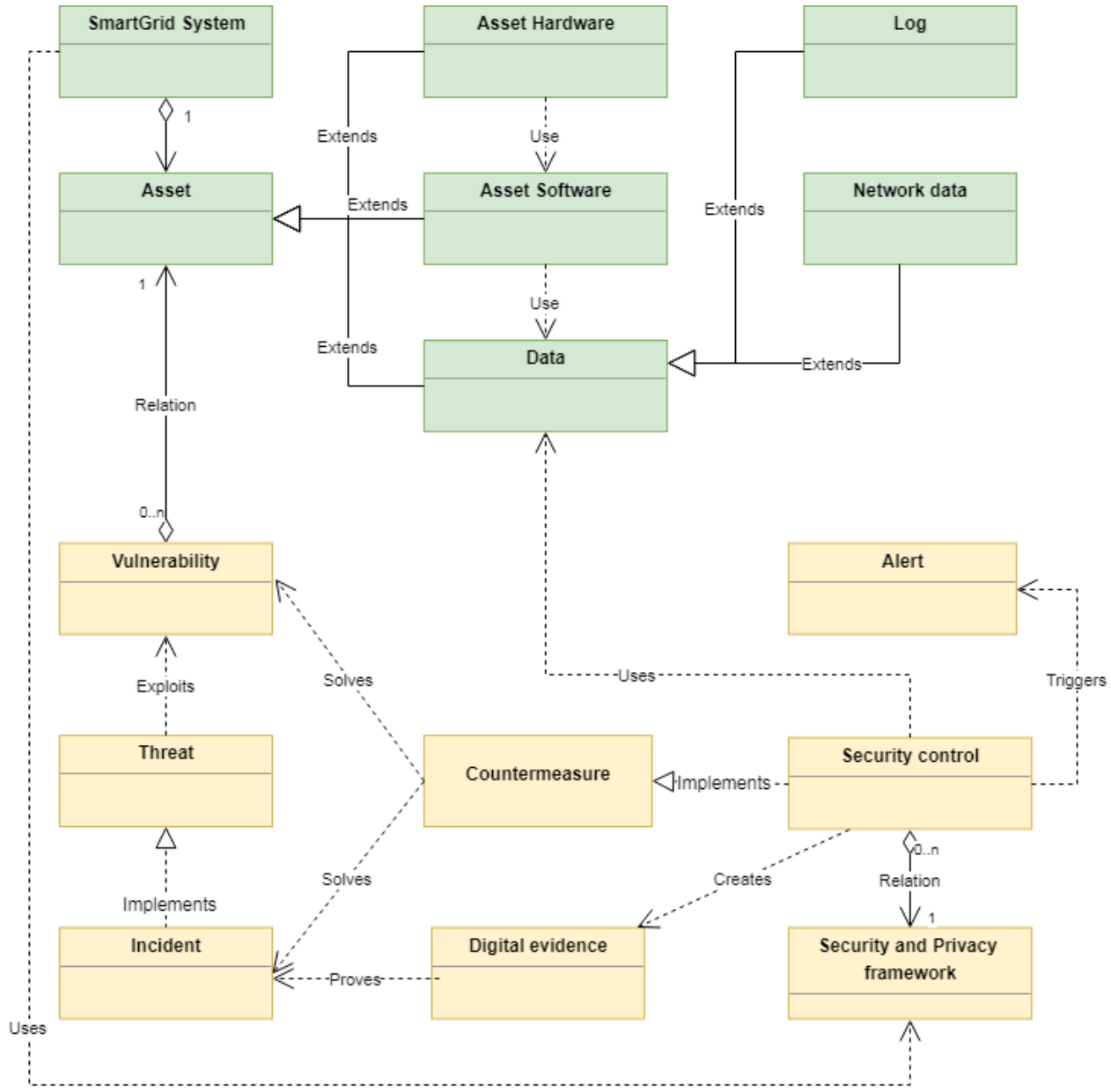


Figure 3: SPEAR domain model.

Table 2 describes the main concepts in the context of the project. The SPEAR Glossary provides a more exhaustive list and definitions of the terms (Section 1.3).

Table 2: Explanation of SPEAR key concepts

Concept name	Description
Smart Grid system	*'Electricity networks that can efficiently integrate the behaviour and actions of all users connected to it - generators, consumers and those that do both - in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply* ' [11].
Asset	*'A system resource that is (a) required to be protected by an information system's security policy, (b) intended to be protected by a countermeasure, or (c) required for a system's mission'* [12]. According to ENISA, there are a plethora of asset types in the SG system. However, regarding cybersecurity, in SPEAR, we consider assets that are mainly related to information and communication technology: hardware, software and information assets. These assets generate or process data and as such are exposed to cybersecurity threats [13].
Hardware Asset	*'The material physical components of an information system'* [12]. In SPEAR, the hardware assets are the physical components of the SG system. According to ENISA, the physical components considered as main assets of SG include RTU, IED, PLC, Distributed Control System (DCS), Smart meters, Servers, Clients (tablet, smart phone, printer, etc.) and network components (routers, gateways, firewalls, etc.) [13].
Software Asset	*'Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution'* [12]. In SPEAR, the software assets are computer programs used by the SG physical components. According to ENISA, the software components considered as main assets of a SG include specific applications such as SCADA systems, standard software (database, web server), operating system, device drivers and firmware [13].
Data Asset	*'Information in a specific representation, usually as a sequence of symbols that have meaning'* [12]. In SPEAR, the data asset refers to representations that can be recognized, processed, or produced by a software asset. According to ENISA, information is a valuable asset as, depending on it, SG system software and/or administrators can make a decision [13]. The main data assets include operational information about electrical assets, historical information., system configuration, network traffic, etc. as well as potential personal data.
Digital evidence	*'Digital evidence is data that supports or refutes a hypothesis that was formulated during the investigation. This is a general notion of evidence and may include data that may not be court admissible because it was not properly or legally acquired'* [14]. In SPEAR, we refer to electronic evidence supporting forensic investigation hypothesis.

Concept name	Description
Log	*'A log, in a computing context, is the automatically produced and time-stamped documentation of events relevant to a particular system'* [15]. In SPEAR, a log refers to automatically produced and time-stamped documentation of events by SG assets.
Network data	'Network data in computer networks is mostly encapsulated in network packets, which provide the load in the network. '
Vulnerability	*'A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy* [12]' . SPEAR is focused on vulnerabilities of SG systems.
Threat	*'A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm'* [12]. A threat is realised by exploiting *vulnerabilities* in a service or application.
Incident	*A security event that involves a security violation* [12]. And a security event is *an occurrence in a system that is relevant to the security of the system* [12].
Countermeasure	*'An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken'* [12].
Security control	The security policies and procedures that are prescribed by Security control frameworks as countermeasures or safeguards to grant specific security characteristics. In SPEAR, the security controls are characterised as a type of countermeasures in security domains that can be used to mitigate or prevent certain risks in the SG system.
Alert	In SPEAR, an alert is a notification that an unwanted incident happened in the SG system.
Security and Privacy framework	A data structure that organizes and categorizes the security controls that an information system or an organization should apply to create business value and minimize risk.

3.2 Business to system mapping model

The *Business to system mapping model* section presents stakeholders and the high-level work process that SPEAR supports.

3.2.1 SPEAR stakeholders

The main stakeholders of the SPEAR platform are those that interact either directly or indirectly with it in the operation of the SG systems.

The main stakeholders of the SPEAR platform are the system administrators or more specifically the security administrators. According to the Internet Security Glossary RFC 4949 [12], an administrator is a person that is responsible for configuring, maintaining, and administering the TOE[1] in a correct manner for maximum security. This concept is related to administrative security, which is defined as Management procedures and constraints to prevent unauthorized access to a system [12].

Other stakeholders that can interact with the SPEAR Platform are in the following:

- the Chief Security Officer (CSO) who is responsible for the physical and digital security of a company, including people, assets, communication and business systems, infrastructure and technology [16].
- the Chief Information Security Officer (CISO) who is responsible for developing and implementing an information security program, which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats [17].
- Data Protection Officer (DPO) who is responsible for ensuring the internal application of the GDPR and that the rights and freedoms of the data subjects are not likely to be adversely affected by the processing operations.

3.2.2 Business process overview: Overall process

The SPEAR Platform supports the operation of the SG system, including partially the configuration of the system and mainly the SG monitoring and incident reporting.

During the deployment and configuration of the SG system, the SPEAR platform needs to be deployed as well. In particular, the AMI honeypots part of the SPEAR platform must be taken into consideration as part of the whole system in case they are deployed as industrial honeypots. In case they are considered as research honeypots, the appropriate configuration must be designed for them isolated from the operation system.

During the SG operation, the SPEAR platform provides monitoring capabilities. In particular, it provides high capacity Security Incident and Event Management capabilities. For that purpose, the SPEAR platform captures data from the SG system from heterogeneous sources such as network traffic (which includes also industrial protocols used in SG environments) and syslogs from devices in the system. Afterwards, the SPEAR platform follows data analytics processes in order to detect anomalies in the system: (i) pre-processing of the collected data (i.e. preparation for the data analytics step), (ii) both data analytics and visual analytics in order to detect anomalies that are classified as incidents by the SPEAR platform, and (iii) the reputation of the system is calculated based on the incidents detected by the SPEAR platform. Finally, the SPEAR platform notifies the system administrator and displays the details of the incidents.

Finally, as part of the incident reporting activity, the SPEAR platform provides services to support the forensic evidence management process; therefore, the collected data can be used legally in court in case any incident is detected by the SPEAR platform. The SPEAR platform also provides an anonymous channel among SG stakeholders with the purpose of exchanging cybersecurity incidents.

[1] Target of Evaluation

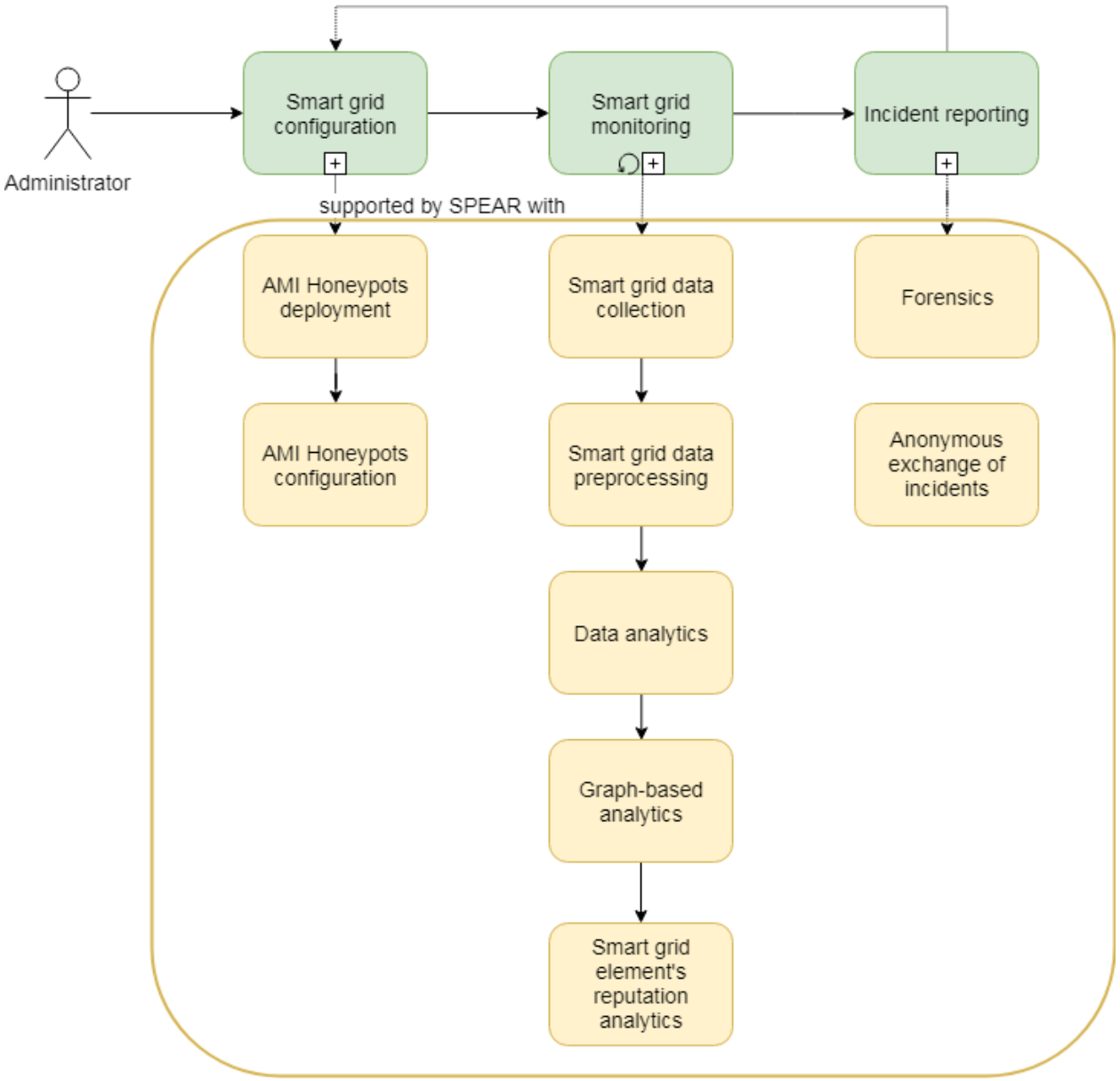


Figure 4: SPEAR support in the operation of the SG operation.

3.3 Environment systems

This section explains the *environment systems* of the SPEAR Platform, i.e., the systems that typically could be found working together with it. The environment systems include the physical and software assets that the SPEAR Platform needs to interface with, and thus influence the operation of the platform.

Mainly the SPEAR Platform will interact with the physical software assets of a SG system (see section 1.1.1).

4. Requirement Viewpoint

This section deals with the description of the functional and non-functional requirements of the SPEAR system. Requirements are descriptions of the services that a software system must provide and the constraints under which it must operate. They can range from high-level abstract statements of services or system constraints to detailed mathematical functional specifications. This section reports on the different types of requirements of the SPEAR Project that have been classified explicitly into categories and have been univocally identified, avoiding inconsistencies and duplication of concepts. ARCADE methodology has been used to report the identified system requirements. The methodology provides a structure that ensures that documentation of the developed requirements in D2.4 and D2.5 will have a uniform structure and content.

There are two different types of requirements in the SPEAR project; user and system requirements. User requirements need to be described in the business domain and in any format that allows a mutual understanding with the users. They aim to describe what the user does with the system, i.e., what activities are necessary for the users. These requirements are accompanied by statements in the natural language, plus diagrams of the services that the systems provide and its operational constraints. User requirements are extensively reported in D2.4; however, they are reflected where appropriate in this deliverable.

System requirements are the building blocks used by the developers to build the system. These are the traditional “shall” statements that describe what the system “shall do.” They are reported in this section and their output will be used by activities of WP3, WP4 and WP5. The System requirements of the SPEAR project are classified following the below criteria:

- Functional requirements, specifying behaviour or functions that the system components should be able to perform. These include ‘statements of services that the system should provide, how the system should react to particular inputs and how the system should behave in particular situations’ [19].
- Non-functional Requirements, which cover the remaining requirements that judge the operation of the system and specify how the system should behave. Non- functional requirements can be ‘constraints on the services or functions offered by the system such as timing constraints, constraints on the development process, standards’ [19].

In order to guide the project development, a set of functional and non-functional requirements have been identified and have undergone a refinement process involving the WP leaders and the technical manager of the project. A dedicated repository file reports the functional and non-functional requirements with the following attributes:

- **Req ID:** An identifier of each requirement (unique for each requirement)
- **Title:** A short title of the requirement (unique title for each requirement)
- **Description:** A description of the requirement, which is written in such a way that the meaning is clear, even when standing alone without the benefit of context
- **Type:** The requirement type, categorized in the following way:
    - Functionality
    - Usability
    - Reliability
    - Efficiency
    - Maintainability
- **Target WP:** The requirements are considered to be project-wide. However, they have been allocated to one or more Work Packages in order to facilitate the gathering, definition, monitoring and analysis of the requirements.
- **Target Module:** The requirements of the SPEAR solution may refer to one or more of the SPEAR components:
    - SPEAR SIEM Basis
    - SPEAR VIDS
    - SPEAR GTM
    - SPEAR-RI

    - SPEAR-FR
    - AMI Honeypot
    - Honeypot Manager
    - BDAC
    - GTM
    - Message Bus
    - SPEAR Platform
- **Priority:** The importance of each requirement for achieving the objectives of the project is indicated based on the following categorization:
    - **M:** Must have this requirement to meet project goals
    - **S:** Should have this requirement if possible, but project success does not rely on it
    - **C:** Could have this requirement if it does not affect anything else on the project
- **How addressed:** It describes the actions that should be done to verify that the particular requirement is met.
- **Relation to User Requirements:** Linking of the requirement with user requirements

The functional and non-functional requirements, reported in the following subsections, are stored in a dedicated Jira Repository of the project's portal website and can be found at https://space.uowm.gr/jira. The repository will be undergoing updates over the course of the project in order to improve the requirements and continuously track their progress. Additionally, to the requirements presented in the following sub-sections, a set of user, privacy, security and ethics requirements pertaining to the SPEAR solution has been also identified and is reported in D2.4.

4.1 Functional Requirements

The functional requirements of the SPEAR system are presented below. The requirements ID, name and description are reported. Furthermore, each requirement is linked with other sources of the SPEAR project, such as user, security and privacy requirements.

Req ID: **F01**	**Title**: Assets Protection
Definition - Description	The SPEAR platform must be able to collect and analyze information for each asset of an environment, thus being able to detect possible security events.
Type	Functionality
Target WP	3
Target Module	SPEAR SIEM Basis, BDAC, VIDS, GTM
Priority	S
How addressed	OSSIM will provide an asset management environment as well as signatures rules that will protect each asset. Accordingly, BDAC and VIDS will analyze network traffic flows and operational data related to the assets monitored. Finally, GTM will calculate the reputation of each asset regarding its criticality. Artificial cyberattacks will be performed to evaluate the response of SPEAR SIEM Basis, BDAC and VIDS during WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-03, UR-02, UR-05, UR-06, UR-12, UR-13

Req ID: **F02**	**Title**: Cyberthreats Visualization
Definition - Description	The system operator or the security administrator must be able to control the lifecycle of a possible threat via a graphical user interface. VIDS should timely detect cyberthreats by utilizing a visualization dashboard.

Type	Functionality
Target WP	3
Target Module	VIDS
Priority	S
How addressed	The system operator or the security administrator will be able to understand the lifecycle of a possible threat via the visual analytics provided by VIDS. Artificial cyberattacks will be performed and the response of the visual analytics will be evaluated during WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-03, UR-05, UR-06, UR-12, UR-13

Req ID: **F03**	**Title**: Data Transmission
Definition - Description	The SPEAR Platform should support high-throughput data transmission between the data sources and the SPEAR SIEM components.
Type	Functionality
Target WP	3
Target Module	SPEAR SIEM Basis, Message Bus, GTM
Priority	S
How addressed	SPEAR SIEM Basis, Message Bus and GTM will handle this requirements by measuring the transmission delay between the various communications. This requirement will be tested on WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-04, UR-11, UR-12

Req ID: **F04**	**Title**: Data Collection
Definition - Description	The SPEAR platform must collect intrusion detection data at a centralized place, which will be accessible to the system operator or the security administrator.
Type	Functionality
Target WP	3, 4
Target Module	SPEAR SIEM Basis, VIDS
Priority	S
How addressed	All security events will be visualised by the OSSIM dashboard and VIDS accordingly. Artificial cyberattacks will be performed and the response of the OSSIM dashboard and the VIDS dashboard will be evaluated during WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-05, UR-13

Req ID: **F05**	**Title**: Data Analysis
Definition - Description	The SPEAR platform should collect and analyze data from different sources, thus detecting possible alerts.
Type	Functionality
Target WP	3

Target Module	SPEAR SIEM Basis, BDAC, VIDS
Priority	S
How addressed	OSSIM (via OSSEC IDPS and Suricata IDPS), BDAC and VIDS will be able to implement deep packet inspection, analyze network traffic flows and operational data for each asset of an environment. This capability will be tested during WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-05, UR-08, UR-09, UR-12

Req ID: **F06**	**Title**: Storage of Data
Definition - Description	Data processing within the SPEAR Platform shall comply with relevant best practices, standards and laws, and for personal data processing GDPR should be addressed.
Type	Functionality
Target WP	3,4,5
Target Module	SPEAR Platform
Priority	S
How addressed	1. Physical location of the server is important to consider (e.g. whether it is within EU or in a third country), taking into account the relevant GDPR provisions (charter V). 2. For each case of personal data storage on remote server, it is essential to assess the purpose of the processing, e.g. whether storage is necessary for the provision of the core service or it is performed for back-up or other purposes (such as analytics). 3. Assess the types of personal data stored in each remote server (content, metadata), paying particular attention to back-ups which in some cases might be stored without the users being aware of them. 4. Define the exact retention period of the personal data on each remote server, as well as whether personal data can be permanently erased from all servers and what is the procedure. 5. Encryption of stored personal data, is an important measure to protect against unauthorized external access. It is essential that standard and up-to-date cryptographic protocols and sufficient key lengths are used, as well as whether personal data can be retrieved in case that the encryption key is lost. An additional point to assess is personal data integrity controls upon retrieval from the remote servers.
Relation to User, Security and Privacy Requirements	UR-09, UR-10 to UR-12, PR-01 to PR-13

Req ID: **F07**	**Title**: Alerts Categorization
Definition - Description	The SPEAR platform should provide near real-time alerts for the suspected intrusions. Alerts should be divided into a) High, b) Medium and c) Low.
Type	Functionality
Target WP	3
Target Module	SPEAR SIEM Basis, BDAC, VIDS
Priority	S

How addressed	Each security event detected by OSSIM Sensor, OSSIM Server, BDAC and VIDS will be characterised by a risk value which will identify how critical an event is and will categorize it into three possible classes: a) High, b) Medium and c) Low. Each security event will be visualised by VIDS with the specific class. Artificial cyberattacks with a different impact will be used to test this capability during WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-02, UR-06, UR-07, UR-12, UR-13

Req ID: **F08**	**Title**: Encrypted Communication
Definition - Description	In order to protect communications, SPEAR components should communicate with each other using encryption methods. The utilization of strong cryptographic protocols and algorithms will support end-to-end encryption, which will ensure that only the communicating components can have access to the content of the communication.
Type	Functionality
Target WP	3,4,5
Target Module	SPEAR SIEM Basis, BDAC, VIDS, GTM, RI
Priority	S
How addressed	1. Standard and up-to-date cryptographic protocols should be used (and not custom solutions), following relevant recommendations of national (e.g. BSI in Germany, ANSI in France, NIST in USA) or international organizations (e.g. IETF, ISO) in the field, including ENISA report on "Algorithms, key size and parameters report". 2. Support of forward secrecy property. 3. Encryption keys should be generated and stored only at the end-user's servers.
Relation to User, Security and Privacy Requirements	UR-04, UR-11, UR-12

Req ID: **F09**	**Title**: Data Preprocessing
Definition - Description	The BDAC component should be able to preprocess smart grid data making them ready for the machine learning models.
Type	Functionality
Target WP	3
Target Module	SPEAR SIEM Basis, BDAC
Priority	S
How addressed	BDAC will utilize Apache SPARK for fast smart gird data preprocessing.
Relation to User, Security and Privacy Requirements	UR-10, UR-12

Req ID: **F10**	**Title**: Interconnectivity

Definition - Description	The BDAC component should be connected with the SPEAR SIEM basis DAPS to receive smart grid data for the models.
Type	Functionality
Target WP	3
Target Module	BDAC
Priority	S
How addressed	The BDAC needs to interconnect with the SPEAR SIEM Basis DAPS for the collection of the data. A client service will poll the SPEAR SIEM Basis DAPS storage mechanism (DB, Elasticsearch, etc.) for the collection of the data.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-03, UR-04

Req ID: **F11**	**Title**: Operation
Definition - Description	The BDAC component should be able to operate both on a single machine and on a cluster of machines for faster data processing.
Type	Functionality
Target WP	3
Target Module	BDAC
Priority	M
How addressed	Apache SPARK can operate both on a single machine as well as on a cluster.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-10

Req ID: **F12**	**Title**: BDAC interconnection with Message Bus
Definition - Description	BDAC should interconnect with the Message Bus.
Type	Functionality
Target WP	3
Target Module	BDAC, Message Bus
Priority	M
How addressed	BDAC needs to interconnect with the Message Bus for the production/reception of cybersecurity alerts. A client service will poll the SPEAR Message Bus storage mechanism (DB, Apache Kafka, etc.) for the management of the alerts.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-04, UR-09, UR-12

Req ID: **F13**	**Title**: Multi-Layer Intrusion/Anomaly Detection
Definition - Description	BDAC should detect possible cyberattacks and anomalies at multiple network layers
Type	Functionality

Target WP	3
Target Module	BDAC
Priority	M
How addressed	BDAC will detect possible attacks by analysing TCP/IP network flows, data from the application layer (OSI level 7) protocols as well as operational data
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-08 to UR-13, PR-01, PR-02, PR-05 to PR-09

Req ID: **F14**	**Title**: Operational data-based Anomaly Detection
Definition - Description	BDAC should detect cyberattacks and anomalies based on operational data
Type	Functionality
Target WP	3
Target Module	BDAC
Priority	M
How addressed	BDAC will detect possible attacks based on the operational data given by the SPEAR end users by adopting ML and DL algorithms.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-08 to UR-13, PR-01, PR-02, PR-05 to PR-09

Req ID: **F15**	**Title**: BDAC re-training
Definition - Description	BDAC should retrain its ML/DL detection models based on the data received in order to enhance and update its detection capability
Type	Functionality
Target WP	3
Target Module	BDAC
Priority	M
How addressed	BDAC will use the data from the SPEAR SIEM Basis as well as python-based machine learning and data handling algorithms and SPARK in order to re-training its models.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-08 to UR-13, PR-01, PR-05 to PR-09

Req ID: **F16**	**Title**: Honeypot-based Anomaly Detection
Definition - Description	BDAC should detect cyberattacks and anomalies based on the information received by the honeypots.
Type	Functionality
Target WP	3
Target Module	BDAC

Priority	M
How addressed	BDAC will detect possible attacks by analysing the network traffic files generated by the honeypots activities
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-08 to UR-13, PR-01, PR-02, PR-05 to PR-09

Req ID: **F17**	**Title**: Intrusion Detection
Definition - Description	The SPEAR platform must detect attacks with a wide range of techniques such as network flows or behaviour analysis and deep packet inspection.
Type	Functionality
Target WP	3
Target Module	BDAC, VIDS
Priority	S
How addressed	OSSIM, BDAC and VIDS will use different methods to detect cyberattacks, including signature-based and anomaly-based processes as well as visual analytics. Also, BDAC will use anomaly detection processes for detecting attacks per application layer packet (e.g., Modbus packets) and per TCP/IP network flows. Also, BDAC will be able to detect attacks based on operational data. All detection processes will be evaluated by performing artificial cyberattacks during WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-03

Req ID: **F18**	**Title**: DoS Protection
Definition - Description	The SPEAR platform must detect Denial of Service (DoS) attacks.
Type	Functionality
Target WP	3
Target Module	BDAC, VIDS
Priority	S
How addressed	OSSIM, BDAC and VIDS will provide mechanisms to detect DoS attacks. DoS cyberattacks will be performed to test the protection mechanisms of the previous components during WP3 and WP7.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-03

Req ID: **F19**	**Title**: VIDS Authentication
Definition - Description	The VIDS dashboard has to include an authentication mechanism.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	S

How addressed	VIDS dashboard will provide an authentication mechanism based on the description of the requirement. The authentication mechanism of VIDS will be tested during WP3.
Relation to User, Security and Privacy Requirements	UR-03, UR-09 to UR-12

Req ID: **F20**	**Title**: Remote Notifications
Definition - Description	The SPEAR platform should be able to send remote notifications for the possible alerts generated. The SPEAR platform should also have the ability to simultaneously provide multiple notifications such as e-mail notifications and SMS notifications.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	M
How addressed	VIDS will provide suitable notifications for each security event detected. This capability will be tested during WP3 and WP7 by executing artificial cyberattacks.
Relation to User, Security and Privacy Requirements	UR-07

Req ID: **F21**	**Title**: VIDS user roles
Definition - Description	The VIDS should support different user roles.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	M
How addressed	The different user roles are identified by the stakeholders and end-user requirements. The VIDS should support different user roles which have different access privileges to the SPEAR platform.
Relation to User, Security and Privacy Requirements	UR-03, UR-05, UR-07, UR-09 to UR-12, PR12

Req ID: **F22**	**Title**: VIDS user role dashboard views
Definition - Description	The VIDS should provide specific dashboard view related with the access privileges and the need of each user role.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	M
How addressed	Based on the end-user requirements and the VIDS features different VIDS dashboard views are going to be created.

Relation to User, Security and Privacy Requirements	UR-03, UR-05, UR-06, UR-07, UR-09 to UR-12

Req ID: **F23**	**Title**: VIDS users authentication DB
Definition - Description	The VIDS should provide an user authentication service with a local DB.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	M
How addressed	The VIDS application is based on a web-application framework which provides user authentication services with the local DB.
Relation to User, Security and Privacy Requirements	UR-03, UR-04, UR-09 to UR-12

Req ID: **F24**	**Title**: VIDS Analytics vendor agnostic application
Definition - Description	The VIDS Visual Analytics dashboard should be a vendor agnostic application.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	S
How addressed	The implementation of the Visual Analytics dashboard is a web based front-end user application.
Relation to User, Security and Privacy Requirements	UR-03, UR-05, UR-06, UR-12

Req ID: **F25**	**Title**: VIDS Analytics user parametrization
Definition - Description	The VIDS Visual Analytics application should provide interaction with the user and user parametrization.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	S
How addressed	The Visual Analytics web based front-end user application will provide user interfaces to accept input and parameters from the user in order to adjust its content based on the user needs.
Relation to User, Security and Privacy Requirements	UR-03, UR-05, UR-06, UR-07,UR-12

Req ID: **F26**	**Title**: VIDS Analytics visualization methods
Definition - Description	The VIDS Visual Analytics application should provide various visualization methods.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	S
How addressed	The Visual Analytics application is based on widely used visualization libraries which support a variety of visualization methods and provide also the framework to adjust and create visualization based on the application needs.
Relation to User, Security and Privacy Requirements	UR-03, UR-05, UR-06, UR-07, UR-08, UR-12

Req ID: **F27**	**Title**: VIDS Analytics response time
Definition - Description	The VIDS Visual Analytics application should be fast and responsive back-end service.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	M
How addressed	The Visual Analytics application has a back-end server to take over all the computational intensive tasks such as the execution of the analytics algorithms. This architecture will make the web application more robust, fast and responsive.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-04, UR-05, UR-12

Req ID: **F28**	**Title**: VIDS Visual Analytics interconnection with SIEM Basis
Definition - Description	The VIDS Visual Analytics back-end services should interconnect with the SPEAR SIEM Basis.
Type	Functionality
Target WP	3
Target Module	VIDS, SIEM Basis
Priority	M
How addressed	The Visual Analytics back-end service needs to interconnect with the SPEAR SIEM Basis for the collection of the data. A client service will poll the SPEAR SIEM Basis storage mechanism (DB, Elasticsearch, etc.) for the collection of the data.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-04, UR-05, UR-12,PF06, SF02

Req ID: **F29**	**Title**: VIDS interconnection with Message Bus
Definition - Description	The VIDS back-end services should interconnect with the SPEAR Message Bus.
Type	Functionality
Target WP	3
Target Module	VIDS, Message Bus
Priority	M
How addressed	The VIDS back-end service needs to interconnect with the SPEAR Message Bus for the production/reception of cybersecurity alerts. A client service will poll the SPEAR Message Bus storage mechanism (DB, Apache Kafka, etc.) for the management of the alerts.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-04, UR-05, UR-06, UR-12, PF06, SF02, SF06

Req ID: **F30**	**Title**: VIDS Analytics data visualization algorithms
Definition - Description	The VIDS Visual Analytics back-end services should provide visual and data analytics methods and algorithms for better analysis and visualization of the data.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	M
How addressed	The Visual Analytics back-end services will host various visual and data analytics methods from well tested and open source libraries. Also, custom algorithms may be developed to cover the SPEAR requirements and objectives.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-04, UR-05, UR-09

Req ID: **F31**	**Title**: VIDS Analytics anomaly detection mechanism
Definition - Description	The VIDS Visual Analytics back-end services may provide local anomaly detection mechanisms complementary with the BDAC functionality.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	C
How addressed	The Visual Analytics back-end service may provide analysis on timeseries or post processed data that is related with anomaly detection techniques. This processing is provided with a service and is complementary to the BDAC functionality.
Relation to User, Security and Privacy Requirements	UR-01, UR-02, UR-05, UR-08

Req ID: **F32**	**Title**: VIDS Analytics processing limitations
Definition - Description	The VIDS Visual Analytics back-end services may should monitor and manage the size of the incoming data in order avoid slow processing and memory limitations.
Type	Functionality
Target WP	3
Target Module	VIDS
Priority	C
How addressed	The specification of the host servers of the Visual Analytics back-end services will determine the size of the data under analysis.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-04, UR-05

Req ID: **F33**	**Title**: VIDS Visual Analytics interconnection with GTM
Definition - Description	The VIDS Visual Analytics back-end services should interconnect with GTM
Type	Functionality
Target WP	3
Target Module	VIDS, GTM
Priority	M
How addressed	The Visual Analytics back-end service needs to interconnect with the GTM for the collection of the data. This interconnection will be achieved via a REST web service.
Relation to User, Security and Privacy Requirements	UR-01, UR-03, UR-04, UR-05

Req ID: **F34**	**Title**: Asset Reputation
Definition - Description	A reputation score that characterises the behaviour (malicious or legitimate) of this asset.
Type	Functionality
Target WP	3
Target Module	GTM
Priority	M
How addressed	GTM will be able to calculate reputation scores for each asset by combining the information generated by BDAC and a set of predetermined rules.
Relation to User, Security and Privacy Requirements	UR-12

Req ID: **F35**	**Title**: Trust Asset Alerts
Definition - Description	Two different alert types that indicate that 1) the node reputation goes below a predefined threshold, 2) the rate of decrease of the node reputation exceeds a predefined threshold.
Type	Functionality
Target WP	3
Target Module	GTM
Priority	S
How addressed	GTM will assess different criteria to raise alert for informing the sys admin about ongoing asset misbehaviours.
Relation to User, Security and Privacy Requirements	UR-12

Req ID: **F36**	**Title**: Trust System Alert
Definition - Description	A system-wide alert that informs the administrators about the number of assets that have been compromised, aiming to accelerate the investigation of an incident before it compromises the entire system.
Type	Functionality
Target WP	3
Target Module	GTM
Priority	S
How addressed	When the number of misbehaving nodes, i.e., the nodes that satisfy the alert criteria of GF02, exceed a predefined threshold, SPEAR platform will raise a system-wide alert to escalate the importance of investigating the entire system.
Relation to User, Security and Privacy Requirements	UR-03, UR-07, UR-12

Req ID: **F37**	**Title**: Sensors and Honeypots Deployment
Definition - Description	The SPEAR platform must be able to deploy the SPEAR SIEM and AMI honeypots in different phases of the energy chain.
Type	Functionality
Target WP	3, 4
Target Module	SPEAR SIEM Basis, AMI Honeypots
Priority	S
How addressed	SPEAR SIEM and the AMI honeypots will be deployed in all SPEAR use cases whose operation corresponds to different phases of the energy chain. The SPEAR SIEM and the AMI honeypots need to be able to capture and emulate (respectively) traffic of diverse industrial protocols depending on the energy chain phase. The deployment of the SPEAR SIEM and AMI honeypots will be evaluated during WP3, WP4 and WP7.
Relation to User, Security and Privacy Requirements	UR-04, UR-10, UR-11

Req ID: **F38**	**Title**: HoneyPots
Definition - Description	A security service should provide a HoneyPot service that emulates the real behaviour of AMI devices of smart grids in order to attract cyber attackers, and monitor and capture attack traces for the SPEAR Platform.
Type	Functionality
Target WP	4
Target Module	AMI Honeypot
Priority	S
How addressed	Honeypots services will be deployed in all SPEAR use cases. Their deployment will be evaluated during WP3, WP4 and WP7.
Relation to User, Security and Privacy Requirements	UR-04, UR-10, UR-11

Req ID: **F39**	**Title**: Forensic Data Collection
Definition - Description	The SPEAR platform must collect necessary forensic data to support forensic investigations
Type	Functionality
Target WP	4
Target Module	FR
Priority	M
How addressed	SPEAR-FR should support collection of: 1. Full content data (pcap files) 2. Session data (flow records - NetFlow) 3. Statistical data (sometimes also referred to as metadata) 4. Log files 5. Security events generated by the SPEAR SIEM Basis, VIDS and BDAC.
Relation to User, Security and Privacy Requirements	UR-10

Req ID: **F40**	**Title**: Forensic Data Transmission
Definition - Description	The network/transport protocol used for transferring the forensic data, it has to: a) be secured against eavesdropping, b) protect the integrity of the forwarded data against manipulation or lost messages and c) be able to deal with network outages.
Type	Functionality
Target WP	4
Target Module	FR
Priority	M
How addressed	1. PCAP files addressed through the use of secure protocols, such as SSH and HTTPS, to ensure protection in transit. 2. For NetFlow traffic addressed through a secured (IPSEC, VPN tunnel) line between the NetFlow probe and collector. 3. For log files addressed through the use the Reliable Event Logging Protocol

	(RELP), which is designed to ensure reliable transfer of syslog messages at a higher layer and can also be used over TLS, although use of RELP over UDP is not advised. 4. Security events will be stored as log entries in the relevant component and forwarded using RELP (see point 3 above).
Relation to User, Security and Privacy Requirements	UR-04, UR-10, UR-11, UR-12

Req ID: **F41**	**Title**: Forensic Data Storage
Definition - Description	The SPEAR Forensic Repository must securely store collected forensic data.
Type	Functionality
Target WP	4
Target Module	FR
Priority	M
How addressed	This requirement will be addressed by using dm-crypt with LUKS extension.
Relation to User, Security and Privacy Requirements	UR-10, UR-11, UR-12

Req ID: **F42**	**Title**: Forensic Data Access
Definition - Description	Access to the forensic data stored in the SPEAR-FR should be controlled.
Type	Functionality
Target WP	4
Target Module	FR
Priority	M
How addressed	In case of a security event that triggers a forensic investigation: 1. Either the affected organization consults an external contractor or 2. Uses own resources. In both cases, the organization should have a well-defined and strict policy on how to decrypt the repository and make it available to the forensic investigator. This should be backed-up by a legal document (contract) that legally binds the investigator from releasing any private information found within the repository.
Relation to User, Security and Privacy Requirements	UR-10, UR-11

Req ID: **F43**	**Title**: Availability of forensic data
Definition - Description	Availability ensures that information and systems are available and accessible. Processes such as redundancy, failover, RAID and high-availability database clusters are used to mitigate consequences when hardware issues occur. It should be assured that accessibility to forensic data is possible; otherwise unavailability of data can become problematic, leading to overall service unavailability or degradation as the data owner is unable to access forensic data. We should regularly backup the SPEAR Forensic Repository
Type	Functionality
Target WP	4
Target Module	FR
Priority	M
How addressed	On a weekly basis a cryptographically verifiable copy of the SPEAR Forensic Repository will be made.
Relation to User, Security and Privacy Requirements	UR-12

Req ID: **F44**	**Title**: Forensic Data Timeline
Definition - Description	SPEAR should address the problem of time skew between servers and the problem of timestamp format, to allow investigators build a comprehensive timeline.
Type	Functionality
Target WP	4
Target Module	FR
Priority	M
How addressed	Addressed via: a) synchronize clocks on all systems using NTP or a similar system, b) standardise time formats as much as possible c) include complete, high-precision timestamps (full four-digit year) with time zone information, in the form of an offset, not the name of the time zone and d) normalise timestamps to UTC as early as possible in the log chain.
Relation to User, Security and Privacy Requirements	UR-09, UR-12

Req ID: **F45**	**Title**: Data Protection Impact Assessment (DPIA)
Definition - Description	DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them).
Type	Functionality
Target WP	4

Target Module	FR
Priority	M
How addressed	SPEAR will ensure that DPIA is successfully executed and all appropriate measures have been taken to ensure compliance.
Relation to User, Security and Privacy Requirements	UR-10, UR-11

Req ID: **F46**	**Title**: Anonymous Information Sharing
Definition - Description	The RI must provide a service for information sharing among different stakeholders in the smart grid industry through an anonymous communication channel. The information shared will be based on the detect events and anomalies by the SPEAR SIEM.
Type	Functionality
Target WP	5
Target Module	SPEAR RI
Priority	M
How addressed	The RI will be addressed in WP5 and will provide anonymous interconnection channels amongst the smart grid operators. It will allow all involved actors to upload and provide details of a cybersecurity incident anonymously
Relation to User, Security and Privacy Requirements	UR-08, UR-10

Req ID: **F47**	**Title**: Event Description
Definition - Description	The RI should provide sufficient supporting data to allow an operator to understand the context of a suspicious event being reported
Type	Functionality
Target WP	5
Target Module	SPEAR RI
Priority	M
How addressed	The RI should provide sufficient supporting data to allow an operator to understand the context of a suspicious event being reported
Relation to User, Security and Privacy Requirements	UR-08

4.2 Non-Functional Requirements

The non-functional requirements of the SPEAR system are presented below. The requirements ID, name and description are reported. Furthermore, each requirement is linked with other sources of the SPEAR project, such as user requirements.

Req ID: **NF01**	**Title**: Optionality
Definition - Description	The SPEAR platform should be able to operate under as many OSes as possibly
Type	Usability
Target WP	3,4,5,6
Target Module	SPEAR SIEM Basis, BDAC, VIDS, GTM, RI
Priority	S
How addressed	The seamless operation of the SPEAR solution should be tested and validated under various OSes
Relation to User, Security and Privacy Requirements	UR-12

Req ID: **NF02**	**Title**: Scalability
Definition - Description	The SPEAR platform must be expandable by adding assets.
Type	Usability
Target WP	3
Target Module	SPEAR SIEM Basis, GTM
Priority	M
How addressed	The SPEAR SIEM Basis will be able to handle this requirement via the asset management functionality. Also GTM will be able to calculate the reputation of any additional node. This requirement will be tested during WP3 and WP7, by inserting new assets.
Relation to User, Security and Privacy Requirements	UR-12

Req ID: **NF03**	**Title**: Data volume
Definition - Description	The SPEAR platform must be able to handle big data (terabytes).
Type	Reliability
Target WP	3
Target Module	BDAC
Priority	M
How addressed	BDAC will satisfy this requirement by using the Apache SPARK tool. This requirement will be tested during WP3 and WP7 testing operations.
Relation to User, Security and Privacy Requirements	UR-4, UR-8, UR-12

Req ID: **NF04**	**Title**: Password Encryption
Definition - Description	The SPEAR solution should make use of encryption to ensure that data is stored securely. The system should not store user passwords in plain-text.

Type	Reliability
Target WP	3,4,6
Target Module	SPEAR SIEM Basis, BDAC, VIDS, GTM, FR, SPEAR RI
Priority	M
How addressed	Encryption of sensitive data, such as passwords, will be tested during WP7 testing operations
Relation to User, Security and Privacy Requirements	UR-04, UR-11, UR-12

Req ID: **NF05**	**Title**: Data Encryption
Definition - Description	The SPEAR solution should not allow, when possible, any data transmission of sensitive information without encryption
Type	Reliability
Target WP	3,4,5, 6
Target Module	SPEAR SIEM Basis, BDAC, VIDS, GTM,, RI
Priority	S
How addressed	The communication between the components of the SPEAR solution will be tested to validate that there is sufficient data encryption.
Relation to User, Security and Privacy Requirements	UR-04, UR-10, UR-12

Req ID: **NF06**	**Title**: Backup
Definition - Description	The platform should backup data frequently (e.g. every hour) such that it may be restored to a working state without any data loss.
Type	Maintainability
Target WP	6
Target Module	SPEAR Platform
Priority	M
How addressed	A backup of the stored Databases should be held, in order to minimize important data loss in the tested use cases.
Relation to User, Security and Privacy Requirements	UR-03, UR-12

Req ID: **NF07**	**Title**: Non-repudiation
Definition - Description	All accesses to the SPEAR components should be registered, using log mechanisms, for non-repudiation effects
Type	Maintainability
Target WP	3, 4, 5, 6
Target Module	SPEAR Platform
Priority	M

How addressed	Log files for the accesses to all SPEAR components should be kept and tested in all three use cases
Relation to User, Security and Privacy Requirements	UR-09

Req ID: **NF08**	**Title**: Bandwidth
Definition - Description	Communication among the SPEAR components should not impose a significant load on the LAN or WAN bandwidth
Type	Efficiency
Target WP	3, 4, 5, 6
Target Module	SPEAR SIEM Basis, BDAC, VIDS, GTM, RI
Priority	S
How addressed	SPEAR solution will validate this requirement in the testing operations for the use cases and ensure that the communication among the SPEAR components does not affect significantly the operation of the LAN or WAN networks
Relation to User, Security and Privacy Requirements	UR-12

Req ID: **NF09**	**Title**: Security
Definition - Description	The system should be secure against unauthorized access to any of its data. Furthermore it should not allow the unauthorized use of any of its components
Type	Reliability
Target WP	3, 4, 5, 6
Target Module	SPEAR Platform
Priority	S
How addressed	SPEAR activities in charge of deploying and validating the integrated platform into the end user environment should ensure the security of the platform in the tested use cases
Relation to User, Security and Privacy Requirements	UR-04, UR-12

Req ID: **NF10**	**Title**: Access Security
Definition - Description	System Components must ensure trusted relationships among themselves. Secure and reliable two-way data communications should be used among the components
Type	Reliability
Target WP	3, 4, 5, 6
Target Module	SPEAR Platform
Priority	M
How addressed	Activities in the integration and testing period should ensure the secure communication among the Components in the tested use cases

Relation to User, Security and Privacy Requirements	UR-04, UR-09

Req ID: **NF11**	**Title**: Compliance
Definition - Description	All system data must be stored in compliance with data protection and privacy legislation
Type	Reliability
Target WP	3, 4, 5, 6
Target Module	SPEAR Platform
Priority	M
How addressed	This requirement will be addressed during the testing operations for the use cases. It will be validated that all data of the SPEAR components are stored in compliance with the EU legislation
Relation to User, Security and Privacy Requirements	UR-10, UR-11

Req ID: **NF12**	**Title**: Impact on Performance
Definition - Description	There should be a low impact on the end-user device performance caused by the SPEAR solution
Type	Efficiency
Target WP	3, 4, 5, 6
Target Module	SPEAR Platform
Priority	M
How addressed	The impact on performance of user devices will be validated in the tested use cases
Relation to User, Security and Privacy Requirements	-

Req ID: **NF13**	**Title**: Guidelines for using SPEAR Solution
Definition - Description	Guidelines could be provided to the end-users for SPEAR's safe and secure operation
Type	Usability
Target WP	7
Target Module	SPEAR Platform
Priority	M
How addressed	A public report with guidelines on the utilization of the SPEAR solution to be delivered to all end-users
Relation to User, Security and Privacy Requirements	UR-12

Req ID: **NF14**	**Title**: User-friendliness
Definition - Description	The visualised components of the Solution should be provided with a user-friendly Graphical-user Interface
Type	Usability
Target WP	3,4,5,6
Target Module	SPEAR Platform
Priority	M
How addressed	The user-friendliness of the GUI will be validated by the three use cases
Relation to User, Security and Privacy Requirements	UR-05, UR-12

5. Component viewpoint

This section defines and describes the decomposition of the SPEAR system into components, including their interfaces, interaction, and information. It presents the SPEAR system in terms of its subcomponents and information objects, and documents how the component interaction and data processing of the SPEAR platform is performed.

5.1 System information model

In this section, we describe the main information elements in the SPEAR Platform as show in Table 4. These information elements are the ones used by the components in the platform or exchanged among them. A more detailed description of the interconnection and interfaces among the SPEAR component is reported in Sections 5.4.2 and 5.4.3

Table 3: Description of items in the information model

Item	Description

Smart Grid Data	In SPEAR, the data asset refers to representations that can be recognized, processed, or produced by a software asset of the SG system. The main data assets that SPEAR is going to handle are:
	• Network traffic that includes:
	  ○ SG specific communication protocols traffic data,
	  ○ Operational information involved in the payload of the SG specific communication protocols traffic data,
	  ○ and TCP/IP Networkflow data.
	• Logsproduced by the SG system assets.

Pre-processed data	SPEAR collects the SG and Honeypot data (previously described) and performs some pre-processing mechanisms before data analytics takes place for detecting attacks.
Events	Events are asynchronous security incidents that involve a security violation of the SG system detected by the SPEAR platform; they can be detected whether by the OSSIM based components or by the SPEAR components by using advanced data analytics techniques.

Item	Description
Forensic evidences	SG data that has been handled with respect to applicable legal and regulatory requirements regarding networks forensics and privacy.
Reputation	Reputation is a metric to assess the trustworthiness of each SPEAR node in terms of its legitimate behaviour.

5.2 System decomposition model

The system decomposition model defines the different modules and components that compose the SPEAR platform and how they are related to each other.

Figure 5 shows a UML component diagram representation of the decomposition model of SPEAR. The model includes the logical components found both in the SPEAR platform related to a particular SG system (in blue in the figure). Notice that we have represented also external SG systems in a simple way (in grey in the figure) for the sake of readability of the model, but multiple SG operators can interact through the SPEAR-RI component. The relationships between the SPEAR platform components have been simplified too in order to preserve the readability of the figure. Section 5.3.2 gives more details of the relationships between the components. These logical components have been described in Table 4, where we relate each of the components to the Work Packages and deliverables identified in the Grant Agreement of SPEAR.

Table 4: Description of components and modules in the SPEAR platform

Component name	Description	Related WP and Deliverables	Related Subcomponents
SPEAR-SIEM	This component supports the detection of threats, anomalies and cyberattacks in SG environments. It enables the collection of information from several architectural levels of the SG 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 cyberattack incidents. It also provides a visual-aided dashboard where visualisations could significantly assist the security administrator to globally inspect the SG infrastructure in near real time. It integrates existing top open-source SIEM tool capabilities such as AlientVault's OSSIM's [18] together with innovative technologies based on advanced analytics, graphical-aided visualisation techniques and trust management mechanisms.	WP3 D3.1 D3.2 D3.3 D3.4	SPEAR SIEM Basis – Log Collector and Aggregator BDAC Visual-aided IDS (VIDS) GTM Message Bus

SPEAR FRF	This component ensures forensic readiness in the SG environment, in the sense that the applied network forensic strategies are deployed before a cyberattack incident takes place, thus ensuring that the network is forensically ready. SPEAR-FRF will make use of the OSCAR methodology for doing network forensics. OSCAR methodology presents some challenges related to a) the required means for gathering forensic evidence, b) how this evidence remains unforged by the attackers and c) how user privacy is ensured. For a) SPEAR-FRF will make use of grid-oriented honeypots and the OSSIM. For b) and c) SPEAR-FRF will make use of advanced encryption techniques to protect the forensic data in transit and at rest.	WP4 D4.1 D4.2 D4.3 D4.4 D4.5	AMI Honeypots Honeypot Manager Forensic Repository
Anonymous SPEAR-RI	This component provides anonymous inter-connection channels amongst SG operators with the purpose of exchanging information related to cybersecurity incidents but preserving the anonymity of the source. The SPEAR SIEM provides with the events information to the Anonymous SPEAR-RI.	WP5 D5.1	

Please, notice that the SPEAR Platform also includes two procedural frameworks:

1. Privacy-preserving Framework part of the SPEAR FRF that supports the Privacy Impact Assessment (PIA) process that evaluates how collected data by the SPEAR SIEM is handled with respect to applicable legal and regulatory requirements regarding privacy.
2. CHF: It provides protection protocols, policies and rules in identifying and addressing relevant risks before they are triggered. The framework will enclose a list of potential cyber threats in terms of confidentiality, integrity and data availability. For each cyberthreat, a training material will be prepared for both industry personnel and energy consumers.

The detailed description of all SPEAR components follows in the next subsections.

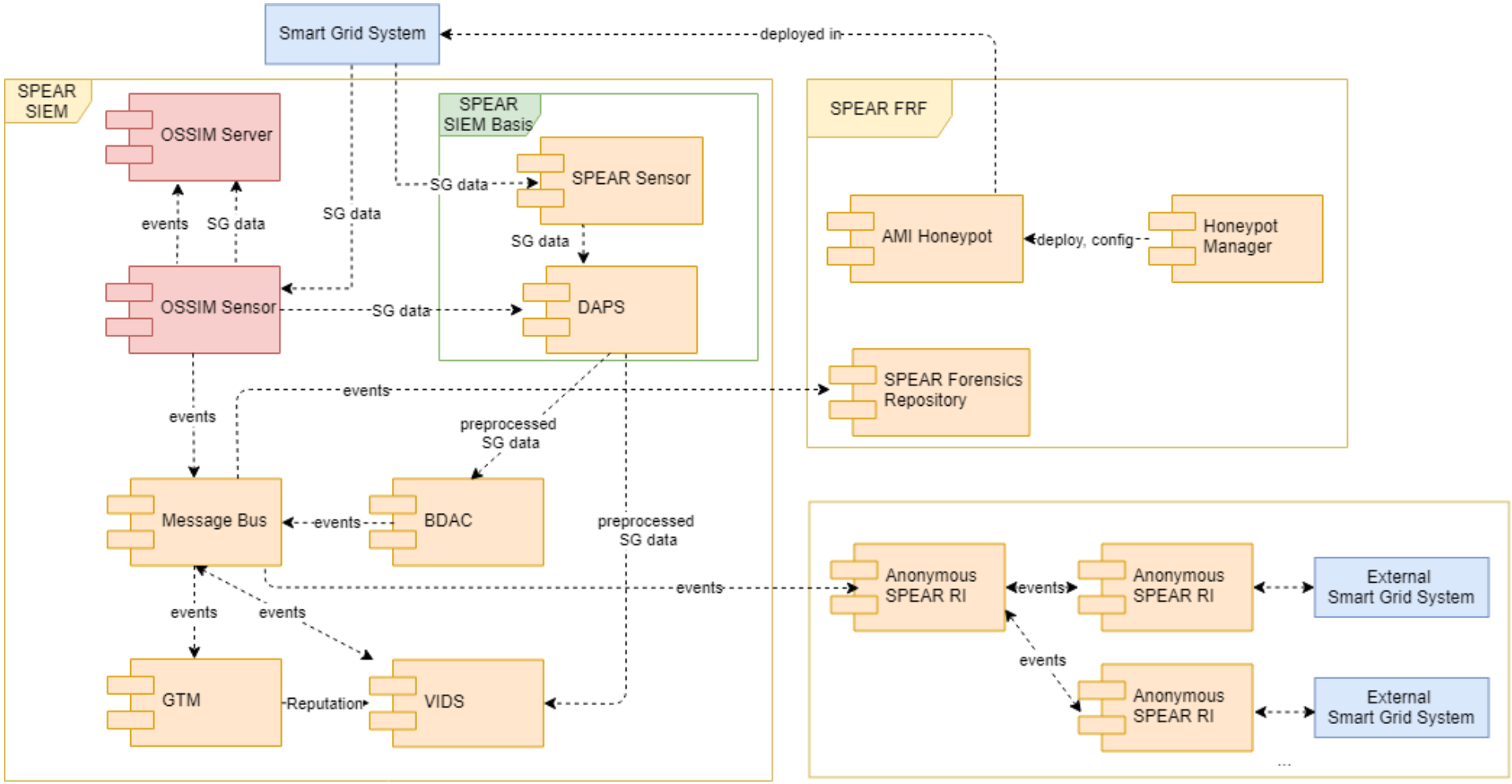


Figure 5: SPEAR Platform Architecture

5.2.1 SPEAR SIEM Basis

5.2.1.1 Main functionalities

This component is part of the SPEAR SIEM tool that allows the collection of SG data, from industrial communication protocols data (e.g., IEC61850 or IEC 60870-5-104) as well as TCP/IP network traffic data to logs of the devices part of the SG system.

It prepares the collected data by using parsing and/or aggregating mechanisms in order to be ready for the usage of the rest of the components of the SPEAR SIEM. It is responsible for handling a large quantity of data from multiple data sources in the SG.

It also integrates some of the most important SIEM capabilities provided by an open-source tool such as AlientVault's OSSIM. OSSIM already includes security capabilities for IT systems: a signature-based NIDS, a Host Intrusion Detection System (HIDS), and an event correlation engine and directives that can be included into the SPEAR SIEM.

5.2.1.2 Internal components

The SPEAR SIEM Basis is composed by two different parts as shown in Figure 6:

1. Distributed agents, called Network Capturer and Parser (NCP) components, which are responsible for collecting and parsing the required data of the SG systems to be monitored. It is required that one NCP component instance to be deployed in the network to be monitored, the same way the OSSIM sensors are deployed in each of the networks to be monitored.

2. All collected SG data by the NCP instances is sent to a centralized component called Data Acquisition, Parsing and Storage (DAPS) component. This component is responsible for acquiring, parsing and storingall data sent by NCP instances; afterwards it distributes the pre-processed data to the other components of the SPEAR SIEM to proceed with the corresponding data analytics to detect anomalies. In the prediction phase, the data is sent in streaming to the BDAC and Visual IDS components to apply data analytics models and detect potential attacks; whereas in training phase, datasets can be recovered from the Storage infrastructure sub-component.

Figure 7 shows a detailed architecture of the NCP component. This component mainly collects and parses two types of data:

1. Industrial communication protocols' traffic data (e.g. IEC61850 or IEC 60870-5-104).
2. Network flow data to generate statistical features.

Once all data is collected and parsed, i.e. is ready to be sent to DAPS, the shipper type sub-components are in charge to send this data. Moreover, the NCP includes another shipper subcomponent responsible for sendingthe required data for forensics backup to the SPEAR Forensic Repository.

The SPEAR SIEM Basis also collects operational data from the SG system to be monitored. A connector will be deployed between the database of the SG system and the Data Capturing and Parser (DCP) sub-component for that purpose.

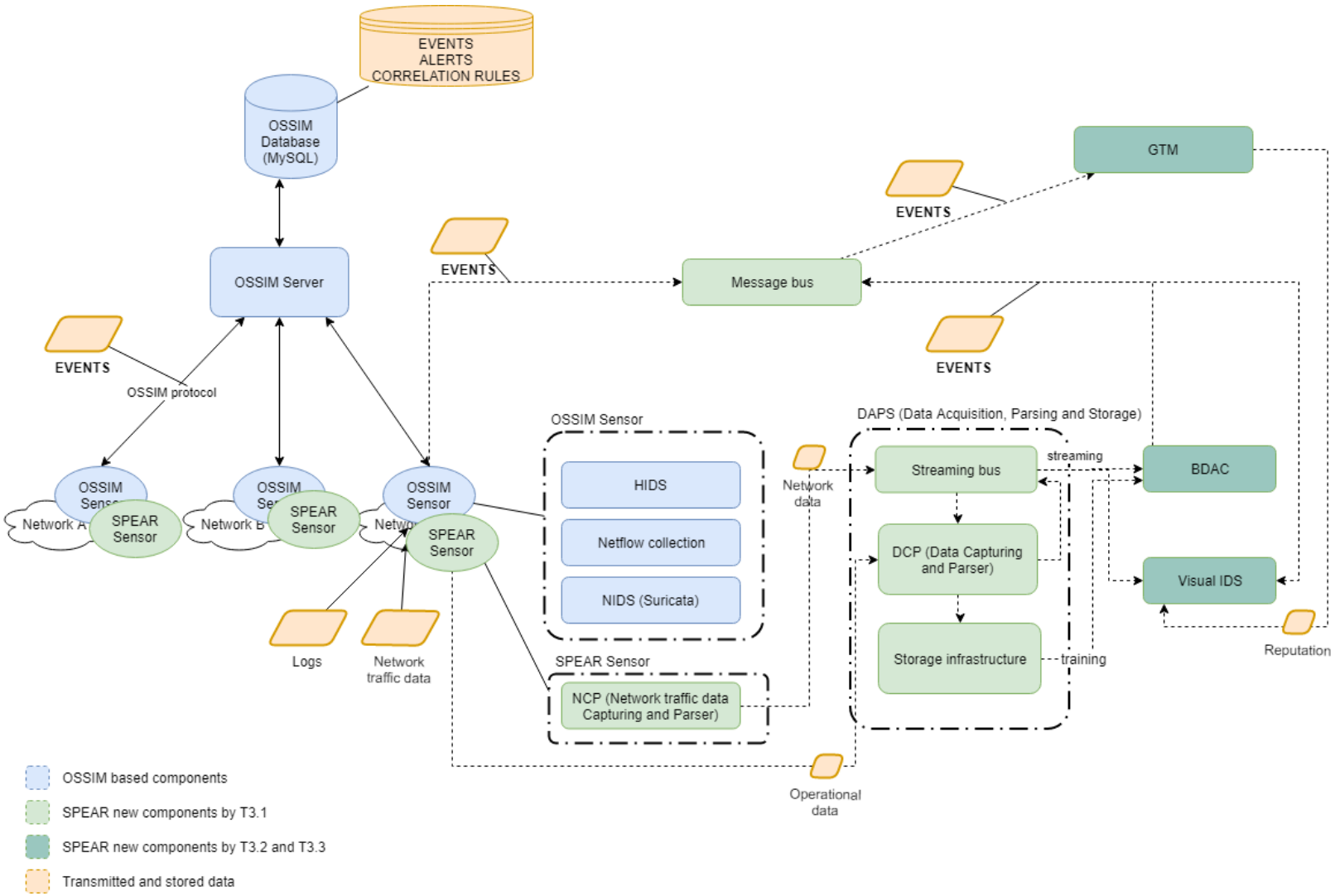


Figure 6: SPEAR SIEM Basis architecture

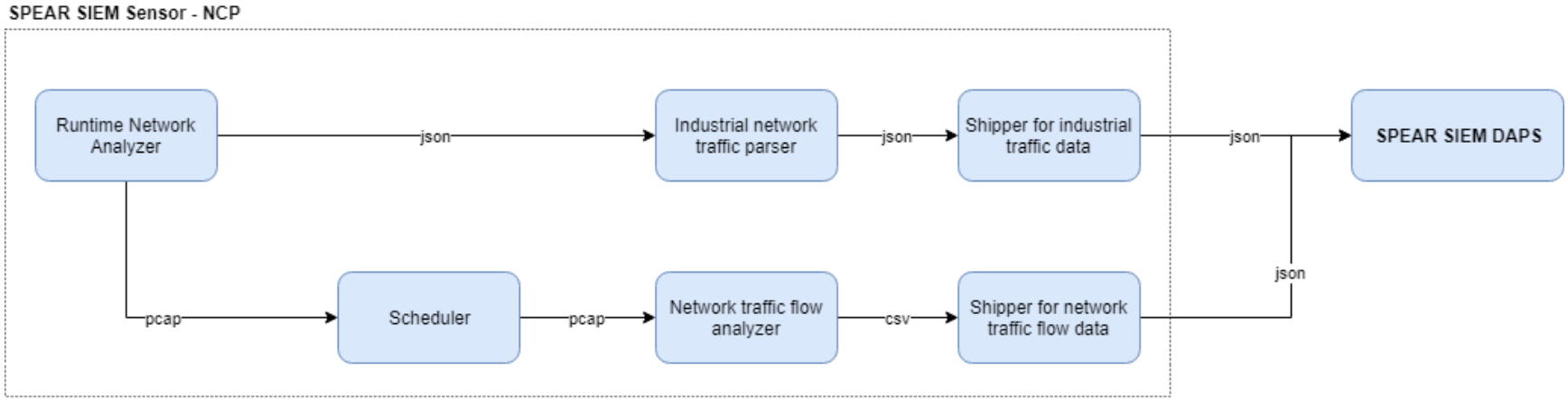


Figure 7: NCP component internal architecture

5.2.1.3 Technical Specifications

The SPEAR SIEM Basis is delivered as a Docker based deployment. Docker needs to be installed in all machines used for deploying the Monitoring Enabler components; Docker installation is well explained in the documentation of Docker[2].

As explained before, the SPEAR SIEM Basis is composed by distributed agents called NCP and a centralized server-side component called DAPS. Next, the base technologies used for these components are listed:

- Technologies used by NCP component:
  - Runtime network analyser T-shark[3]
  - Network traffic flow analyser Cicflowmeter[4]
  - Elastic Filebeat[5]
- Technologies used by DAPS component:
  - Apache Kafka[6]
  - Elastic Logstsh[7]
  - Elasticsearch[8]

Instances of the NCP component need to be deployed in each of the networks to be monitored in the SG system. In order to monitor the network traffic that is not being sent to or from the monitoring machine, the network interface of the machine needs to be enabled as promiscuous mode, and on a switched Ethernet network, it also needs to be set up the use of port mirroring.

DAPS needs to be deployed in a machine that at least fulfils the following hardware requirements of the base technologies:

- Streaming bus based on Kafka: HW requirements can be found in https://kafka.apache.org/documentation/#hwandos
- Data storage based on Elasticsearch: HW requirements can be found in https://www.elastic.co/guide/en/elasticsearch/guide/current/hardware.html

Besides the technical specifications for the SPEAR SIEM Basis components, the specifications for AlientVault's OSSIM need to be considered, which can be found in https://www.alienvault.com/documentation/usm-appliance/initial-setup/ossim-installation.htm.

[2] About Docker CE installation documentation, https://docs.docker.com/install/

[3] https://www.wireshark.org/docs/man-pages/tshark.html

[4] http://netflowmeter.ca/netflowmeter.html

[5] https://www.elastic.co/products/beats/filebeat

[6] https://kafka.apache.org/

[7] https://www.elastic.co/products/logstash

[8] https://www.elastic.co/products/elasticsearch

5.2.1.4 Dependencies to other components

The following table depicts and describes the interactions of SPEAR SIEM Basis (Component 1) with the other SPEAR components and subcomponents (Component 2).

Component 1	Component 2	Dependence Description
SPEAR SIEM Basis	BDAC	SPEAR SIEM Basis will provide the required parse SG data to BDAC, so BDAC can perform data analytics to detect incidents and anomalies in the SG system. The required data will be provided in two forms: (1) in streaming for prediction phase and (2) in the form of datasets for the training phase.
SPEAR SIEM Basis	Visual IDS	SPEAR SIEM Basis will provide the required parse SG data to Visual IDS, so Visual IDS can perform data analytics to detect incidents and anomalies in the SG system.

5.2.1.5 Addressed Requirements

Table 5 depicts and describes the system requirements satisfied by SIEM Basis.

Table 5: System requirements addressed by SIEM Basis

Requirement ID	Requirement Name
F01	Assets Protection
F03	Data Transmission
F04	Data Collection
F05	Data Analysis
F07	Alerts Categorization
F08	Encrypted communication
F09	Data Preprocessing
F28	VIDS Visual Analytics interconnection with SIEM Basis
F37	Sensors and Honeypots Deployment
NF01	Optionality
NF02	Scalability
NF04	Password Encryption
NF05	Data Encryption
NF08	Bandwidth

5.2.2 BDAC

5.2.2.1 Main Functionalities

BDAC is part of the SPEAR SIEM and performs machine learning and deep learning models in order to detect possible cyberattacks and anomalies that are identified as security events. In particular, BDAC constitutes an anomaly-based IDS which perfectly complements the signature-based HIDS (OSSEC) and NIDS (Suricata) of OSSIM. BDAC can detect cyberattacks and anomalies by analysing TCP/IP network flows, data from the application layer (OSI level 7) used by the SPEAR end-users, such as Modbus, DNP3,

MMS, IEC 60870-5-104, etc., as well as operational data (e.g., electricity measurements such as current and voltage). Moreover, it is noteworthy that BDAC can handle and process efficiently huge volumes of data coming from multiple sources and it will be able to detect cyberthreats, using the network traffic information provided by the SPEAR honeypots.

5.2.2.2 Internal Components

Figure 8 illustrates the internal architecture of BDAC. In particular, BDAC consists of 5 modules, namely: a) the Data Receiving Module, b) the Data Preprocessing Module, c) the Training Module, d) the Analysis Engine Module and e) the Security Event Extraction Module. The first one is responsible for receiving data from the SPEAR SIEM Basis DAPS. Specifically, it receives data related to a) TCP/IP network flows, b) application layer protocols (OSI L7, e.g., Modbus, DNP3, MMS, IEC-104, etc.), c) operational data (e.g., voltage and current values) as well as d) honeypots network traffic. The second module undertakes to pre-process this data, thus forming appropriate datasets that are used by the Training Module, which also applies machine learning and deep learning algorithms in order to provide efficient anomaly detection models. Based on the data received, the appropriate datasets are formed and the corresponding anomaly detection models are generated by the Training Module. Therefore, four categories of anomaly detection models are defined: a) TCP/IP Network Flow-Based Anomaly Detection Models, b) Application Layer-Based Anomaly Detection Models, c) Operational Data-Based Anomaly Detection Models and e) Honeypot-Based Anomaly Detection Models. It is worth mentioning that the Training Module periodically generates new anomaly detection models that replace the previous ones whether their detection performance is considered better in terms of the metrics defined in D2.3. All the aforementioned models form the Analysis Engine Module, which receives the preprocessed data form the Data Preprocessing Module and performs the anomaly detection process in near real-time, generating the appropriate security events. Finally, the Security Event Extraction Module receives the security events and forward them to the Message Bus component.

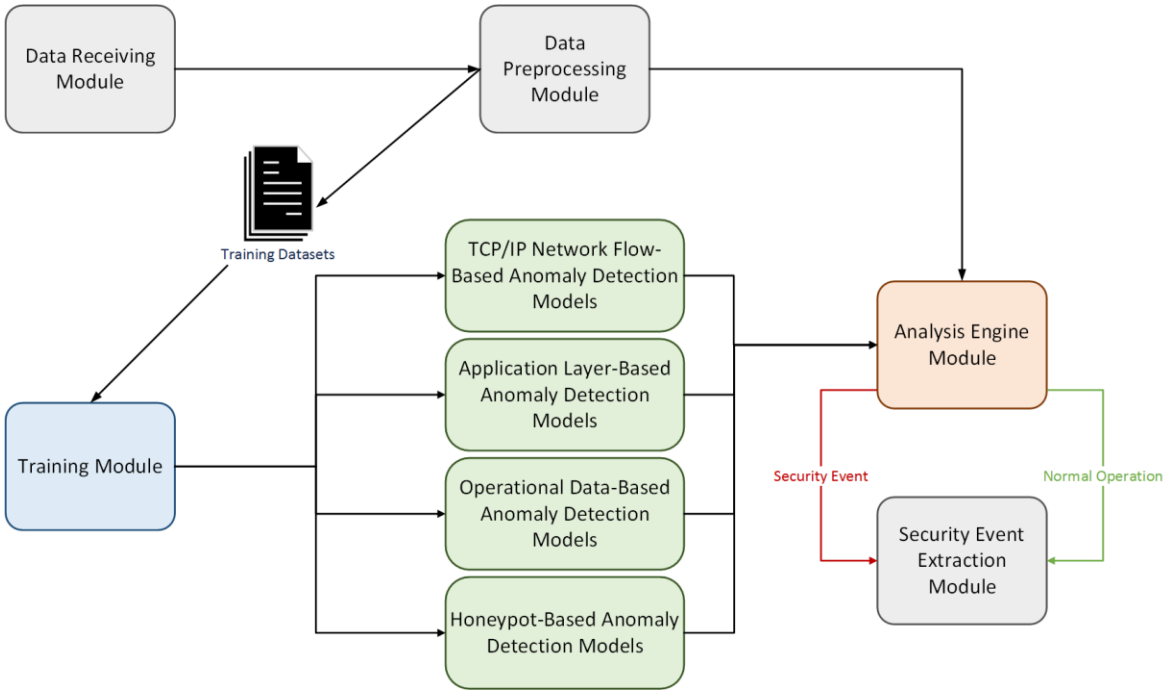


Figure 8: BDAC Internal Components.

5.2.2.3 Technical Specifications

BDAC will utilise python-based machine learning libraries, such as Numpy, Pandas, Scikit-learn, Tensorflow, Caffe, Keras, PyOD and PyTorch in order to construct effective intrusion and anomaly detection models. In particular, BDAC will apply the previous libraries in order to examine and form both supervised and unsupervised learning models that will be trained with network traffic and operational data provided by the SPEAR end-users as well as public reliable intrusion detection datasets, such as CICIDS 2017, UNSW-NB15. Moreover, the operations provided by Apache Spark will be adopted in order to handle efficiently huge volumes of data. Specifically, the PySpark interface will be used. Table 6 summarises the technologies that will be used by BDAC.

Table 6: Technologies of BDAC

Component Name	Possible Technologies
Data Receiving Module	Python 3.7,
Data Preprocessing Module	Python 3.7, Numpy, Pandas, Pyspark, Python Elasticsearch API (based on the SPEAR SIEM DAPS implementation)
Training Module	Python 3.7, Numpy, Pandas, Pyspark, Scikit-learn, Tensorflow, Caffe, Keras, PyOD, PyTorch, pickle
Analysis Engine Module	Python 3.7, Numpy, Pandas, Pyspark, Scikit-learn, Tensorflow, Caffe, Keras, PyOD, PyTorch, pickle
Security Event Extraction Module	Python 3.7, Apache Kafka Python API (based on the Message Bus implementation)

5.2.2.4 Dependencies to other components

Table 7 depicts and describes the dependencies of BDAC with the other SPEAR components. In particular, BDAC communicates with the SPEAR SIEM Basis DAPS in order to obtain SG data and based on them to identify possible security events. In addition, BDAC communicates with the Message Bus component in which the security events are pushed.

Table 7: BDAC Dependencies with the other SPEAR components

Component	Dependence Description	Possible Technologies
SPEAR SIEM Basis DAPS	BDAC will take from SPEAR SIEM Basis DAPS preprocessed smart grid data such as network traffic and operational data in order to detect possible security events.	Elasticsearch Python API
Message Bus	BDAC will send to Message Bus the various security events generated.	Apache Kafka Python API

5.2.2.5 Addressed Requirements

The following table depicts and describes the system requirements satisfied by BDAC.

Table 8: System requirements addressed by BDAC

Requirement ID	Requirement Name
F01	Assets Protection
F05	Data Analysis
F07	Alerts Categorization
F08	Encrypted communication
F09	Data Preprocessing
F10	Interconnectivity
F11	Operation
F12	BDAC interconnection with Message Bus
F13	Multi-Layer Intrusion/Anomaly Detection
F14	Operational data-based Anomaly Detection
F15	BDAC re-training
F16	Honeypot-based Anomaly Detection
F17	Intrusion Detection
F18	DoS Protection
NF01	Optionality
NF03	Data Volume
NF04	Password Encryption
NF05	Data Encryption
NF08	Bandwidth

5.2.3 VIDS

5.2.3.1 Main Functionalities

VIDS offers a visual display of the potential threats offering an intuitive approach to the administrator, as she/he is capable to instantly detect anomalies in the incoming threats through the offered visualization. The visual-aided IDS receives as input the pre-processed smart grid data and based on the features of the incoming traffic pre-defined schemes indicating specific threats are visualized. The visual results of the component will be reflected on both web-based and mobile-based applications, in order for the administrator to react as soon as possible.

Based on the end-user and stakeholder requirements (D2.4) and the role identification process that have been followed, three groups of SPEAR VIDS roles were identified. All the VIDS functionalities will be tailored upon the three user roles since each role will support different dashboard views, functionalities and accessibilities. Table 9 depicts the identified SPEAR VIDS user roles.

Table 9: Identified SPEAR VIDS user roles

VIDS user role	Description	End-User suggested roles (D2.4)	Pilot
SPEAR Security Engineer	This role has access to all VIDS dashboard features, functionalities and internal components. Based on the role hierarchy, the users have access to advanced information mechanisms (visual analytics, visualization diagrams and widgets).	SPEAR Security Engineer	Hydro plant scenario
		Substation Security Administrator	Substation scenario
		SPEAR Security Engineer	Combined IAN and HAN scenario
		Facility Manager	Smart-home scenario
SPEAR Facility Operator	This role targets users with technical knowledge (engineers, technicians, operators, etc.) but with no cybersecurity background. In this manner, they have access to broad but specific features. They have an advisory role regarding the SPEAR platform operation.	Hydro Power Plant operator	Hydro plant scenario
		Substation end-user Engineer	Substation scenario
		IAN Operator	Combined IAN and HAN scenario
SPEAR Non-Technical End-User	This role targets users with no technical background. The users are provided with the SPEAR security services but have limited to the SPEAR system (overview of the cybersecurity status).	HAN user	Combined IAN and HAN scenario
		Smart-home End-user	Smart-home scenario

5.2.3.2 Internal Components

Figure 9 depicts the VIDS architecture. VIDS consists of ten internal components. The following subsection provides details regarding the functionalities of these components.

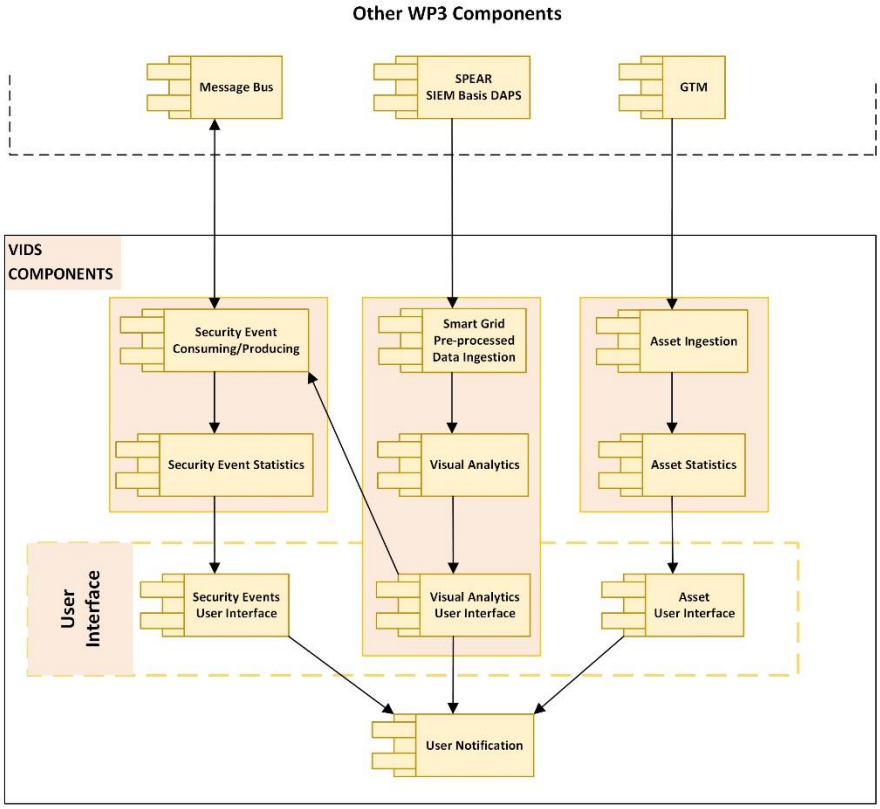


Figure 9: VIDS Internal Components.

5.2.3.2.1 User Interface component

This component is responsible for orchestrating the several User Interface components. Figure 10 depicts the User Interface component software modules:

- User Authentication/Authorization: This software module authenticates the VIDS users based on their profile credentials. It also authorizes them based on their role. Based on their role, different dashboard views are presented to each user.
- Security Events Visualization Widgets: This software module presents to the user all the security events fetched from the Message Bus. User-friendly visualizations assist the user in order to easily estimate the networks' status.
- Visual Analytics Visualization Widgets: This software module presents the visual analytics results. These results are presented via several visualization diagrams and methods.
- Network Asset Visualization Widgets: This module is responsible for demonstrating the asset list transferred from the GTM component. It supports several visualization widgets (tables, bar charts, etc.) in order to offer a detailed overview of the network assets.

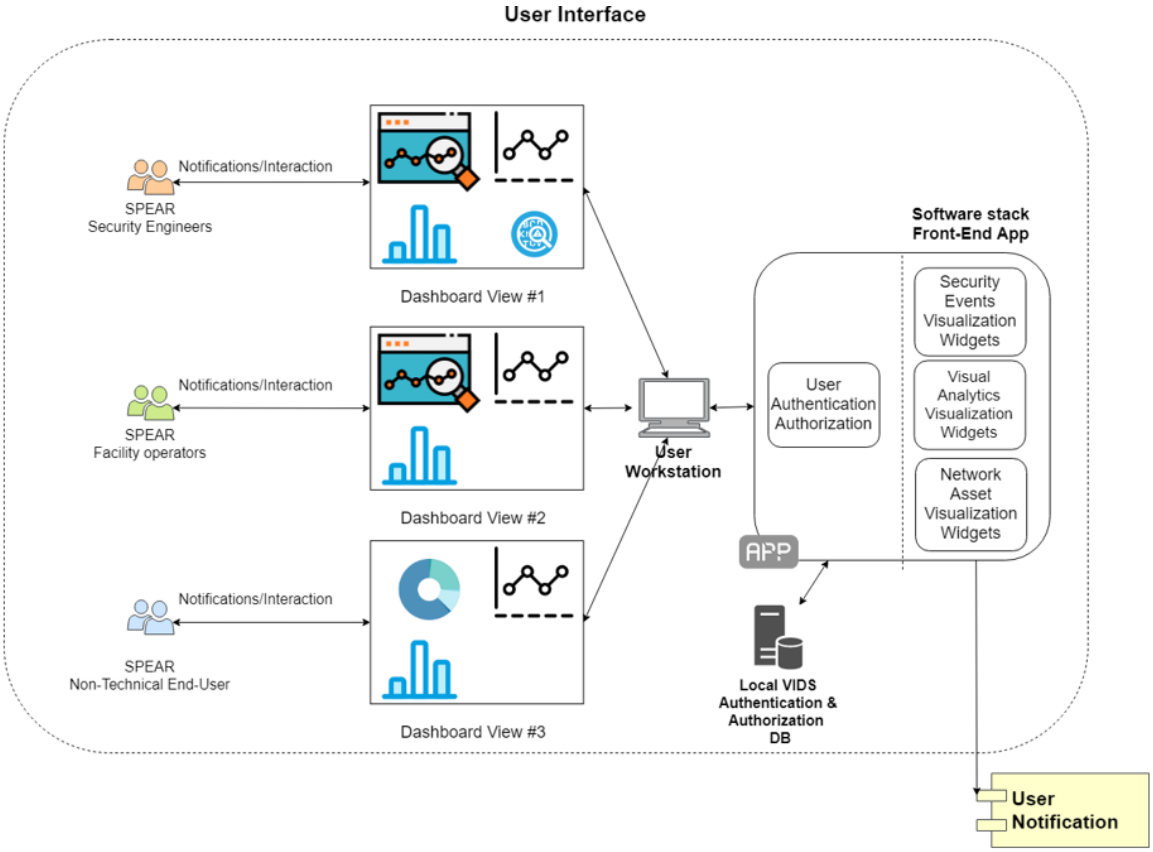


Figure 10: Schematic of the User Interface component.

5.2.3.2.2 Security Event Consuming/Producing, Security Event Statistics & Security Events User Interface components

VIDS consists of the user dashboard where the user can be informed about the security events that are generated from the Message Bus. These security events are mostly generated by the OSSIM Server, the OSSIM Sensor, the BDAC but also the VIDS. Due to the fact that Visual Analysis is considered an intuitional based functionality, none of the Visual Analytics mechanisms will automatically generate security events. However, the VIDS allows the user to create and push security events into the message bus.

Figure 11 presents a diagram of the Security Event Consuming/Producing component, Security Event Statistics & Security Events User Interface modules functionalities.

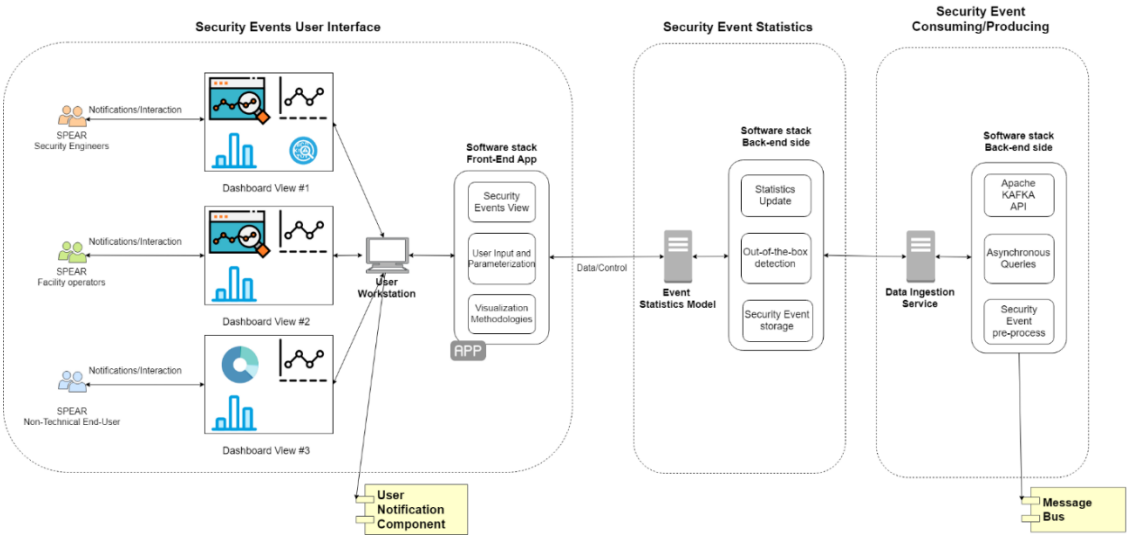


Figure 11: Schematic of the Security Events User Interface, Security Event Statistics and Security Event components.

The Security Event Consuming/Producing component is responsible for establishingthe connection between the Message Bus and the VIDS in order to consume and produces Security Events. More specifically, this component is divided into the software modules:

- Apache KAFKA API: This moduleestablishes the communication with the Message Bus component in order to transfer security events from one component to the other. The Message Bus is based on the Apache KAFKA so this module has a dependency on this tool.
- Asynchronous Queries: Since the Security Events might be generated at non periodical time, this module is responsible for detecting whether or not there are new security events in the Message Bus that is not yet consumed by the VIDS.
- Security Event pre-process: This module pre-processes the security events in a format that makes them ready to be used by the next components. Homogenization procedures must precede since Security Events are produced from three different components (OSSIM Sensor, OSSIM Server, BDAC and the VIDS).

The Security Event Statistics component is responsible for updatingthe Security Events statistics and save the security events in the local database. This component consists of three software modules:

- Statistics Update: This module updates the Security Events statistics models based on the data coming from the previous component.
- Out-of-the-box detection: This software module handles the statistic models for Security Event categories that are initial detected. The module will assign a unique identification key to the security event category and initiate its statistics variables.
- Security Event storage: This module will store the new Security Event in the local VIDS database. Moreover, it supports all the necessary functions regarding the Security Event object restoration, deletion etc.

The Security Events User Interface component is responsible to presents the security events and their statistics to the end user. This component is divided into three software modules, more specifically,

- Security Events View: The module presents the security events and their statistical models to the user interface. Different visualization widgets, diagrams and charts are provided to the VIDS user.
- User input and Parameterization: This software module handles the inputs of the users and the parameterization of the visualization widgets.
- Visualization Methodologies: This software module contains all the front-end visualization methods available in for the Security Events statistics models. The user selects the security event for the models and selects the methodology to dynamically create the visualization widgets.

5.2.3.2.3 Smart grid pre-processed Data Ingestion, Visual Analytics & Visual Analytics User Interface components

Figure 12 presents a diagram of the Smart grid pre-processed Data Ingestion, Visual Analytics & Visual Analytics User Interface components. The Visual Analytics User Interface component will create different dashboard views for each user role (Table 9). More specifically:

- SPEAR Security Engineer: The dashboard view is a user-friendly UI with technical details and parameters. More specifically, the user can access all the available visualization methods and data/visual analytics methods. The user can tune and adjust the parameters of the data/visual analytics algorithms in order to evaluate and investigate cyberattack incidents and anomalies.
- SPEAR Facility operator: The user has access to broad but specific features of the Visual Analytics component. The dashboard view is a user-friendly UI with technical details. In this context, the user can access all the available visualization methods but has limited access to tune the data/visual analytics methods.
- SPEAR Non-Technical End-User: The Visual Analytics dashboard presents to these users an overview of the cybersecurity status of the SPEAR installation.

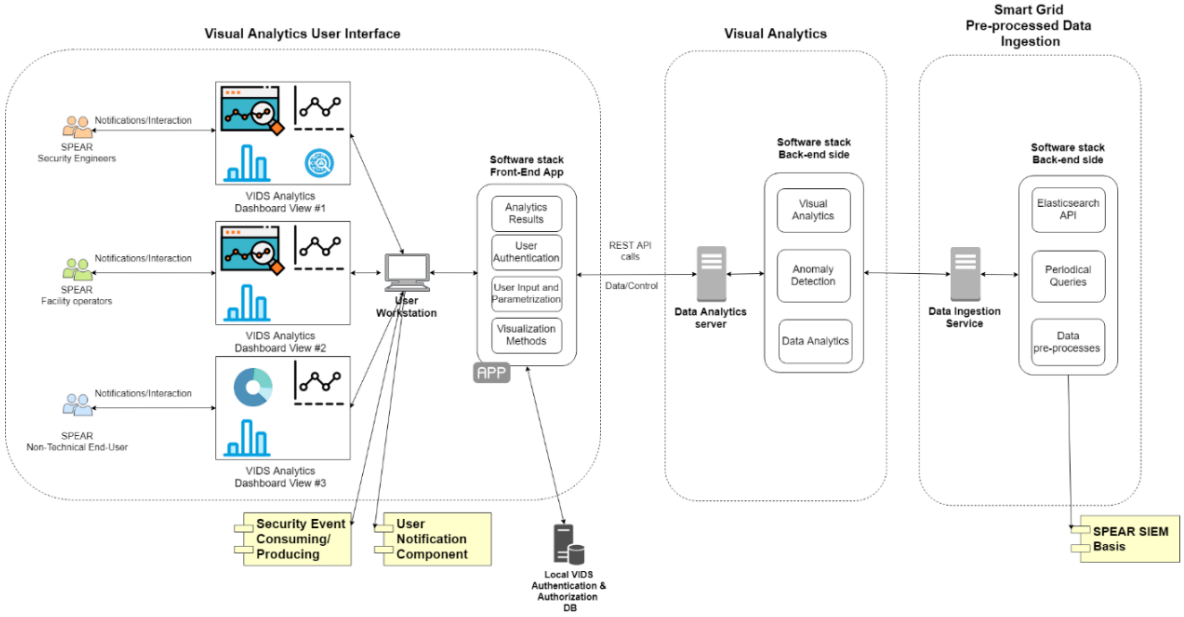


Figure 12: Schematic of the Visual Analytics User Interface, Visual Analytics and Pre-processed Data Ingestion components.

The Visual Analytics User Interface component is a front-end web application with escalated privileges for each user role. The software stack of the front-end application is divided into the software modules:

- Analytics Results: The source of the input data for this software module comes from results from the visual/data analytics algorithms.
- User Authentication: The users need to authenticate in order to acquire access to the Visual Analytics dashboard view. Each user belongs to a user role or user group with different privileges and dashboard views. The authentication and authorization database is part of the User Interface component (section 5.4.2.4.2.1).
- User input and Parametrization: This software module handles the inputs of the users and the parametrization of the Visual Analytics component.
- Visualization Methods: This software module contains all the front-end visualization methods available in the Visual Analytics component. The visualizations methods could apply in raw data or in the results of the data/visual analytics algorithms.

The front-end application runs on the user workstation and communicates with the back-end servers mainly with REST-API calls. The Visual Analytics back-end server hosts a software stack, which has implemented all the visual/data analytics methods. The software modules are:

- Visual Analytics: This software module contains visual analytics methods. More specifically, it provides algorithms that consume the raw data and provide visualization results such as graphs.
- Anomaly Detection: This module contains anomaly detection algorithms that support the visual/data analytics methodologies, especially for time-series analysis.
- Data Analytics: This software module contains data analytics methods. It differentiates with the *Visual Analytics* module because this module consumes raw data and produces processed data. The outcome of these methods are data that need the Visual Analytics User Interface module in order to be presented to the user.

The last component in this group is the Smart Grid Pre-processed Data Ingestion component. This component is divided into three software modules,

- Elasticsearch API: This module establishes the communication with the SPEAR SIEM Basis DAPS component in order to fetch the data. The SPEAR SIEM Basis DAPS is based on the Elasticsearch so this module has a dependency on this tool.
- Periodical Queries: This task will be periodically fetching the pre-processed smart grid data after a pre-defined amount of time (determined by the user).
- Data pre-process: This module pre-processes the data in a format that makes them ready to be used by the analytics algorithms. The pre-processing techniques are imposed from the input data format for each data/visual analytics method.

5.2.3.2.4 Asset Ingestion, Asset Statistics & Asset User Interface components

VIDS consists of the user dashboard where the user can be informed about the network assets and their reputations. This information is generated by the GTM component and are transferred to the VIDS dashboard.

Figure 13 presents a diagram of Asset Ingestion, Asset Statistics & Asset User Interface components modules functionalities.

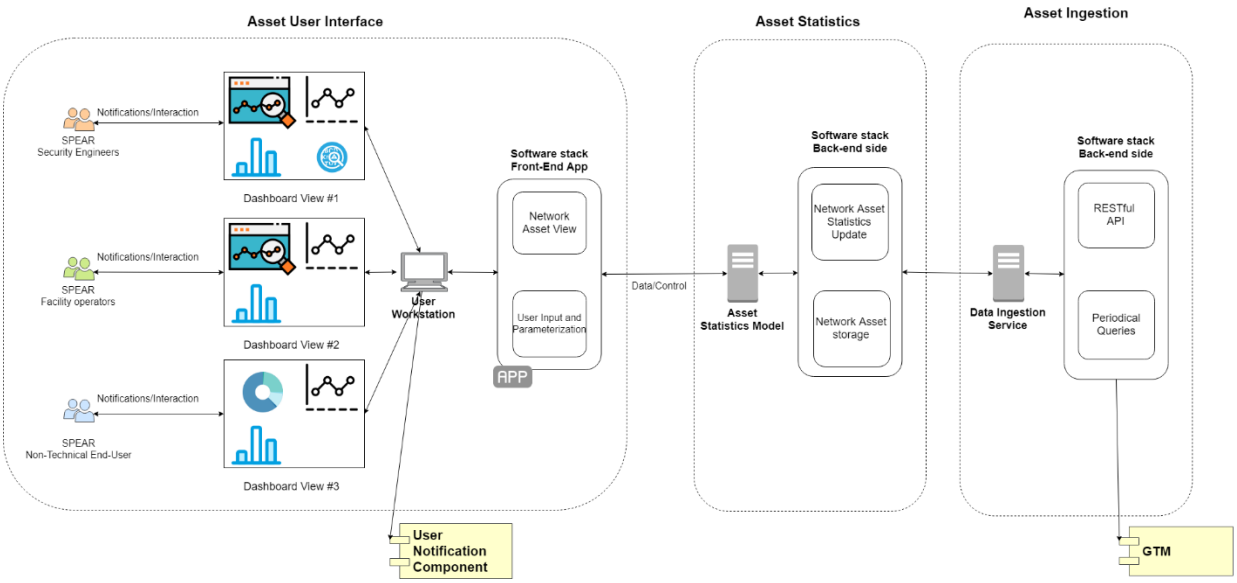


Figure 13: Schematic of the Asset Ingestion, Asset Statistics & Asset User Interface components

The Asset Ingestion component is responsible for establishingthe connection between the GTM and the VIDS in order to transfer the information regarding the network assets. This component is divided into two software modules, more specifically,

- RESTful API: This module establishes the communication with the Message Bus component in order to transfer security events from one component to the other. The Message Bus is based on the Apache KAFKA, so this module has a dependency on this tool.
- Periodical Queries: The VIDS should fetch the GTM data in a predefined time period. The Periodical Queries software module is responsible for this functionality.

The Asset Statistics component is responsible for updatingthe Network Assets statistic models and save the updated information in the local database. This component consists of two software modules:

- Network Asset Statistics Update: This module updates the Network Assets statistics models based on the data coming from the GTM.
- Network Asset storage: This module will store the fetched information in the local VIDS database. Moreover, it supports all the necessary functions regarding the Network Asset object restoration, deletion etc.

The Asset User Interface component is responsible to presents the network assets and their statistics to the VIDS user. This component is divided into two software modules. More specifically:

- Network Asset View: The module presents the network assets and their statistical models to the user interface. Different diagrams, types of charts and visualization widgets, are provided based on the user role.
- User input and Parameterization: This software module handles the inputs of the users and the parameterization of the visualization widgets.

5.2.3.2.5 User Notification module

The User Notification module is responsible for notifyingthe user regarding changes in networks' status. The user via the VIDS dashboard can parameterize the system in order to get notifications regarding several security incidents (e.g. new Security Events, new data for Visual Analysis, reputation updates in the Network Asset List etc.). Thereby, the user either via her/his email or the smartphone will be always informed regarding the network status.

5.2.3.3 Technical Specifications

The user will interact with the VIDS via a lightweight UI based on advanced UX principles and methodologies, while all the back-end functionalities will be optimised in order to leverage systems' resources. Table 10 presents all the VIDS proposed technologies and algorithms.

Table 10: Proposed technologies for VIDS components.

Component Name	**Possible Technologies**	
User Interface	Front-End	Bootstrap 4.3.1, JQuery 3.3.1, Datatables 1.10.19, Highcharts JS v7.1.2, Font awesome v5.8.1
	Back-End	Python Django Web Framework 2.2, Python 3.5, Gunicorn, Numpy, Pandas, Celery, Redis, PostgresSQL
Security Event Consuming/Producing	Back-End	Pyhton 3.5, Apache Kafka Python API
Smart Grid Pre-processed Data Ingestion	Back-End	Python 3.5, Python Elasticsearch API
Visual Analytics	Back-End	Python, C++, Node.js, express, Elasticsearch-Python-client, Keras, Tenserflow, Sklearn, etc
	Visual/Data Analytics algorithms	CUSUM, LSTM NN, LSTM Seq2Seq, Multi-objective graphs, k-partite graph, Histograms, Pie chart, dimensionality reduction methods, SVD, ICA, ISOMAP, etc.
Visual Analytics User Interface	Front-End	Vega-Lite, Vega, D3, Chart.js, AngularJS, etc
Asset Ingestion	Back-End	RESTful API

5.2.3.4 Dependencies to other components

Within the VIDS, there are several external connections with other SPEAR components. Table 11 presents the VIDS dependencies with other SPEAR components and subcomponents.

Table 11: External connection between the VIDS and other SPEAR components.

VIDS Component	SPEAR Component	Dependence Description	Possible Technologies
Smart Grid Pre-processed Data Ingestion	SPEAR SIEM Basis DAPS	VIDS will get preprocessed smart grid data (network traffic, operational data) from SPEAR SIEM Basis DAPS in order to conduct the visual analytics	Elasticsearch
Security Event Consuming/Producing	Message Bus	VIDS will produce and consume security alerts from and to the Message Bus	Apache Kafka
Asset Ingestion	GTM	VIDS will interact with the GTM in order to fetch all the available network assets and their reputations	RESTful API

5.2.3.5 Addressed Requirements

The following table depicts and describes the system requirements satisfied by the VIDS.

Table 12: System requirements addressed by VIDS

Requirement ID	Requirement Name
F01	Assets Protection
F02	Cyberthreats Visualization
F04	Data Collection
F05	Data Analysis
F07	Alerts Categorization
F08	Encrypted communication
F17	Intrusion Detection
F18	DoS Protection
F19	VIDS Authentication
F20	Remote Notifications
F21	VIDS user roles
F22	VIDS user role dashboard views
F23	VIDS users authentication DB
F24	VIDS Analytics vendor agnostic application
F25	VIDS Analytics user parametrization
F26	VIDS Analytics visualization methods
F27	VIDS Analytics response time
F28	VIDS Visual Analytics interconnection with SIEM Basis
F29	VIDS interconnection with Message Bus
F30	VIDS Analytics data visualization algorithms
F31	VIDS Analytics anomaly detection mechanism
F32	VIDS Analytics processing limitations
F33	VIDS Visual Analytics interconnection with GTM
NF01	Optionality
NF04	Password Encryption
NF05	Data Encryption
NF08	Bandwidth

5.2.4 GTM

5.2.4.1 Main Functionalities

This component is part of the SPEAR SIEM aiming at enabling node-centric reputation computations algorithms in order to improve the detection of internal security threats and incidents, such as accidental mistakes, hardware failures and malicious actions from inside. It will analyse the security events generated by OSSIM Sensor, OSSIM Server, BDAC and VIDS to provide the mentioned results.

The GTM component implements algorithms to compute the changes to nodes' reputation based on these security events. The values of these changes depend on the criticality of the different security events evaluated by GTM itself with the knowledge coming from the OSSIM risk assessment model. The reputation of each node, along with other essential information is presented by VDS to support awareness of the SPEAR sysadmins.

GTM will raise three different types of alerts to the administrator with the goal to optimize the time the former spends on investigating potential incidents.

- **Alert Type A**: GTM will alert the SPEAR sysadmins whenever a node's reputation decreases below a predefined threshold computed based on the node's value as given by SPEAR SIEM Basis or OSSIM.
- **Alert Type B**: GTM will alert the SPEAR sysadmins whenever the "speed" (i.e., the rate) of a node's reputation change increases above a predefined threshold.
- **Alert Type C**: GTM will alert the SPEAR sysadmins whenever the total number of nodes that have generated Alerts of type A and B has exceeded a predefined threshold (5% as KPI in D2.3).

5.2.4.2 Internal Components

The main component of GTM is the Reputation Calculation Component (RCC). It is a rule-based system which accepts "facts" (i.e., security events from BDAC and VIDS as well as information about the current state of the nodes) and calculates the new reputation of the nodes. Its decisions are based on the pre-defined rules, which tells the rule engine how much to decrease the reputation of misbehaving nodes or increase the reputation of the nodes, which are not involved in the security events. Input Handler Layer converts the security events into facts, suitable for RCC, while Output Former converts the results of RCC work into the proper output format. GTM also has an inner database (GTM db) where it stores information about nodes in the system and their reputation, including current and historical data. Figure 14 illustrates the GTM internal components.

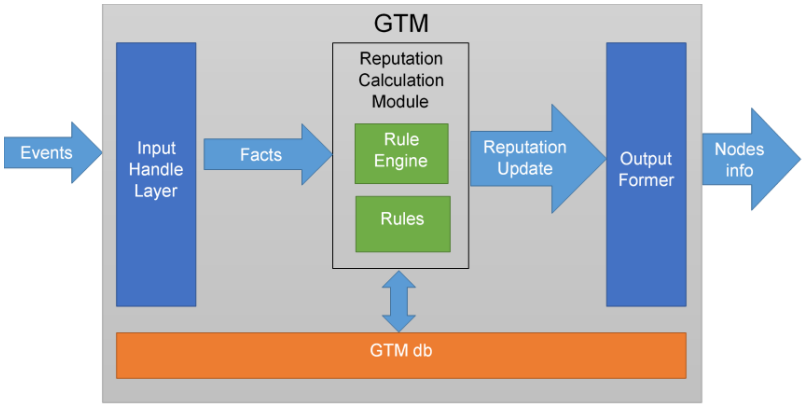


Figure 14: GTM Internal components.

5.2.4.3 Technical Specifications

GTM will be written in Python 3.7. This will allow to achieve high performance and will give an access to many open-source libraries, like rule engines, which will save time of development. Python is a cross-platform language which will allow to build a system working under different operation systems, which satisfies the requirement NF01("The SPEAR platform should be able to operate under as many OSes as possibly"). GTM will use MySQL to manage its inner database. It is one of the most powerful and popular management systems for relational databases which provides high performance for data operations. The rule engine used by GTM will be open source library for python called "Durable Rules" (ver. 2.0.5). It has simple syntax and allows to build complex rule-based systems. Table 13 summarises the technical specifications of GTM.

Table 13: Technologies of GTM.

Component Name	Possible Technologies
Input Handle Layer	Python 3.7, Apache Kafka Python API (based on the Message Bus implementation)
Reputation Calculation Component	Python 3.7
Output Former	Python 3.7
GTM db	Python 3.7, MySQL

5.2.4.4 Dependencies to other components

The following table depicts and describes the dependencies of GTM with the other SPEAR components and subcomponents. In particular, GTM takes security events as input from the underlying layers and computes a node-centric reputation.

Table 14: GTM dependencies with the other SPEAR components and subcomponents.

Component	Dependency description
VIDS	GTM will send information about the node reputation to VIDS.
Message Bus	GTM receives from the Message Bus asset-related information, anomaly-based detected security events as well as signature-based detected security events.

5.2.4.5 Addressed Requirements

The following table depicts and describes the system requirements satisfied by GTM.

Table 15: System requirements addressed by GTM.

Requirement ID	Requirement Name
F01	Assets Protection
F03	Data Transmission
F08	Encrypted communication
F33	VIDS Visual Analytics interconnection with GTM
F34	Asset Reputation
F35	Trust Asset Alerts
F36	Trust System Alert
NF01	Optionality
NF02	Scalability
NF04	Password Encryption
NF05	Data Encryption
NF08	Bandwidth

5.2.5 Message Bus

5.2.5.1 Main functionalities

This component offers a communication system between all SPEAR components that are interacting and exchanging events information. This component will handle the events exchange, which nature is asynchronous, therefore it will be based on the publish–subscribe paradigm.

5.2.5.2 Internal components

The Message bus is a unique component based on Apache Kafka technology.

5.2.5.3 Technical Specifications

Like the SPEAR SIEM Basis, the Message bus is delivered as a docker based deployment and it is based on Apache Kafka technology. HW requirements can be found in https://kafka.apache.org/documentation/#hwandos

5.2.5.4 Dependencies to other components

As shown in Figure 15, the Message bus communicates with multiple SPEAR components. The following table depicts and describes the interactions of Message bus (Component 1) with the other SPEAR components and subcomponents (Component 2).

Component	Dependency Description
BDAC	BDAC will publish the events detected as anomaly of the SG system.
Visual IDS	Visual IDS will publish the events detected as anomaly of the SG system. Visual IDS will also be subscribed to the events generated by other SPEAR components, so it can visualize those events in a user-friendly dashboard.
GTM	GTM will be subscribed to the events generated by other SPEAR components, so it can calculate the reputation of the assets of the SG system.
OSSIM	OSSIM will publish the events detected as suspicious.
Anonymous SPEAR-RI	Anonymous SPEAR-RI will be subscribed to the events generated by other SPEAR components, so it can decide whether the events need to be reported in the RI ecosystem.
SPEAR-FR	SPEAR-FR will get security events from Message Bus that will be considered as a start point for the forensic investigator

5.2.5.5 Addressed Requirements

The following table depicts and describes the system requirements satisfied by Message Bus.

Table 16: System requirements addressed by Message Bus.

Requirement ID	Requirement Name
F03	Data Transmission
F12	BDAC interconnection with Message Bus
F29	VIDS interconnection with Message Bus

5.2.6 AMI Honeypot

5.2.6.1 Main functionalities

AMI Honeypots as part of SPEAR FRF provide a set of systems that emulate SG elements and act as a decoy to attract cyberattackers, and to detect, deflect and/or study attempts to gain unauthorised access to the system. This component is designed to emulate and hide real SG elements. The gathered Honeypots data is sent to the SPEAR SIEM to be analysed.

Different types of AMI honeypots will be developed and deployed in the project Use Cases:

- RTU honeypots: Remote Terminal Units are key components of the Smart Grids by Schneider.
- PLC honeypots: Programable Logic Controllers manage analogic and digital I/O in Smart grids of PPC and VETS.
- Smart Home honeypots: For smart-devices and smart-grid equipment (HVAC smart-systems, smart-meters, smart-inverters, etc.) used in CERTH Smart Home.

5.2.6.2 Internal components

Figure 15 shows a component view of the RTU Honeypot, which describes the base technologies used:

- Open-source ICS/SCADA Honeypot called Conpot[9]
- Open-source SSH/Telnet Honeypot called Cowrie[10]
- IEC61850 server simulator

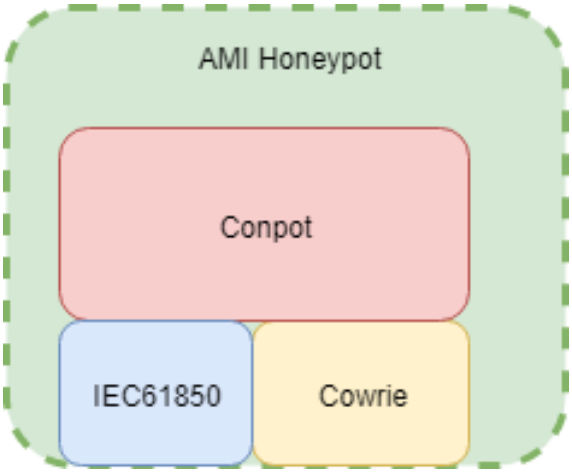


Figure 15: RTU Honeypot component view

In the next subsection, we will deep into technical details of each one of these components.

[9] http://conpot.org/

[10] https://github.com/cowrie/cowrie

5.2.6.3 Technical Specifications

SPEAR AMI Honeypots will utilise python-based libraries, such as pandas and modbus-tk as well as the Conpot open-source project. In particular, the SPEAR AMI Honeypots will be based on Conpot, which implements a framework for emulating numerous industrial and IT protocols, such as Modbus, BACnet, HTTP and FTP. Cowrie SSH and Telnet open source Honeypot project and IEC61850 server simulators will be used as well.

In the context of the SPEAR project, the utilisation of the modbus-tk library will be adopted so that the Conpot-based SPEAR honeypots can emulate real devices, such as Modbus PLCs and AMI components in a more realistic manner since Conpot itself can use only default messages and options. In particular, the network traffic of the real devices will be used to modify appropriately the messages of the Conpot-based SPEAR honeypots in order that they will be similar to those messages generated by the actual devices. By processing network traffic files (PCAP files) of the real industrial devices, SPEAR honeypots will adopt the relevant characteristics (e.g., function codes, register addresses and coil values of the Modbus messages), thus being able to generate the corresponding response messages.

The RTU honeypot that will be developed in SPEAR is one of the most complete industrial honeypots, which will be able to emulate many different industrial OT and IT protocols listed below:

- IEC 60870-5-101
- IEC 60870-5-103
- IEC 60870-5-104
- DNP 3.0
- MODBUS
- IEC61850
- MMS
- Goose
- SSH
- FTP
- Telnet
- HTTP
- HTTPS

Together with the protocol emulation, the AMI honeypots will be able to emulate traffic as required to simulate the normal behaviour of the real equipment. For example, the RTU Honeypots will emulate communications with Modbus and DNP3 protocols to better fake a real system.

Furthermore, the AMI honeypots will need to record all the traffic reaching any of their ports. These traffic logs will be afterwards sent to the SPEAR SIEM for their analysis. Note that all traffic captured by the AMI Honeypot is malicious traffic, and therefore, this will ease forensic investigation as the Honeypot allows tracing and understanding the attacker's activity.

5.2.6.4 Dependencies to other components

The following table depicts and describes the interactions of AMI Honeypots with the other SPEAR components and subcomponents.

Component	Dependence Description
Honeypot Manager	Honeypot Manager will be responsible for configuring and deploying the various honeypot instances.
SPEAR SIEM Basis	SPEAR SIEM Basis will get the data captured by the AMI Honeypots deployed in the Smart Grid.
BDAC	BDAC will use the data captured by the AMI Honeypots in order to enhance its functionality.

AMI Honeypots will interact with the Honeypot Manager component which is in charge of setting up and managing individual AMI Honeypots and AMI Honeypot networks, i.e. this component allows to deploy several honeypots into a single infrastructure considering different configurations. This component will also manage the honeypots by starting and stopping them and allows to control them remotely. As the AMI Honeypots will incorporate scripts to perform these tasks, it is quite straightforward to execute them from the Honeypot Manager.

Figure 16 shows the interaction between the Honeypot Manager and the AMI Honeypots.

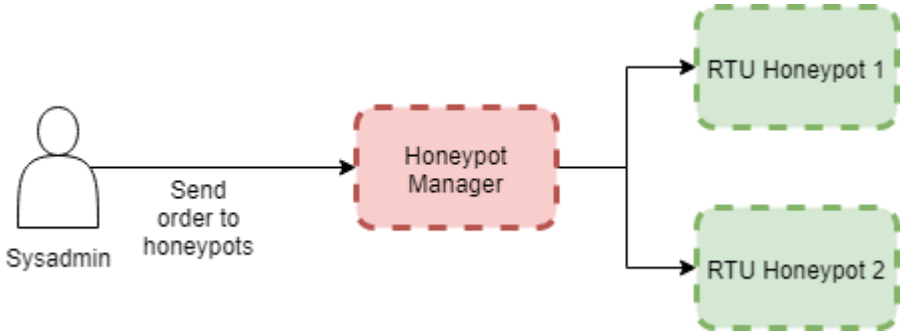


Figure 16: Honeypot Manager.

AMI Honeypots interact with the SPEAR SIEM as well by sending it the different logs to enhance the cyber intelligence capabilities of the SIEM and try to prevent further attacks. Each component from the AMI Honeypot generates its own logs and it is planned that all logs will be merged together to generate a single logging mechanism.

5.2.6.5 Addressed Requirements

The following requirements are addressed by AMI Honeypots:

Table 17: System requirements addressed by AMI Honeypot.

Requirement ID	Requirement Name
F37	Sensors and Honeypots Deployment
F38	HoneyPots

5.2.7 Honeypot Manager

5.2.7.1 Main functionalities

The Honeypot Manager is the component responsible for automating and optimizing AMI Honeypot deployment and creating honeynets, i.e. it manages the creation, deployment, configuration and removal of the individual and sets of AMI honeypots developed in SPEAR, as required in the project use cases.

The Honeypot Manager can perform the following actions:

- Load a specific honeypot configuration to be deployed by Terraform in one of the virtual machine providers it supports. Each honeypot will be deployed and started in a separate virtual machine instance. The main providers that Terraform supports are:

Amazon Web Services (AWS)	Digital Ocean	Oracle Cloud Platform
Azure	Google Cloud Platform	VMWare vSphere

- Stop/destroy a deployed infrastructure of running virtual machine instances.

5.2.7.2 Internal components

Honeypot Manager is composed of thee sub-components: (1) Planner, (2) Initial data loader, and (3) Controller, as depicted in Figure 17.

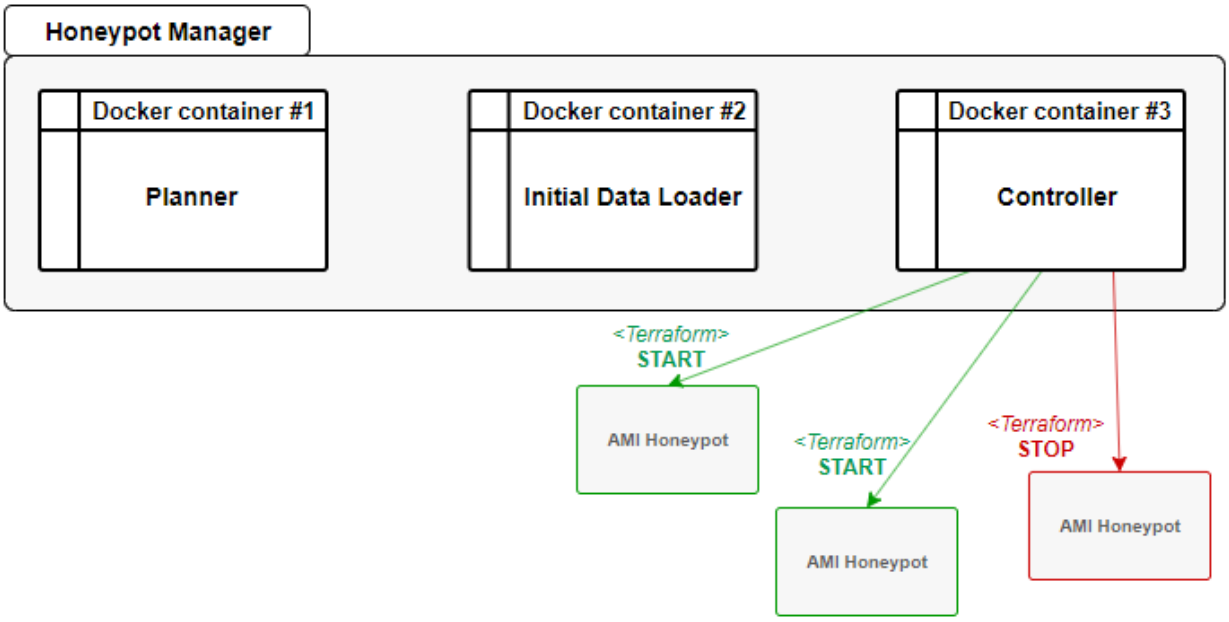


Figure 17: Honeypot Manager components diagram.

- **Planner**. This database server is deployed inside a Docker container. It consists of a database with information about the Controller configurations for different VM providers, honeypots deployment configurations, etc. This component will be the one exploiting Game theory-based optimization methods to decide on best deployment strategies.
- **Initial data loader**: This component is responsible for loading the initial information that the database will contain. In the same way as the Planner, the component is deployed inside a Docker container.

- **Terraform Server**: This component implements the REST API to launch the Controller, to deploy or destroy the infrastructure of virtual machine instances containing the different honeypots. It is also deployed in a Docker container.

5.2.7.3 Technical Specifications

The Honeypot Manager is delivered as a docker based deployment. Docker needs to be installed in all machines used for deploying the Monitoring Enabler components; Docker installation is well explained in the documentation of Docker[11] .

Next, the base technologies used for the Honeypot Manager are listed:

- The Planner is based on MySQL[12] Server
- The Initial data loader is based on MySQL Client
- The Controller is based on Terraform Server[13]

5.2.7.4 Dependencies to other components

The following table depicts and describes the interactions of Honeypot Manager (Component 1) with the other SPEAR components and subcomponents (Component 2).

Component 1	Component 2	Dependence Description
Honeypot Manager	AMI Honeypots	The Honeypot Manager will manage the creation, deployment, removal and configuration of the set of SPEAR AMI honeypots.

5.2.7.5 Addressed Requirements

The following requirements are related to Honeypot Manager:

Table 18: System requirements addressed by Honeypot Manager.

Requirement ID	Requirement Name
F37	Sensors and Honeypots Deployment
F38	HoneyPots
NF11	Compliance

[11] About Docker CE installation documentation, https://docs.docker.com/install/

[12] https://www.mysql.com/

[13] https://www.terraform.io/

5.2.8 SPEAR Forensic Repository (SPEAR-FR)

5.2.8.1 Main functionalities

SPEAR-FR will support forensic investigations by centrally collecting the most prevalent (but not exhaustive) sources for host and network-based forensics, namely: a) syslogs for Linux systems and EventLog for Microsoft Windows family of operating systems, b) network traffic data, including packet captures, network flows, statistical data (sometimes also referred to as metadata) and c) security events generated by the SIEM Basis, BDAC and VIDS.

At the same time to ensure the privacy of individuals and protection of their sensitive data SPEAR-FR will employ encryption mechanisms for data in transit and at rest.

5.2.8.2 Internal Components

There are not any internal components in the SPEAR Forensic Repository.

5.2.8.3 Technical Specifications

For SPEAR-FR to function properly, Linux operating system running a syslog server and a NetFlow collector will be used, including an externally mounted storage employing dm-crypt with LUKS extension.

To ensure protection of forensic data in transit:

1. PCAP files will be transmitted using secure protocols, such as SSH and HTTPS.
2. NetFlow traffic will be forwarded to a NetFlow collector through a secured (IPSEC, VPN tunnel).
3. For log files will be collected to a syslog server using the Reliable Event Logging Protocol (RELP).

5.2.8.4 Dependencies to other components

SPEAR-FR depends on:

1. Collecting PCAP files using “port mirroring” configured through the switch administrative interface (passive evidence acquisition).
2. NetFlow traffic exported via the routers.
3. Log files from all developed applications/components, including identified servers within the targeted organization, such as DHCP servers, DNS servers, authentication servers, NIDS/HIDS servers, Firewalls.
4. Security events generated by the OSSIM, VIDS and BDAC

5.2.8.5 Addressed Requirements

The following table depicts and describes the system requirements satisfied by FR.

Table 19: System requirements addressed by SPEAR-FR.

Requirement ID	Requirement Name
FRF01	Forensic Data Collection
FRF02	Forensic Data Transmission
FRF03	Forensic Data Storage
FRF04	Forensic Data Access
FRF05	Availability of forensic data
FRF06	Forensic Data Timeline
FRF07	Data Protection Impact Assessment (DPIA)

5.2.9 SPEAR-RI

5.2.9.1 Main functionalities

This component provides anonymous interconnection channels amongst SG operators with the purpose of exchanging information related to cybersecurity incidents but preserving the anonymity of the source.

The SPEAR RI will therefore be the basis for a common anonymous communication channel, where energy-related organisations across Europe will be able to broadcast sensitive information in an anonymous way without exposing the reputation of the organisation victim of an attack.

5.2.9.2 Internal components

The SPEAR Anonymous RI will be basically a Database based on MISP (https://www.misp-project.org/) platform plus an anonymisation component in charge of making sure that information in the published incidents do not result in victim identifiable information.

As shown in Figure 18, the events in the SPEAR Anonymous RI will be the publishable subset of all the events identified by the SIEM previously filtered by the Event filtering component and anonymised by the Anonymisation component. These events will serve as a feed of the organisation MISP database who will share the information with SPEAR MISP database for the electricity MISP community, which in turn will share the incident information with other MISP communities.

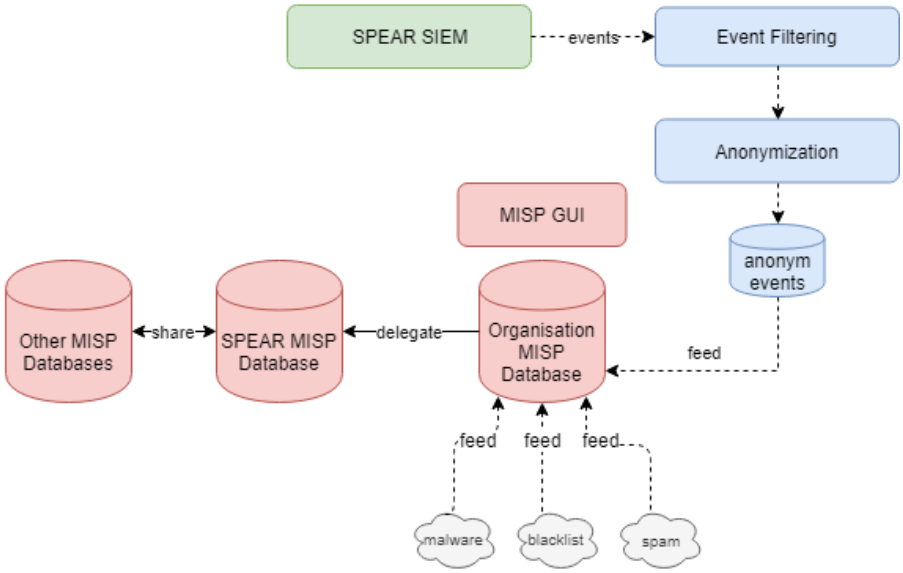


Figure 18: SPEAR RI components

5.2.9.3 Technical Specifications

The SPEAR Anonymous RI will be based on the MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (https://www.misp-project.org/) platform.

MISP software is adopted and promoted around the CERT world and CERT-EU, CIRCL, and many others are successfully using it already, although no specific MISP community exists yet for electricity organisations. MISP Architecture is depicted in Figure 19.

Figure 19: MISP architecture

In order to anonymise incident information and avoiding the victim be identified, anonymisation technologies will be to ensure anonymised victim identity and location. Still, the technical details of the attack will be available for everyone to take countermeasures timely.

To achieve this, the SPEAR Anonymous RI will exploit as much as possible the technologies adopted in MISP to anonymise victim's identifiable information and enhance them with other anonymisation techniques such as the group signature and the k-anonymity technique if required.

5.2.9.4 Dependencies to other components

The SPEAR SIEM provides with the events information to the Anonymous SPEAR-RI. The incident publication in the SPEAR RI will be a post-forensics process, where the responsibility for the information sharing will decide on incidents and content to be published for the benefits of cybersecurity intelligence collaboration among the community members.

Component	Dependence Description
SPEAR SIEM Basis	Part of the shared incident information will be retrieved from SPEAR SIEM Basis captured traffic and log traces.
SPEAR FRF	The forensics results will be used to inform on incident details and recommended countermeasures and protections to prevent the incident to occur.

5.2.9.5 Addressed Requirements

The following table depicts and describes the system requirements satisfied by SPEAR-RI.

Table 20: System requirements addressed by SPEAR-RI.

Requirement ID	Requirement Name
F08	Encrypted communication
F46	Anonymous Information Sharing
F47	Event Description
NF01	Optionality
NF04	Password Encryption
NF05	Data Encryption
NF08	Bandwidth

5.3 Interfaces Model

The interface specification model shows which logical interfaces are exposed by each of the platform components in 5.2. The information (i.e., parameters) that goes in and out of the interfaces refers to the System information model in Section 5.1. Please note that for the present high-level description of the SPEAR architecture we provide only the main services offered in the interfaces and additional or refined services may be found in prototype implementations.

5.3.1.1 SPEAR SIEM Basis

This component is responsible for collecting, parsing and storing smart-grid data. The main services offered by the SPEAR SIEM Basis component are the following:

- publishSGData (SGdata, topic): allows to publish SG data to a specific topic of the Streaming Bus. This service will be used by the NCP component to send parsed data to the DAPS.
- parseSGData(SGdata): allows to acquire and parse SG data. It can handle different type of data: network data including industrial protocols, network flow and operational data. This service will be provided by the NCP sub-component.
- storeSGData(SGdata): allows to store all collected and parsed SG data in the Storage infrastructure (DAPS).
- retrieveSGData(SGDataAttribute[]): allows to retrieve the parsed SG data which is stored in the Storage infrastructure (DAPS).
- suscribeToSGData (topic): allows to retrieve the parsed SG data in streaming. It will be used by BDAC and Visual IDS.

5.3.1.2 Big Data Analytics Component (BDAC)

This component performs big data analytics on the collected SG data in order to detect anomalies in the SG related to cyberattacks. The main services offered by the BDAC component are the following:

- analyticsOnSmartGridData(preprocessedData): applies data analytics techniques to detect possible anomalies and cyberattacks in the SG system via a plethora of machine learning and deep learning based models that form the Analysis Engine Module of BDAC.
- publishBDACEvent(attackDetails): sends security events to the Message Bus via the Security Events Extraction Module.

5.3.1.3 Visual-aided IDS

This component visualizes the security events generated by BDAC and SPEAR SIEM Basis. The main services offered by the VIDS component are the following:

- visualAnalytics(preprocessedData): perform visual analytics on the pre-processed smart grid data coming from SPEAR SIEM Basis via the Visual Analytics subcomponent.
- publishVisualIDSEvent(attackDetails): publish security events (cyberattack) to the message bus to be exchanged with the SPEAR tools that need to be fed with this information via the Security Event Consuming/Producing component.
- retrievesSmartGridData(smartGridData) - retrieves smart grid data via the Smart grid pre-processed Data Ingestion internal component.

5.3.1.4 Grid Trusted Module (GTM)

This component improves the detection of internal security threats and incidents such as accidental mistakes, hardware failures and malicious actions from inside. The reputation of each node is presented by the visual-aided IDS to support awareness of the SPEAR sysadmins. The main services offered by the Grid Trusted Module component are the following:

- calculateNodeReputation(Events): Calculates the SG system nodes' reputation based on events received by the SPEAR SIEM via the RCC component.
- nodeReputation(nodeId):Reputation - sends the reputation of each node to the visual-aided IDS to support awareness of the SPEAR sysadmins.

5.3.1.5 Message Bus

This component collects all SG data and using the privacy-preserving libraries (part of the SPEAR FRF) prepares them to be securely stored in the SG database, while at the same time ensuring compliance with relevant data protection regulation (GDPR). The main services offered by the Message Bus are the following:

- suscribeToEvents(topic): allows to retrieve the events generated by the SPEAR SIEM.
- publishEvents(event, topic): allows to publish events to a specific topic of the Message Bus. This service will be used by OSSIM, BDAC and VIDS to publish detected incidents and anomalies in the SG system.

5.3.1.6 AMI Honeypot

The AMI Honeypot component simulates an AMI to trap attackers and capture all the malicious activity for its further analysis in the SIEM. Therefore, the main services offered by the AMI Honeypot are the following:

- controlAMIHoneypot(controlAction): allows to control and manage the AMI honeypot; e.g. by stopping, starting or modifying some configuration of the Honeypot. This service usually will be used by the Honeypot Manager.
- sendSystemActivity(SystemId): sends the captured activity over a system to SPEAR SIEM for its analysis.

Please note that these services may be transformed into a more detailed API during the project lifetime.

5.3.1.7 Honeypot Manager

This component manages the creation, deployment, removal and configuration of the set of SPEAR AMI honeypots. The main services offered by the AMI Honeypot Manager are the following:

- createAMIHoneypotImage(smartGridNode, smartGridNodeCharacteristics): creates a VM custom image of a specific smart-grid node that we want to emulate.
- updateAMIHoneypotImage(AMIHoneypotImageId, smartGridNodeCharacteristics): updates a previously created VM custom image instance using the provided node sw/hw characteristics.
- getAMIHoneypotImagesList(): returns all available smart-grid node VM images.
- deployAMIHoneypot(imageId): deploys a new AMI honeypot (VM) according to the image we want to emulate and returns its deployment id.
- undeployAMIHoneypot(honeypotId): deactivate a given AMI honeypot; i.e., removes it from the smart-grid.
- getAMIHoneypotList(): returns all deployed AMI honeypots.

5.3.1.8 SPEAR-FR

The SPEAR-FR contains the specification of the service implementing the business logic pertaining to the management of the forensic data in the SPEAR system. The main services offered are the following:

- storeForensicData(ForensicData, Component_ID): stores forensic data in the encrypted file system.
- retrieveForensicData(Component_ID): decrypts and retrieves forensic data from the encrypted file system.

5.3.1.9 Anonymous SPEAR Repository of Incidents (RI)

This component provides anonymous interconnection channels amongst SG operators for incident information sharing. The main services offered are the following:

- createEvent(eventDetails): creates a new entry in the SPEAR RI in an anonymous way without exposing the reputation of the organization posting the event.
- readEvent(eventId):AnomizedEvent - Returns the anonymized event
- updateEvent(eventId, eventDetails): updates selected event in the repository.
- deleteEvent(eventId): Removes the selected event from the repository.

5.3.2 Collaboration Model

The system collaboration model describes the main interaction between the components of the SPEAR platform using information items defined in Section 5.1 as well as the interfaces defined in Section 5.3. The sequence diagrams below show the main and high-level interactions and there may be other possible interaction sequences for a process.

The following four main processes have been envisaged for the SPEAR platform:

1. Anomaly detection.
2. Honeypots captured attack analysis
3. Information sharing with third parties
4. Forensic Analysis

The **anomaly detection process** is shown in Figure 20, Figure 21 and

Figure 22. The system or security administrator of the SG will use the SPEAR SIEM Basis to start monitoring the system and to collect the SG data generated by the system. The SG data collected by the SPEAR SIEM Basis includes mainly network traffic and log data produced by the SG system assets. The SPEAR SIEM Basis will pre-process the network traffic, specifically it will parse SG specific communication protocols traffic data as well as operational information included in the payload of those protocols, and extract and store the attributes defined in the protocols. Therefore, the SG data is ready to be used by data analytics techniques in the following step.

The analysis of the collected SG data can be done by several SPEAR SIEM components, i.e. BDAC, Visual-aided IDS and SPEAR SIEM Basis based on integrated OSSIM components.

Figure 20 shows the **anomaly detection process in which the analytics is performed by BDAC**. The BDAC will retrieve the pre-processed SG data and will apply near real-time data analytics techniques to detect anomalies in the SG system. The BDAC will implement an anomaly-based intrusion detection system. In particular, BDAC will be able to detect possible anomalies and cyberattacks based on the

network traffic of the network, transport and application layers (based on the OSI model) as well as by inspecting specific electricity values such as current, voltage and phase. Once an anomaly event is detected by the BDAC, it will be published in the SPEAR SIEM message bus to be exchanged with the SPEAR tool that needs to be fed with this information (i.e., Visual-aided IDS and GTM).

The GTM component will calculate the SG system nodes' reputation based on events received by the SPEAR SIEM. The reputation of each node is presented by the Visual-aided IDS to support awareness of the SPEAR administrator.

The Visual-aided IDS will also display potential risks based on historical data, patterns and behavioural analysis and supports decision making in triggering alarms to the SPEAR administrator.

Figure 21 shows the **anomaly detection process in which the analytics is performed by Visual-aided IDS**. SPEAR SIEM basis will pre-process the collected data and feed Visual-aided IDS, which will perform visual analytics methods. Visual-aided IDS will provide web-based and mobile-based applications to illustrate its results as well as the results provided by BDAC. Once an incident is detected by the Visual-aided IDS, it will be published in the SPEAR SIEM message bus to be exchanged with the SPEAR tool that needs to be fed with this information (i.e. GTM). The GTM component will calculate the SG system nodes' reputation based on events received by the message bus. Then, the Visual-aided IDS will also display all the details of the incidents to the SPEAR administrator.

Figure 22 shows the **anomaly detection process in which the analytics is performed by SPEAR SIEM Basis**. The analysis of the data is performed by the OSSIM components integrated into the SPEAR SIEM Basis; i.e., Network IDS based on known patterns and Host IDS. Once an incident is detected by the SPEAR SIEM Basis, it will be published in the SPEAR SIEM message bus to be exchanged with the SPEAR tool that needs to be fed with this information, i.e., GTM, so the reputation of the SG can be re-calculated.

The **honeypots captured attack analysis process** is shown in Figure 23. The SPEAR AMI honeypots will be emulating the behaviour of AMI devices of the SGs and their objective is to attract cyberattackers, and to detect and study attempts to gain unauthorised access to the system. Since the honeypots are not part of the real SG operation process, all interactions with the honeypots are considered hostile or malicious. Therefore, the SPEAR AMI honeypots will provide SPEAR SIEM with Honeypots data that will be in turn analysed for detecting cyberattacks and anomalies.

In a similar way than in the previous process, the SPEAR SIEM Basis will pre-process the collected data by the honeypots and the data will be ready to be analysed by BDAC and Visual-aided IDS. The BDAC component will study the data in order to detect new intrusion detection patterns and will publish new honeypot events accordingly into the SPEAR Message bus. The Visual-aided IDS will display all the information related to the honeypots events.

The **incident information sharing with third parties process** is shown in Figure 24. The anonymous SPEAR-RI will be fed with all detected events by the SPEAR SIEM through the Message bus. The CISO together with the DPO responsible of the SG can check all the events and decide which one they want to share with external entities that are managing also SGs. For that, first, the data need to be anonymized by using capabilities offered by the Anonymous SPEAR-RI and afterwards the data is ready to be shared. On the other hand, the anonymous SPEAR-RI also provides the option to display all the events shared by third parties.

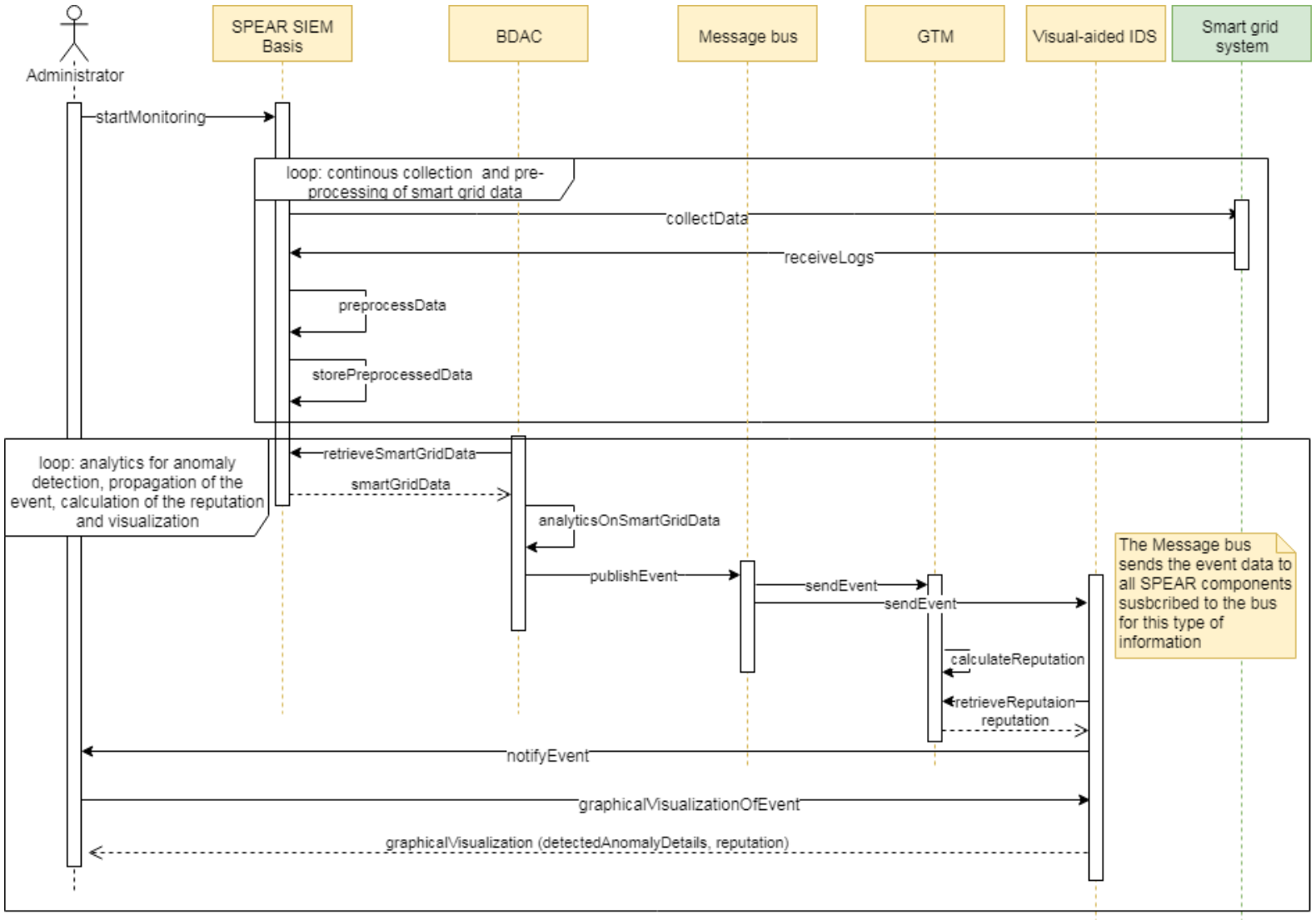


Figure 20: SPEAR anomaly detection process (BDAC)

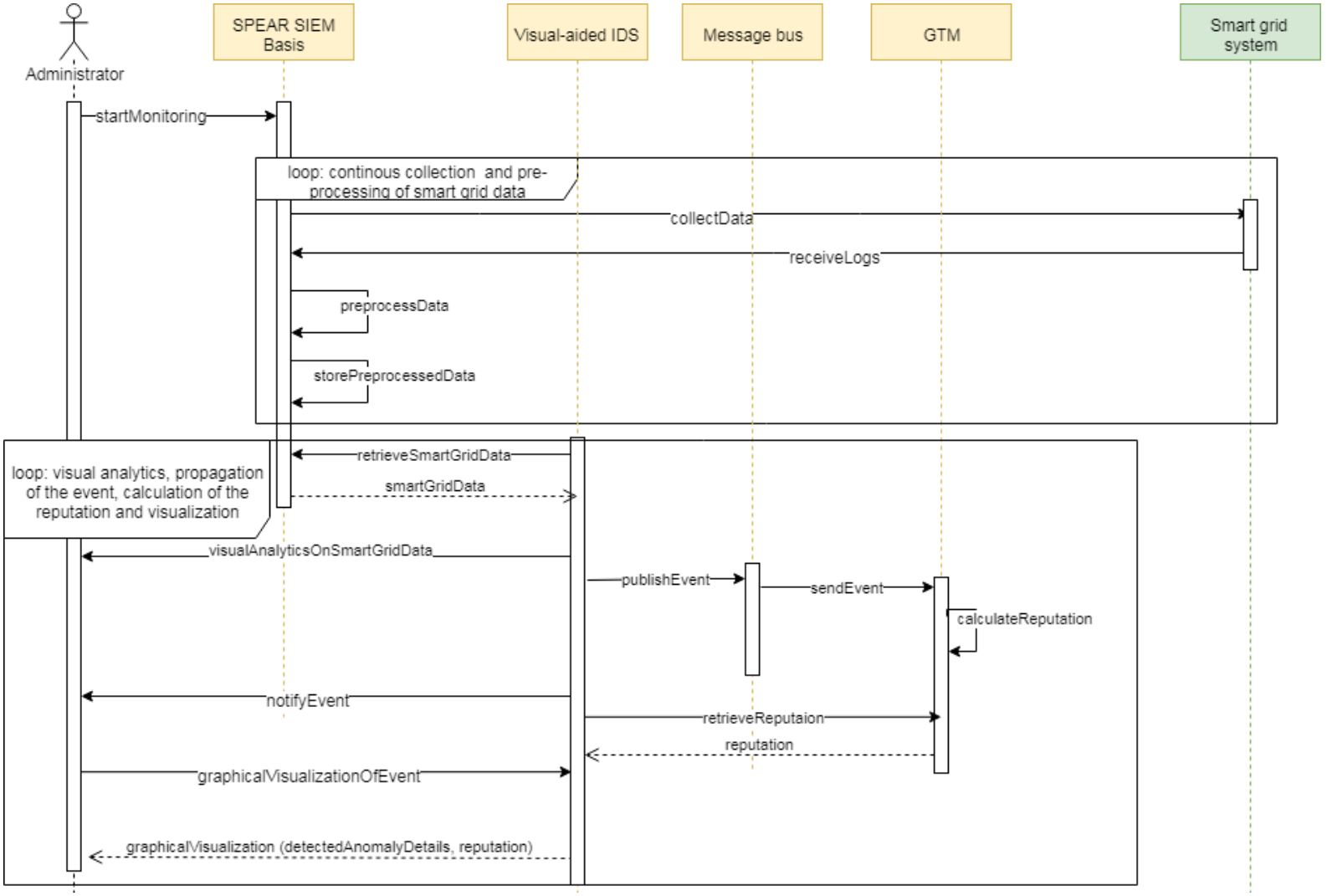


Figure 21: SPEAR anomaly detection process (Visual-aided IDS)

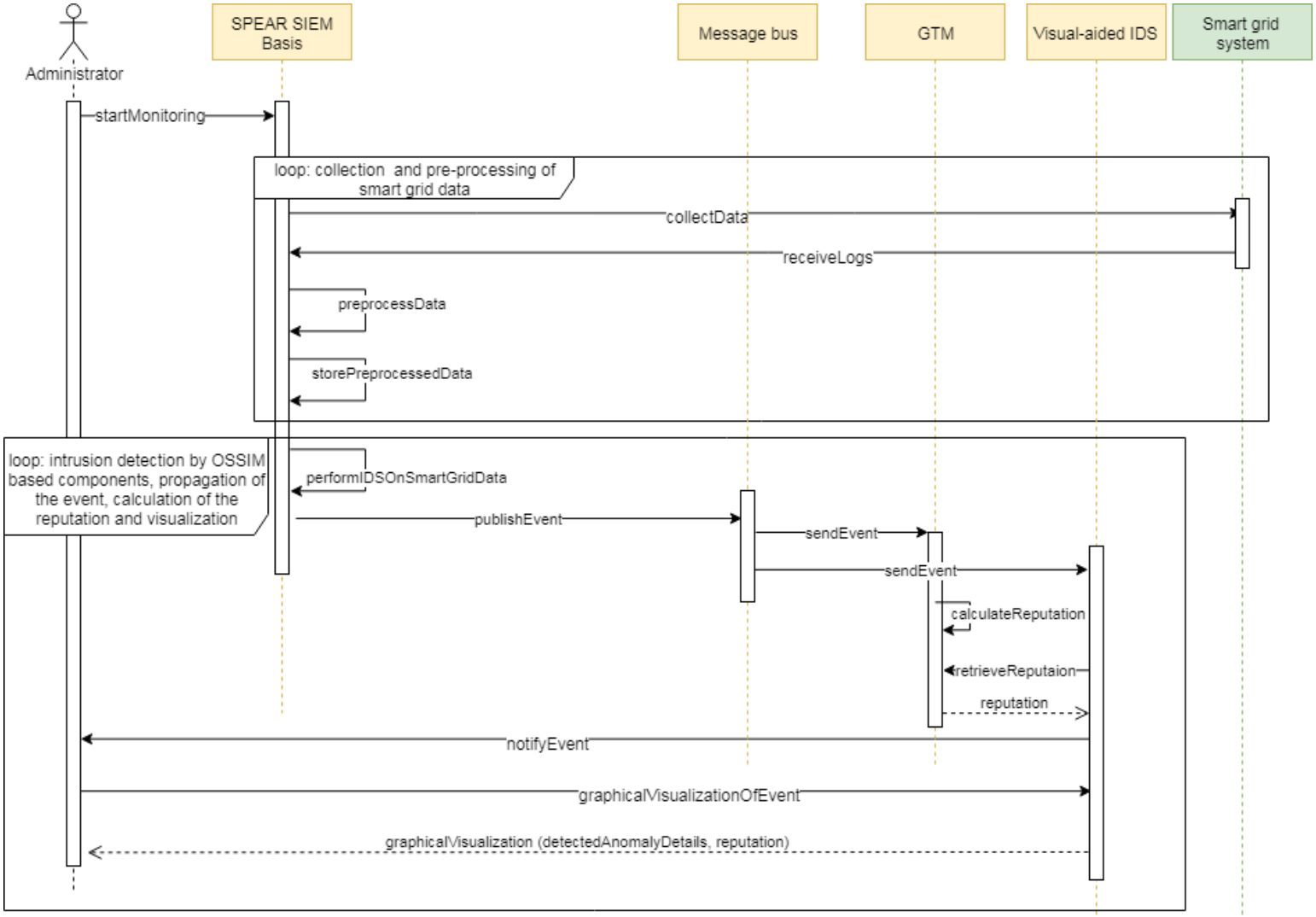


Figure 22: SPEAR anomaly detection process (SPEAR SIEM Basis)

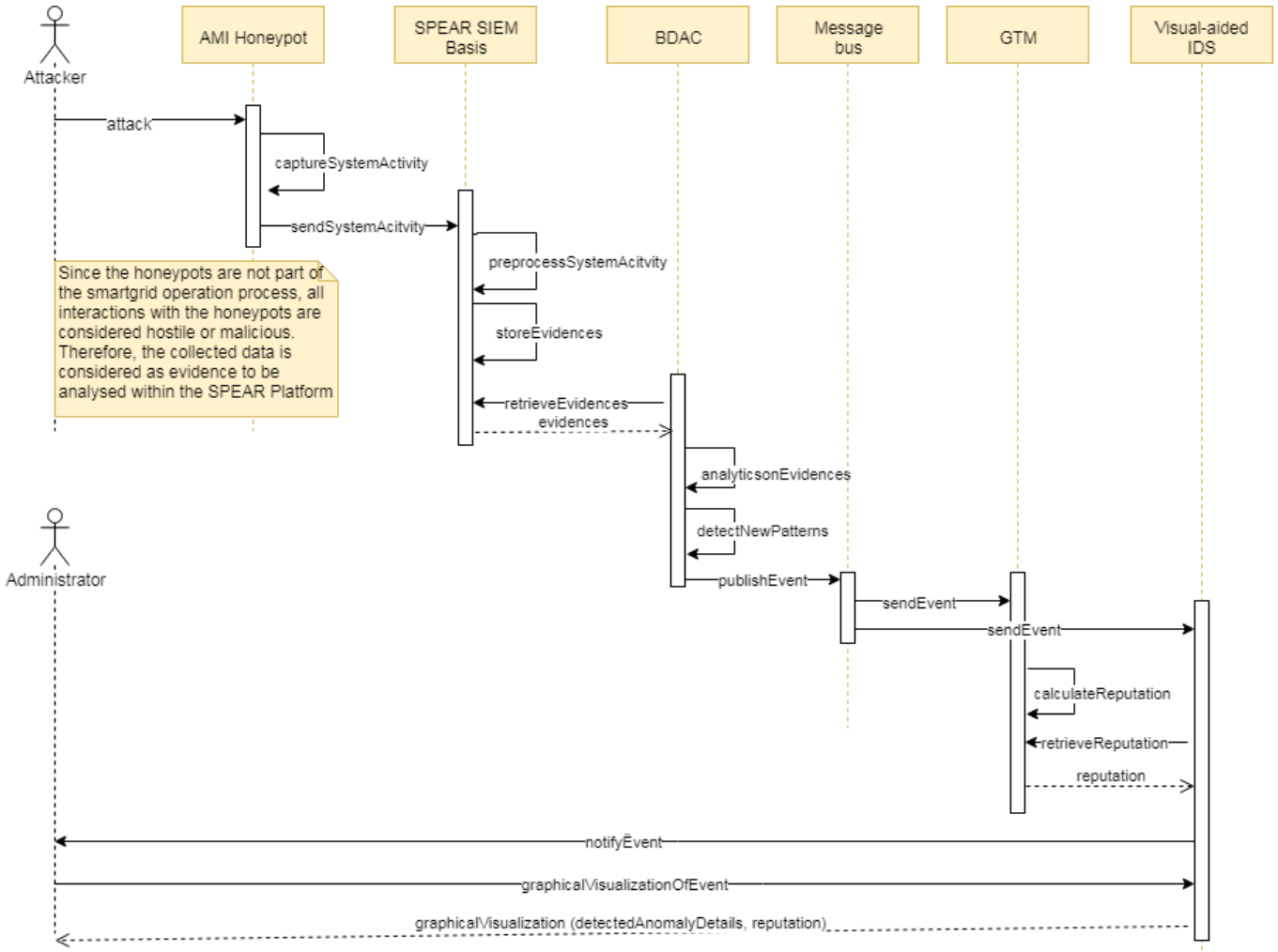


Figure 23: SPEAR Honeypots captured attack analysis by SPEAR SIEM.

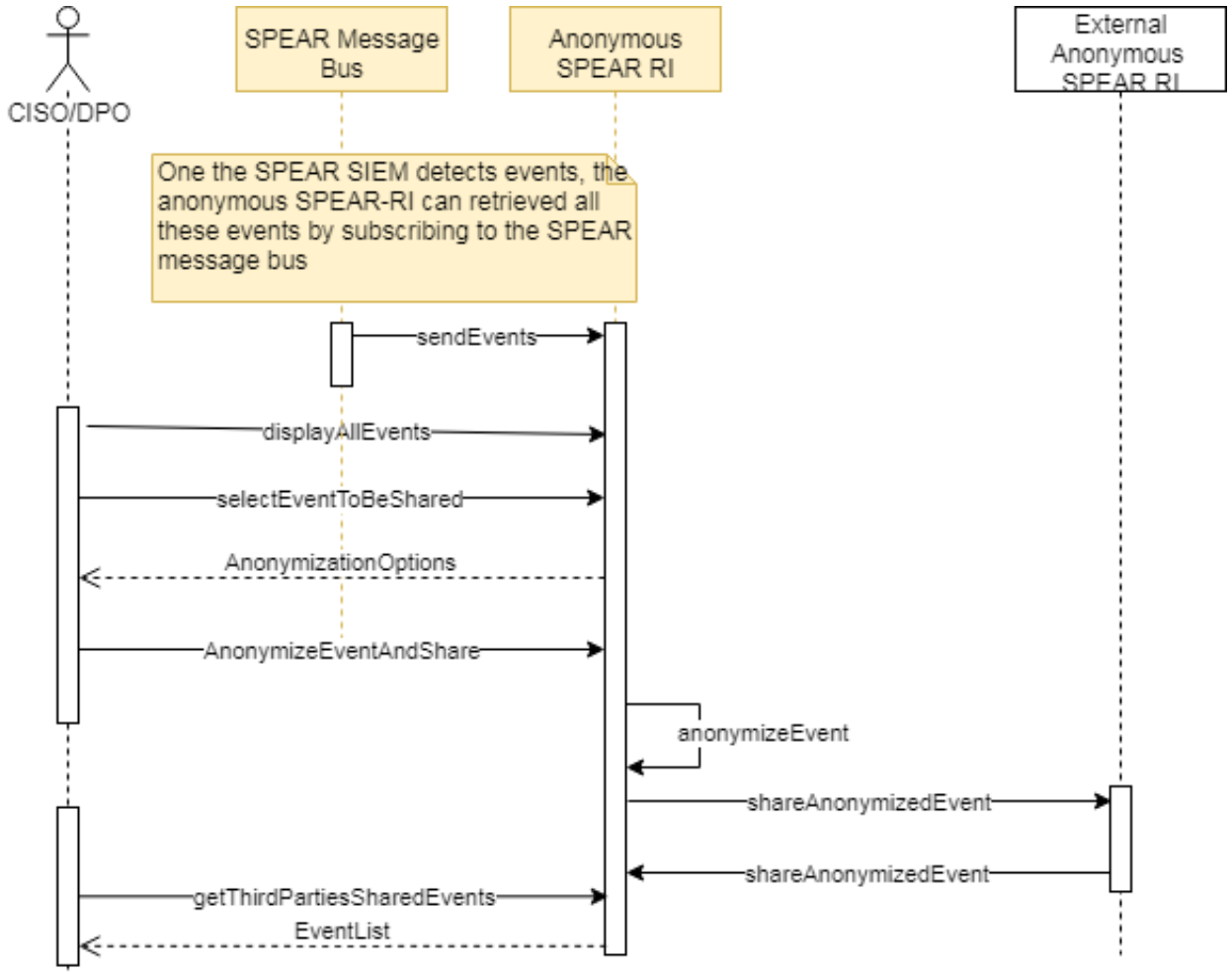


Figure 24: SPEAR Information sharing process with third parties (SPEAR RI)

Figure 25 shows the process for collecting forensic evidences in the SPEAR platform. The SPEAR Evidences Manager component will receive all detected events by the SPEAR SIEM through the message bus. To securely store data related to this event in the SG database, the evidences manager will use the Privacy-Enhancing Technology (part of the SPEAR FRF) in order to ensure compliance with GDPR. Finally, the Evidences Manager securely stores the evidences in the SG database using the provided API.

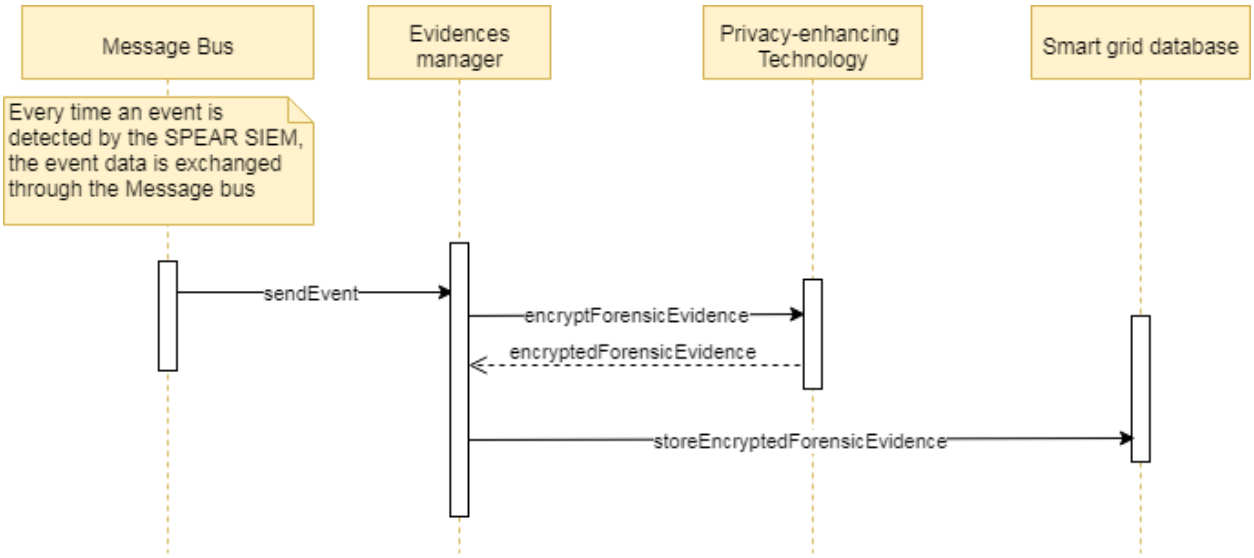


Figure 25: SPEAR Forensic evidences collection

6. Adoption of the SPEAR Platform in the SPEAR Use Cases

This section presents how the SPEAR platform architecture fits in each SPEAR use case. Each sub-section describes first the use case architecture and the available equipment in the premises of each pilot. As a next step, a description of how the SPEAR solution architecture is integrated into the use case architecture is provided together with a brief description of how the functionality of the SPEAR components is intended to protect the SG under test

6.1 Adoption of the SPEAR Platform in the Hydro Power Plant scenario

6.1.1 Hydro Power Plant scenario

The hydro power plant scenario constitutes a roadmap in validating the SPEAR architecture towards securing renewable energy SG utilities. It incorporates real testing of the developed SPEAR tools and components in an operational electricity production facility by VETS partner in Rahzlog, Bulgaria. It is an example of a utility that requires supreme technical skills and knowledge, where any potential vulnerabilities could harm major components of the SG infrastructure. The SPEAR components will be installed on a virtual machine that mirrors the HMI in the facility, which ensures pilot testing can be conducted even when the plant is operational. Different attack simulations will be carried out, targeting the vulnerable components of the power plant architecture. A detailed description of the use case can be found in Section 3.2.1 of D 2.4.

The infrastructure of the use case includes turbines, generators, electrical systems and the transformer. This equipment is governed by smart devices and smart meters by using IP interfaces and API systems. The SPEAR SIEM system will be installed in the control center, while a set of AMI honeypots will be deployed in the power generation area. The honeypots will be capable of emulating the behaviour of smart meters and other smart devices and they will be controlled by a virtual machine manager. The SPEAR SIEM tool will be connected with two databases, namely the trust management database and the incident database. The hydro power plant use case will validate the efficiency of the SPEAR platform in a renewable energy SG in terms of: a) response time to the attack, b) accuracy of the SPEAR SIEM tool, c) effectiveness of the AMI honeypots and d) robustness of the SPEAR platform against DoS, DDoS, Man in the Middle (MiM) and physical attacks.

The main components of the Hydro Power Plant are as follows:

- Turbine Control PLC - the Speed Control and Valve Control unit gathers measurements from the plant turbine and valve regarding rotation speed and valve position. The measurement PLC gathers data from the plant generator. They both transfer the collected data to the control module through Profibus TCP/IP.
- PLC control module – the SIEMENS Programmable Logic Controller manages the manufacturing processes in the plant. It collects the information from the turbine control tools, as well as from the additional sensors, which collect data regarding water level in the pressure chamber, pressure, temperatures of different plant equipment and others. Based on the information, the controller makes different decisions:
    - start the power plant if all measurements are in order
    - open the valve at a specific position, based on the collected parameters

    - limit the capacity of the turbine to a specific level lower than 100%, if water levels are insufficient
    - stop/prevent starting of the power plant if any of the measurements are outside the acceptable limits
- HMI – All the information from the PLC control module is visualized on an operator station inside the power plant via Modbus TCP/IP communication. The HMI is not only used for monitoring, but also control of the entire power plant, since every operational parameter can be manipulated from it. The HMI and PLC Control Module are both vulnerable to cyber-attacks and they are the most important elements of the power plant, which need to be protected from attackers.
- IoT Devices – 2 main types are deployed:
    - Raspberry Pi - there are 2 third-party IoT devices installed in the power plant, which collect information from the control module regarding the plant performance via Modbus TCP/IP communication. They send the data to a cloud server, where it is obtained and analyzed by the third-party service providers (Grid Balancing Operator and O&M contractor.
    - Particle Photon – an open source IoT device, which communicates via Modbus TCP/IP with the control module and collects data. The gathered information is then visualized on an IoT application called “Blynk”, which is used for remote monitoring of the PLC visualization module on a mobile device. We are working on upgrading the capabilities of the IoT application to include control functions.

6.1.2 SPEAR Components

The following description presents the use of the SPEAR solution components in the Hydro Power Plant use case:

- SPEAR SIEM – the Security Information and Event Management tool, including its comprising components, will monitor the traffic to/from the hydro power plant for suspicious activity. The BDAC and Visual-aided IDS components will detect anomalies in the data packets and will report them to the operator or security administrator. The system will monitor the different PLC controllers in the power plant, the Human Machine Interface, the router, as well as the vulnerable IoT devices, which are used for monitoring and control (Raspberry Pi and Particle Photon).
- SPEAR-FRF and SPEAR-CHF work together to collect information from the cyber-attack incidents in the Hydro Power Plant that is valuable for the court. These two frameworks are a set of rules and policies derived from national and European laws and regulations. Honeypots - the SPEAR honeypot service will have 2 separate components, which imitate a vulnerable PLC controller and an IoT device (Raspberry Pi and Particle Photon) to attract potential attacks and to record crucial information about the incident and attacker. The gathered data will be forwarded to the SPEAR-SIEM tool for analysis.
- SPEAR-RI – the repository of incidents will gather data about attacks from the different SPEAR Use Cases and store it in a database. Since such information is private and/or sensitive, which dictates that it will be anonymized to prevent potential use of the data with malicious intent.

6.2 Adoption of the SPEAR Platform in the Substation Scenario

6.2.1 Electrical Substation scenario

The substation scenario will address one of the critical infrastructures defined by the European Program for Critical Infrastructure Protection (EPCIP). This use case is focused on the Substation Automation Systems (SAS) that control and monitor the electrical infrastructure of the Substation.

The challenge of SPEAR is to improve the security of the SAS to protect the electrical network. In this context, Schneider Electric will provide the 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 emulate a real Substation Automation Systems of the Electrical Distribution Network. A more detailed description of this use case can be found in Section 3.2 of Deliverable D2.4.

The substation scenario will be part of the SPEAR architecture, integrating Configuration tool and security server, RTU and RTU Honeypots components. All these components will provide logs to the SIEM log collector component. In addition, the RTU honeypot will provide information to the Honeypot Manager. The scenario will integrate the needed components from the SPEAR SIEM.

The main components existing in the substation are as follows:

- Configuration tool and security server, companion products to be used with Intelligent Electronic Devices.
- RTU, already defined in Section 1.3
- RTU Honeypot, a virtual component that simulates the behaviour of a Real RTU.

6.2.2 SPEAR Components

The following description presents the use of the SPEAR solution components in the Substation use case:

- SPEAR Security Information and Event Management (SIEM), including its components. This component supports the detection of threats, anomalies and cyber-attacks in SG environments. It enables the collection of information from several architectural levels of the SG 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 visualizations could significantly assist the security administrator to globally inspect the SG 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.
- SPEAR-FRF and SPEAR-CHF work together to collect information from the cyber-attack incidents in the Substation use case. These two frameworks are a set of rules and policies derived from national and European laws and regulations.
- SPEAR-RI – the repository of incidents will gather data about attacks from the different SPEAR Use Cases and store it in a database. Since such information is private and/or sensitive, which dictates that it will be anonymized to prevent potential use of the data with malicious intent.
- AMI Honeypot: RTU Honeypot is a virtual component that simulates the behavior of a real RTU and captures all attacks to it so they can be analysed later to understand the purpose, causes, agent and means of the attack.

6.3 Adoption of the SPEAR Platform in the Combined IAN and HAN scenario

The SPEAR platform will be evaluated and validated in the Public Power Corporation (PPC) premises in Greece, subject to its ability to detect and respond to cyberattacks in combined Industrial Area Networks IANs and HANs. In particular, PPC will deploy two scenarios in realistic conditions that are described further below.

6.3.1 The TRSC Combined IAN and HAN scenario

The first scenario will be deployed on the Testing, Research and Standards Centre (TRSC) laboratory of PPC, located in Athens, Greece. The SPEAR platform will be validated subject to its ability to detect and respond to cyber-attacks in IAN and HAN networks. The IAN network will consist of a SCADA system, including industrial equipment such as a testing generator (a synchronous AC machine with the DC motor exciter and relative auxiliary equipment such as electronic starters, water and oil pumps etc.), a power distribution network with switching devices (master breaker and circuit switches) and a testing transformer. This equipment simulating a real scenario of the electrical grid will be controlled by PLCs that in turn will communicate with Master Terminal Units (MTUs) transmitting and receiving data and commands respectively. Finally, this data will be visualized in a HMI.

The HAN scenario on the TRSC premises will include smart meters that will gather data from IEDs, such as office Personal Computers (PCs), as well as from a photovoltaic plant that has been placed on the top of the building and generates power that is injected to the national power grid. The connection of the HAN system is accomplished through a medium voltage substation with five 20/0.4 kV transformers. Smart meters measure the total energy exchange that takes place in this system. Finally, both HAN and IAN will be controlled and supervised by a CCS running on the TRSC premises. A detailed description of this use case can be found in Section 3.2.3.1 of Deliverable D2.4.

6.3.2 Lavrio Unit 5 Combined scenario

The second scenario involves the Lavrio 378 MW combined cycle natural gas thermal power plant. The Lavrio no 5 unit is one of PPC's newest power plants. It is a modern, fully automated power station that is controlled, monitored and protected entirely by a DCS. Signals generated from advanced industrial equipment, like turbines, generators and wastewater treatment plants, will be controlled by PLCs that in turn will be controlled by MTUs. As in the previous case, HMIs will undertake to visualize the corresponding data. The SPEAR components will be deployed in a similar manner, but on a larger scale in contrast to the TRSC Combined IAN and HAN Scenario. A detailed description of this use case can be found in Section 3.2.3.1 of Deliverable D2.4.

6.3.3 SPEAR Components

Both networks will be directly connected to the SPEAR SIEM, that will be deployed on the TRSC premises, including the initial AlienVault OSSIM, BDAC, Visual-aided IDS and GTM. The SPEAR SIEM will be able to detect known cybersecurity threats applying the signature-based IDSs of OSSIM as well as zero-day cyberattacks, by detecting possible anomalies through BDAC and Visual-aided IDS. More detailed, BDAC and Visual-aided IDS will analyze the network traffic of the network, transport and application layers based on the OS) model, thus identifying possible cyberattack patterns. Moreover, they (BDAC and Visual-aided IDS) will examine electricity metrics such as voltage, current, phase, power and frequency, thereby

identifying possible anomalies. Furthermore, appropriate honeypots simulating vulnerable PLCs and smart meters will feed BDAC and Visual-aided IDS with additional information. SPEAR-FRF and SPEAR-CHF will establish a set of rules and regulations that will define the best cybersecurity practices and provide sufficient elements appropriate for the court. Finally, the necessary anonymity mechanisms and interfaces will be deployed for the functionality of the SPEAR Repository of Incidents (SPEAR-RI) which will aggregate various cybersecurity incidents from different organizations, without revealing private information.

6.4 Adoption of the SPEAR Platform in the SMART Home scenario

6.4.1 SMART Home scenario

The smart home scenario will be held in an actual smart home, located at CERTH premises in Thessaloniki, Greece. This scenario will perform extensive trials on the SPEAR technologies to smart home and micro-generation scenarios, where IoT devices, multi-sensorial networks and Photovoltaic systems have been already installed, supporting also demand response strategies and net metering services. The overall aim of the scenario is to showcase that SPEAR technologies can safeguard SG availability, integrity, confidentiality. In particular, SPEAR intends to assess the proposed architecture in addressing the following cyber-attacks:

- Eavesdropping attack strategies, where SPEAR will assess SPEAR SIEM capabilities for detecting cyber-attackers who enable smart devices secretly to listen or record private sessions,
- data integrity attacks & false data injection attack, where SPEAR will monitor the data exchanged in the application layer aiming at detecting cyber-attacks that intend to modify data exchange in the network traffic,
- DoS attack against smart appliances, where SPEAR honeypots will try to hide the real smart devices and expose the cyber attackers to leave traffic traces and
- sophisticated theft-oriented attacks.

A detailed description of this use case can be found in Section 3.2.4 of Deliverable D2.4.

6.4.2 SPEAR Components

The following description presents the use of the SPEAR solution components in the Smart-Home use case:

- SPEAR SIEM system with its related components, namely BDAC, Visual-aided IDS and GTM. Specifically, in the main network switch of the Smart Home the port mirroring functionality has been activated. This mechanism dumps all the incoming/outgoing traffic to/from the Smart Home network to raw network traffic files in a .pcap format. This traffic includes packets and messages from all the smart devices and gateways connected in the Smart Home network. The raw network traffic data are used as an input to SPEAR SIEM and after pre-processing are fed to the BDAC and the Visual-aided IDS to detect and report anomalies. The SPEAR SIEM monitors and secures all the network equipment in the Smart-Home such as gateways, smart-devices, routers and servers. The SPEAR SIEM reports the cyber-security status of the network infrastructure and cooperates with the SPEAR-FRF and SPEAR-CHF frameworks. The GTM component receives the identified by the other components events via the message bus and applies node-reputation algorithms to all nodes of the smart home and the feeds visual-aided IDS with the calculated scores.

- The SPEAR-FRF and the SPEAR-CHF work together to collect information from the cyber-attack incidents in the Smart-Home that is valuable for the court. These two frameworks are a set of rules and policies derived from national and European laws and regulations.

- The SPEAR-RI is a database that collects anonymous data from the Smart-Home and the other use case partners. These data contain all the information collected from the SPEAR system regarding a real cyber-attack or incident. The sensitivity of this information imposes the deployment of anonymity mechanisms and interfaces in order to protect from the misuse of any private information. The goal of this database is to create a repository with known cyber-attack and incidents related with smart-grid network infrastructure such as the Smart-Home.

- The SPEAR honeypot will imitate a vulnerable smart device in the Smart-Home. The honeypot attracts adversaries and gathers information for the attacks against the Smart-Home network. This collected data are registered in log files and processed to understand attacks/anomalies by the SPEAR SIEM. The analysis in the SIEM may be used by the Smart-Home facility administrator to understand and secure the Smart-Home network.

7. Conclusions

This deliverable aims at defining the SPEAR project architecture and interpreting the project specifications and requirements based on various constraints. The report addresses the complexity of the SG applications through security and privacy assessment techniques and provides an understanding of the scope of the project.
We have introduced the methodology applied to the Framework Design phase of the project. Following the ARCADE framework methodology, we have provided different viewpoints on the architecture. The platform's architecture has been described and the detailed functionalities and system requirements have been introduced.
This document is meant to serve as a starting point for the following actions that will be carried out in WP3, WP4, and WP5.

References

[1] Smart Grid Cybersecurity, A EURELECTRIC report. Available at: https://www3.eurelectric.org/media/314732/smart_grid_cyber_security_report-2016-030-0652-01-e.pdf

[2] Congressional Research Service, Electric Grid Cybersecurity. Available at: https://fas.org/sgp/crs/homesec/R45312.pdf

[3] L. Ardito, G. Procaccianti, G. Menga and M. Morisio, "Smart Grid Technologies in Europe: An Overview", *Energies*, vol. 6, no. 1, pp. 251-281, 2013. Available: 10.3390/en6010251

[4] Momoh, James, Smart grid: fundamentals of design and analysis, vol. 63. John Wiley & Sons, 2012.

[5] W. Wang and Z. Lu, "Cybersecurity in the Smart Grid: Survey and challenges", *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, 2013. Available: 10.1016/j.comnet.2012.12.017.

[6] Jeff Meyers, “Preparing for the Future: How Asset Management Will Evolve in the Age of Smart Grid”. Available at: https://pdfs.semanticscholar.org/9c43/b26cbd32b515915810d3c00a6fcab864e2fa.pdf

[7] Smart Grid Asset Descriptions. Available at: https://www.smartgrid.gov/files/description_of_assets.pdf

[8] C. Sun, A. Hahn and C. Liu, "Cybersecurity of a power grid: State-of-the-art", *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45-56, 2018. Available: 10.1016/j.ijepes.2017.12.020.

[9] Stav, E., 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

[10] IEEE 1471-2000, Recommended Practice for Architecture Description of Software-Intensive Systems. Available at: https://standards.ieee.org/findstds/standard/1471-2000.html

[11] EC Directorate-General for Energy 2011.

[12] Shirey, R., Internet Security Glossary, Version 2 (RFC4949). 2007, Network Working Group.

[13] ENISA, Smart Grid Threat Landscape and Good Practice Guide. December 2013.

[14] Carrier, Brian D (7 June 2006). "Basic Digital Forensic Investigation Concepts". http://www.digital-evidence.org/di_basics.html

[15] Log file. Available at: https://whatis.techtarget.com/definition/log-log-file (January 2019)

[16] Chief Security Officer (CSO) definition. Available at:https://whatis.techtarget.com/definition/CSO-Chief-Security-Officer (January 2019)

[17] Chief Information Security Officer (CISO) definition. Available at: https://searchsecurity.techtarget.com/definition/CISO-chief-information-security-officer (January 2019)

[18] AlientVault's open-source SIEM: OSSIM. Available at: https://www.alienvault.com/products/ossim (January 2019)

[19] M. Ramachandran and Z. Mahmood, Requirements Engineering for Service and Cloud Computing. Cham: Springer International Publishing, 2017.