dominoes
smart distribution grid

DOMINOES – DELIVERABLE

D2.6 Design and Implementation of a Data Security Framework

This project has received funding from the European Union's Horizon 2020 research and innovation programme under **Grant Agreement No. 771066.**

Deliverable number:	D2.6
Due date:	31.07.2019
Nature[1]:	R
Dissemination Level[1]:	PU
Work Package:	WP2
Lead Beneficiary:	UoL
Contributing Beneficiaries:	EDPD, VPS
Reviewer(s):	ISEP

[1] **Nature:** R = Report, P = Prototype, D = Demonstrator, O = Other
Dissemination level PU = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)
Restraint UE = Classified with the classification level "Restraint UE" according to Commission Decision 2001/844 and amendments
Confidential UE = Classified with the mention of the classification level "Confidential UE" according to Commission Decision 2001/844 and amendments
Secret UE = Classified with the mention of the classification level "Secret UE" according to Commission Decision 2001/844 and amendments

Version	Date	Description
0.1	01/09/2018	Initial outline by (UoL)
0.2	06/11/21018	Update to section 2 by (UoL)
0.3	05/02/2019	Update table of contents (UoL)
0.4	14/03/19	Section 2 added (All)
0.5	29/04/2019	Section 3 added (All)
0.6	16/05/2019	Section 4 added (All)
0.7	20/05/2019	Executive summary added (UoL)
0.8	27/05/2019	Section 1 introduction added (UoL)
0.9	31/05/2019	Section 5 conclusions added (UoL)
1.0	11/06/2019	Draft ready for internal review (All)
1.1	18/06/2019	Corrections based on Zhou review
1.2	29/07/2019	Corrections based on ISEP review

Authors

Nebrase Elmrabit, University of Leicester (UoL)

Huiyu Zhou, University of Leicester (UoL)

Nuno Medeiros, EDP DISTRIBUIÇÃO (EDPD)

Eduardo Boratto, EDP DISTRIBUIÇÃO (EDPD)

Jorge Landeck, Virtual Power Solutions (VPS)

Reviewers:

Omid Abrishambaf, Instituto Superior de Engenharia do Porto (ISEP)

Fernando Lezama, Instituto Superior de Engenharia do Porto (ISEP)

Executive Summary

This deliverable (D2.6) is a part of Task 2.5 to present the DOMINOES cybersecurity architecture. The architecture proposed in this report aims to ensure that the DOMINOES platform and its clients are protected from any potential cybersecurity threats.

To achieve a secure implementation of the DOMINOES platform, this document includes a detailed description of the current data protection regulations, the existing smart grid cybersecurity guidelines and standards, the effective smart grid cybersecurity measures, and the DOMINOES cybersecurity challenges. They are followed by the DOMINOES cybersecurity architectures, data security and privacy objectives, and data classifications and cybersecurity threat landscape. At the final stage of this deliverable, a set of recommendations are mapped to the DOMINOES security architecture layers, and a brief discussion on security tools requirements.

In summary, this deliverable reports the architecture and design of the data security framework for the DOMINOES platform.

List of Acronyms

AAA	Authentication, Authorisation and Accounting
API	Application Programming Interface
C&C	Command and Control
CSIRTs	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial-of-Service
DoS	Denial-of-service
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operator
DSP	Digital Service Providers
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
H2M	Human to Machine
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Mechanism Protocol
ICT	Information and communications technology
IDS	Intrusion Detection Systems
IKE	Internet Key Exchange
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Protection Systems
IPsec	IP security
IT	Information Technology
LFI	Local File Inclusion
M2M	Machine to Machine
MAC	Media Access Control

NIST	National Institute of Standards and Technology
NMAP	Network Mapper
NTP	Network Time Protocol
NVD	National Vulnerability Database
OES	Operators of Essential Services
OpenVAS	Open Vulnerability Assessment System
OT	Operational Technology
OWASP	Open Web Application Security Project
P2P	Peer to Peer
PKI	Public key Infrastructure
RSA	Rivest, Shamir, and Adleman
SABSA	Sherwood Applied Business Security Architecture Framework
SCADA	Supervisory control and data acquisition
SEGRID	Security for Smart Electricity GRIDs
SGTF	Smart Grid Task Force
SPARKS	Smart Grid Protection Against Cyber Attacks
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
TCP SYN	Transmission Control Protocol Synchronized Packet
TLS	Transport Layer Security
TSO	Transmission System Operators
UDP	Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WP	Work Package
XSS	Cross-site Scripting
XXE	XML External Entity

1 Introduction

The increasing demand of using smart grid infrastructure and the future of the implementations of the next generation power systems, known as peer to peer energy trading, (P2P), has led of increasing the challenges in reducing the cybersecurity threats risk levels, and maintaining the privacy issues within the smart grid [1]. To achieve this ambitious target, in the earliest stages of any projects, such as the DOMINOES project, we have to set a clear vision of the current cybersecurity standards, recommendations, controls and threats.

The DOMINOES smart grid platform, like any other platform, can be a target of cyber-attacks from internal users, external actors or from its clients. Therefore, a cybersecurity architecture for the DOMINOES project will be defined in this deliverable and will serve as a basis for the implementation of the security controls to this project's use cases. This will lead to reducing the number of cybersecurity vulnerabilities in the platform and to ensure clients' privacy and no disruption of the electrical supply based on cyber-attacks.

1.1 Purpose and Scope of the Deliverable

The purpose of the present deliverable is to introduce the high abstraction level architecture of the cybersecurity framework for the DOMINOES platform. It comprises the existing regulations and standards and provides a list of recommendations and requirements that are mapped to the DOMINOES ICT architecture (reported in D1.4). This will help our partners in the related tasks of ensuring a secure design and implementation of the project platform and its environment, to allow potential DOMINOES customers to trade energy securely.

In the DOMINOES project, a number of cybersecurity objectives are considered:

- Maintain confidentiality of measurements, users' data and system parameters used in each operator.
- Protect and segregate, appropriately, information from all the stakeholders involved.
- Protect the DOMINOES platform from current and future threats.
- Ensure the good and consistent operation of the whole system.
- Maintain integrity of communication information between operators in the network.
- Prevent tampering and data manipulation.
- Ensure the availability of data.

1.2 Relationship to other Deliverables

This report is based on WP1 D1.2, which represents the initial DOMINOES ICT reference architecture design, and the cybersecurity challenges in the smart grid. Also, in this deliverable, we consider the ICT platform KPIs reported on the implementation plan for the validation environment on WP1 D1.4, and the WP6 D6.9 standardisation proposals year one were considered.

Further contributions that will have a direct link to this deliverable and cybersecurity will be in the WP3 – D3.6 by developing and implementing an anomaly detection component, which will help us to detect any potential cybersecurity attacks to the DOMINOES platform and its clients. Finally, in WP4 D4.2, we will perform penetration testing and validation activities for maintaining cybersecurity in all the use cases, to achieve the required objectives.

1.3 Structure of the Document

The remaining structure of the deliverable is as follows:

- Chapter 2 (following this introductory section) provides a comprehensive evaluation of our analysis regarding secure data handling, which covers the current data protection regulations and the existing standards and approaches for smart grid cybersecurity. Moreover, this section introduces a discussion related to the DOMINOES cybersecurity challenges.
- Chapter 3 introduces the DOMINOES platform data security architecture, which provides a set of data security and privacy objectives, DOMINOES platform data classification and a picture of the current and emerging vulnerabilities and threats to the DOMINOES platform.
- Chapter 4 provides a guideline of cybersecurity recommendations and requirements mapped to the proposed architecture that will be used for securing the DOMINOES platform.
- Chapter 5 concludes the deliverable.

2 Secure Data Handling

This chapter provides an assessment of the evaluation and analysis of the existing regulations (Section 2.1), and standards and methods (Section 2.2) for the smart grid cybersecurity and its privacy. A discussion is then generated which is related to the key DOMINOES cybersecurity challenge (Section 2.3).

2.1 Regulation

The regulatory environment for information management and security is undergoing a major transformation, as escalating privacy concerns bring the subject under new scrutiny. Although the energy sector is not an exception, it has some peculiarities – data protection shares the stage with other cyber-resilience issues, which consequently reflects on the way the regulations are developed. This section aims to discuss three important milestones for this regulatory context, each with a different approach: the General Data Protection Regulation [2], the NIS Directive [3] and the Network Code on Cybersecurity.

Two years after its publication in April 2016, the new European Union General Data Protection Regulation (GDPR) [2] was formally adopted on May 25th 2018. Many of the GDPR principles are similar to those in the previous Data Protection Directive (the 1995 Act), that specifies the rules for the protection of an individual's personal data in all EU organisations. However, the security principle from the previous Act has been replaced with integrity and confidentiality.

This particular change requires that personal data be handled in the manner that guarantees appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate measures. This includes the transfer, storage and processing of data, including data outside the EU borders.

Article 83 of the GDPR states that any organisation that fails to meet GDPR obligations can be charged a potential administrative fine of up to €20 million or 4% of the annual global turnover of the previous year, whichever is higher, creating additional pressure on its compliance. The GDPR requires organisations to implement "Data protection by design and by default", aiming to achieve end-to-end data protection throughout its lifecycle:

- Data protection by design consists of considering data protection and privacy from the earliest stages of any system or process throughout its lifecycle, in order to meet GDPR requirements and protect the rights of data subjects.

- Data protection by default intends to ensure that technical controls are in place to limit the amount of personal data to be processed, so that data is not collected or retained beyond what is strictly necessary.

A checklist has been created by the UK Information Commissioner's Office [4] to help organisations to make self-assessments regarding GDPR's Article 25 (1) and Article 25 (2), that specify requirements for data protection by design and by default, respectively. Complementarily, the progressive adoption of smart grids and smart metering systems creates new risks for data subjects, with the potential to impact on different areas, previously not present in the energy sector (e.g., price discrimination, profiling for behavioural advertisement, taxation, law enforcement access, household security).

The Expert Group 2[2] of the Smart Grid Task Force (SGTF) [5], under the mandate of DG Energy, published a Smart Grid Data Protection Impact Assessment (DPIA) template. The template is an evaluation and decision-making tool which helps entities planning or executing investments in smart grids, to identify and anticipate risks to data protection, privacy and security, whilst providing guidance to help ensure the fundamental rights to protection of personal data and privacy. The NIS Directive [3], on the other hand, is more holistic and also the first piece of EU-wide cybersecurity legislation, but applies only to Operators of Essential Services (OES) and Digital Service Providers (DSP), with the goal of promoting a culture of risk management and ensuring that the most serious incidents are reported. It constructs:

> *"A set of unified network and information security rules that require regulatory obligations in coordinating national cybersecurity policies and incident response. This Directive provides legal measures to improve the level of cybersecurity and targets at identifying good practices for the entire organisation to follow*" D6.9 DOMINOES.

Its main pillars consist of creating cybersecurity capabilities individually for each of the member states (e.g., by establishing national Computer Security Incident Response Team - CSIRTs), fostering cross-border collaboration between EU countries and imposing constant supervision of critical sectors. Being an EU directive, every member state has to elaborate national legislation, which follows or 'transposes' the directive, and it is also necessary to explicitly identify the OES and DSPs subjects to the obligations imposed. Although it is up to each member state to determine the operators of essential services with an establishment on their territory, Annex II already identifies the electable types of entities, and electricity companies such as Distribution System Operators

[2] EG2 - responsible for regulatory recommendations for privacy, data protection and cyber-security in the Smart Grid Environment. URL: https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force

(DSO), Transmission System Operators (TSO) and Suppliers are first on the list. Thus, even though there is no way to guarantee that all players from the energy sector will be regarded as OES, the sector is definitely under the scope of the directive and its requirements.

As an additional attempt to increase the cybersecurity maturity level from transmission and distribution system operators, a proposal for secondary legislation, the Network Code on Cybersecurity, was submitted to the European Commission in December 2018. It resulted from a request made by the European Commission under the scope of the SGTF, to prepare the ground for sector-specific rules on demand response, energy-specific cybersecurity and common consumers' data format, focusing particularly on the electricity market. The proposal of a Network Code on Cybersecurity was then developed by the SGTF Expert Group 2, aiming to:

- Protect the energy systems based on current and future threats and risks;
- Support the functioning of the European society and economy in a crisis situation;
- Create trust and transparency for cybersecurity in the supply chain for components and vendors used in the energy sector;
- Harmonise maturity and resilience for cybersecurity across the EU with a defined minimum level, while favouring higher maturity.

The proposal contains recommended security requirements, a structure to identify different levels of maturity and supportive elements to assist in implementing controls and minimum-security baselines. Complementarity among the three approaches (i.e., the General Data Protection Regulation [2], the NIS Directive [3] and the Network Code on Cybersecurity) is an important takeaway from the current regulatory framework. To tackle the new data privacy challenges, brought by digital transformation and smart grids, it is not enough to look at data protection measures individually – the whole cybersecurity framework, governance and maturity have to be assessed.

2.2 Existing Standards and Methods for Smart Grid Cybersecurity

In this section, the current standards and measures for smart grid cybersecurity will be discussed, that were presented by different sources (EU projects and research papers).

2.2.1 Standards and Guidelines for Smart Grid Cyber Security

In the DOMINOES project, we recognise that adopting security standards play a critical role in the energy sector and is one of the most effective solutions for mitigating the risk of cybersecurity threats in any enterprise. In section 4 of deliverable D6.9 (Standardization Proposals Year 1 report), we discuss cybersecurity standards by surveying several EU standards and examining other related international standards and guidelines. We follow with an evaluation of all existing standards, regulations and guidelines published in the society, to decide what standards should be used for smart grid cybersecurity systems. Recommended standards and solutions, from a security point of view, were presented in D6.9, to address security requirements. The table below describes the standards that are recommended for implementation in this project.

Table 1 Standards Recommendations

Standard & Technology names	Recommendations
TLS (IETF FRC 5246)	This standard can be used to ensure confidentiality and integrity in a centralised architecture. The use of Public Key Infrastructure (PKI) makes this standard difficult to deploy in a decentralised architecture with client authentication.
IEC 62351	Security in energy management systems: provides security recommendations for important protocols, most of them used mainly in the energy sector (includes IEC 60870-5, DNP3, IEC 60870-5-101 and IEC 60870-5-104).
NIST SP 800-82	Guide to Industrial Control Systems which defines the typical topology of SCADA systems, identifying threats and vulnerabilities and providing recommendations and countermeasures to mitigate these risks.

Furthermore, to the above recommendations, further suggestions are put forward:

- Each standard and technology shall implement a logging capability so that abnormal events can be recorded at any time.

- Each standard and technology are advised to follow ENISA recommendations with respect to cryptographic algorithms and key sizes. This helps avoid privacy issues. For example, for RSA algorithms, the key size is at least 2048 bits.

2.2.2 Smart Grid Cyber Security Measures

European Commission 2012/148/EU [6] provides guidance on a set of 10 common minimum functional requirements for developing a smart grid system to ensure the fundamental right to protection of personal data, as listed below:

- Provide readings directly to the consumer and any third party designated by the consumer.
- Update the readings referred to in point 1, frequently enough to allow the information to be used to achieve energy savings.
- Allow the operators to read data remotely.
- Allow the maintenance and control of the metering system via two-way transmission between the smart metering system and external networks.
- Update the readings frequently enough for the data to be used for network planning.
- Support advanced tariff systems.
- Allow remote on and off control of the supply and flow or power limitation.
- Allow data to exchange securely.
- Provide a fraud prevention system.
- Provide import, export and reactive metering.

SGTF EG2 [7] presented a set of recommendations and requirements for data handling, and safety to smart grid at the European countries. They grouped smart grid security measures into relevant domains, where each of these domains has a set of measures to mitigate the cybersecurity threats, as the table below explains [8]:

Table 2 Recommendations and Requirements [8]

Recommendations	Requirements
Security Governance & Risk Management	Information security policy, an organisation of information security, information security procedures, risk management framework, risk assessment, and risk treatment plan.
Management of Third Parties	Agreements with third parties, validating solutions and monitoring third party services against predefined acceptance criteria.
Secure Lifecycle	Security requirements analysis and specification, inventory of smart grid systems, secure configuration

	management of smart grid systems, secure configuration documentation, maintenance of smart grid systems, software/firmware upgrade of smart grid systems, disposal of smart grid systems, and change management.
Personnel Security	Personnel screening, security awareness training.
Incident Response & Information Exchange	Incident response capabilities, vulnerability assessment and treatment, and incident information sharing.
Audit and Accountability	Monitoring of smart grid information systems exchange, and protection of audit information.
Continuity of Operations	Continuity of operations capabilities and necessary communication services.
Physical Security	Monitoring physical access, physical security on third party premises.
Information Systems Security	Classification and disclosure policy, data security, account management, logical access control, secure remote access, and media handling.
Network Security	Functional and secure network segregation and secure network communications.
Resilient and Robust Design of Critical Core Functionalities and Infrastructures	Minimum exposure, resiliency, and safe interruption-continuity of operation.

The National Institute of Standards and Technology in the USA has the most comprehensive coverage of cybersecurity problems in the smart grid and is pretty mature and well-documented. NISTIR 7628 “Guidelines for Smart Grid Cybersecurity” [9] introduced the high-level security recommended requirements for the smart grid systems. They used 19 categories, with each category having a number of requirements (as shown in Table 3).

Table 3 NISTIR 7628 Recommendations [9]

Recommendations	Requirements
Access Control	Remote Access Policy and Procedures, Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Login Attempts, Information System Use Notification, Previous Login Notification, Concurrent Session Control, Session Lock, Remote

	Session Termination, Permitted Actions without Identification or Authentication, Remote Access, Wireless Access Restrictions, Access Control for Portable Devices, Use of External Information Systems, Control System Access Restrictions, Publicly Accessible Content, Passwords
Awareness and Training	Policy and Procedures, Security Awareness, Security Training, Records, Contact with Security Groups, Security Responsibility Training, Planning Process Training
Audit and Accountability	Policy and Procedures, Auditable Events, Content of Audit Records, Audit Storage Capacity, Response to Audit Processing Failures, Monitoring, Analysis, and Reporting, Analysis of Tools and Report Generation, Time Stamps, Protection of Audit Information, Audit Record Retention, Conduct and Frequency of Audits, Auditor Qualification, Audit Tools, Security Policy Compliance, Audit Generation, Non-Repudiation
Security Assessment and Authorization	Policy and Procedures, Security Assessments, Continuous Improvement, Information System Connections, Security Authorization to Operate, Continuous Monitoring
Configuration Management	Policy and Procedures, Baseline Configuration, Configuration Change Control, Monitoring Configuration Changes, Access Restrictions for Configuration Change, Configuration Settings, Component Inventory, Addition, Removal, and Disposal of Equipment, Factory Default Settings Management, Configuration Management Plan
Continuity of Operations	Policy and Procedures, Continuity of Operations Plan, Roles and Responsibilities, Continuity of Operations Training, Continuity of Operations Plan Testing, Continuity of Operations Plan Update, Alternate Storage Sites, Alternate Telecommunication Services, Alternate Control Center, System Recovery and Reconstitution, Fail-Safe Response
Identification and Authentication	Identification and Authentication Policy and Procedures, Identifier Management, Authenticator Management, User Identification and Authentication, Device Identification & Authentication, Authenticator Feedback

Information and Document Management	Policy and Procedures, Information and Document Retention, Information Handling, Information Exchange, Automated Labeling
Incident Response	Policy and Procedures, Roles and Responsibilities, Incident Response Training, Testing and Exercises, Incident Handling, Incident Monitoring, Incident Reporting, Investigation and Analysis, Corrective Action, Smart Grid Information System Backup, Coordination of Emergency Response
Smart Grid Information System Development and Maintenance	Policy and Procedures, Legacy Smart Grid Information System Upgrades, Information System Maintenance, Maintenance Tools, Maintenance Personnel, Remote Maintenance, Timely Maintenance
Media Protection	Policy and Procedures, Media Sensitivity Level, Media Marketing, Media Storage, Media Transport, Media Sanitization and Disposal
Physical and Environmental Security	Policy and Procedures, Physical Access Authorizations, Physical Access, Monitoring Physical Access, Visitor Control, Visitor Records, Physical Access Log Retention, Emergency Shutoff Protection, Emergency Power, Delivery and Removal, Alternate Work Site, Location of Information System Assets
Planning	Policy and Procedures, Information System Security Plan, Rules of Behavior, Privacy Impact Assessment, Security-Related Activity Planning
Security Program Management	Security Policy and Procedures, Security Program Plan, Senior Management Authority, Security Architecture, Risk Management Strategy, Security Authorization to Operate Process, Mission/Business Process Definition, Management Accountability
Personnel Security	Policy and Procedures, Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, Access Agreements, Contractor and Third-Party Personnel Security, Personnel Accountability, Personnel Roles
Risk Management and Assessment	Policy and Procedures, Risk Management Plan, Security Impact Level, Risk Assessment, Risk Assessment Update, Vulnerability Assessment

Smart Grid Information System and Services Acquisition	Policy and Procedures, Security Policies for Contractors and Third Parties, Life-Cycle Support, Acquisitions, Information System Documentation, Software License Usage Restrictions, User-Installed Software, Security Engineering Principles, Developer Configuration Management, Developer Security Testing, Supply Chain Protection
Smart Grid Information System and Communication Protection	Policy and Procedures, Communications Partitioning, Security Function Isolation, Information Remnants, Denial-of-Service Protection, Resource Priority, Boundary Protection, Communication Integrity, Communication Confidentiality, Trusted Path, Cryptographic Key Establishment and Management, Use of NIST Approved Cryptography, Collaborative Computing, Transmission of Security Parameters, Public Key Infrastructure Certificates, Mobile Code, Voice-Over-Internet Protocol, System Connections, Security Roles, Message Authenticity, Secure Name/Address Resolution Service, Fail in Known State, Thin Nodes, Honeypots, Operating System Independent Applications, Confidentiality of Information at Rest, Heterogeneity, Virtualization Techniques, Application Partitioning, Smart Grid Information System Partitioning
Smart Grid Information System and Information Integrity	Policy and Procedures, Flaw Remediation, Malicious Code and Spam Protection, Monitoring Tools and Techniques, Security Alerts and Advisories, Security Functionality Verification, Software and Information Integrity, Information Input Validation, Error Handling.

Therefore, several cybersecurity approaches were integrated into the smart grid systems based on the previous requirements and measures to mitigate the levels of cybersecurity threats. Guidelines for Smart Grid Cyber Security NIST 7628 [9], identifies the need for future Intrusion Detection Systems (IDS) tools with a deep contextual understanding of device operation to discover anomalous behaviours, that may lead to cybersecurity breaches. Smart Grid Protection Against Cyber Attacks (SPARKS) EU project [10] proposed a multi-attribute SCADA IDS using different techniques such as whitelist, state full analysis and machine learning, to detect anomalous behaviour on SCADA systems that use IEC 61850 protocol.

Another EU project aims to enhance existing vulnerability modelling tools, Security for Smart Electricity GRIDs (SEGRID) [11]. In their project, they managed to enhance the securiCAD tool, to be used against cyber-attacks in the smart grids. Piatkowska et al. [12], as a part of the Nobile Grid EU project, proposed a web-based application that supports the implementation of data impact assessment in the smart grid. This was based on the data protection impact assessment template for smart grid and smart metering systems, that has been recommended by the Smart Grid Task Force [5], and the checklist that has been created by the UK Information Commissioner's Office [4]. Tong et al. [13] proposed secure and unlikable data sharing mechanisms, which enable peer operators to outsource and share information without compromising their privacy, using light-weighted private key based encryption. Other approaches for smart grid infrastructure protection, that can be useful techniques to model the repeated interactions of the attacker and the protector, for the security analysis of emerging smart grids, is by applying Markov decision tools [14]. A new emerging Blockchain technology can be integrated to the smart grid systems to allow the exchange, verification and storage of data via a peer to peer transaction, without the need to rely on a central point, to ensure anonymity on the BlockChain platforms, where peers are identified using their public keys [1].

2.3 DOMINOES Cybersecurity Challenge

The smart grid's cybersecurity challenges are basically the same as the ones for the other information systems. In general terms, the information systems security, sometimes also called InfoSec as a shortened term, is the practice of several techniques to prevent the unauthorised access, usage, disclosure, inspection, recording, tampering, modification or destruction of physical or electronic data.

Smart grid systems can be subject to the same attacks as information systems. Depending on the attack, it can be performed in a direct mode, where the attacker has physical access to the target system or, alternatively, in an electronic mode where the attacker has means to access the target using the network. There are a number of different ways in which the smart grid components are attacked:

- Authentication attack – In this type of attacks, the attacker tries to trick the system's authentication mechanism to gain access, without having any valid credentials (i.e. username/password pair or digital certificate). One form of doing this is to brute-force the authentication system in order to gain access.
- Authorisation attack – This form of attack implies that the attacker already has a means of authentication into the system, even if in an unprivileged "guest" account, and then tries to gain illegitimate privileges over resources on the system.

- Breaking into a system – In this type of attack, the attacker gains access to the resources which are not accessible to him, by means of illegitimate authentication and/or by gaining access levels greater than s/he has.
- Eavesdropping attack – In this type of attack, the attacker illegitimately gains access to information either by chance or purpose [15].

The high-level smart grid's cybersecurity requirements, identified by all the organisations working on the development of security requirements, include: availability, integrity, and confidentiality. These requirements are also relevant to other generic information systems and are ensured by a set of practices and technologies that aim to prevent the unauthorised access, usage, disclosure, inspection, recording, tampering, modification or destruction of physical or electronic data. Yet, the smart-grid and DOMINOES, as one of its components, present a set of specific challenges, which are described next.

2.3.1 Heterogeneity

The heterogeneity and complexity of the smart-grid, in terms of devices, communications, and deployment, raises one of the main challenges when it comes to guaranteeing an end-to-end secure data transmission. The difficulties arise, firstly, from the lack of standards or the fact that different sub-systems may use different standards to comply with various regulations and best practices that prioritise slightly different security requirements. Secondly, some of the field devices (e.g. sensors, actuators, meters, controllers, and gateways) implement proprietary (legacy or "old" standard) communication protocols with weak or no security features at all and have limited computational capabilities, which prevent the implementation of more secure alternatives. These constraints are particularly noticed in the implementation of authentication and encryption mechanisms that are fundamental to guarantee integrity and confidentiality [16]. In fact, the development and standardisation of lightweight cyphers and key management procedures for smart-grid devices is extremely important.

2.3.2 Internet of Things

Smart-grid applications benefit from using the emerging Internet of Things (IoT) technologies, including architecture paradigms and communication protocols. These technologies usually (or can easily) incorporate strong authentication and encryption mechanisms which simplify the implementation of secure data channels [17]. However, since these protocols are part of the large family of the Internet (and TCP/IP) protocols the resulting systems become more vulnerable to well-known cyber-attacks (e. g. denial-of-service) which poses a significant challenge. Protection against these general threats includes the installation of appropriate tools and an obligation to keep all systems updated and monitored.

2.3.3 Big Data

DOMINOES and generic smart-grid application may, to a lesser extent, depend on the collection, storing, and processing of large amounts of data. This data includes end-users' personal details, energy consumption and production time series, distribution network operational data, and market prices and transactions that can be stored on a single database, or more frequently, on a distributed set of databases [18]. The challenge here is in keeping these databases secure to preserve the privacy of the end-users, protect the operation of the distribution network, and prevent market manipulation. Furthermore, strong authorisation and aggregation mechanisms must be implemented, considering the potential risk in disclosing energy usage patterns that may be considered sensitive for individual end-users.

2.3.4 Peer-to-Peer (P2P)

P2P energy trading clients (sellers and buyers) are communicating directly with each other, to negotiate unit prices, exchange of contract, make or receive payments, and other processes. This business architecture may lead to a numerous number of security vulnerability and privacy issues that could affect the DOMINOES platform and its users [1]. The main challenge will be to ensure the environmental integrity by guaranteeing no fake contracts, double spending of energy or money. Also, ensuring the confidentiality of users' identities, like personal information and locations. Finally, ensuring the availability of the services when the clients request it.

2.3.5 Trust

One last challenge for DOMINOES as a market platform, concerns the protection against impersonation and the definition of non-repudiation mechanisms. If authentication mechanisms are important for field devices, as stated, they are even more important for entities (persons or systems) that participate in the market, where fairness and reputation must be preserved at all costs.

3 DOMINOES Data Security Architecture

There are several available security architectures that the DOMINOES project might choose to deploy in the enterprise levers, to protect the DOMINOES platform from any malicious or non-malicious security threats. The implementation of cybersecurity architectures or frameworks is subject to several organisational factors such as: skills and experience, budgets, scope, and risk appetite.

Several well-known security architectures are available to deploy, where each of them has its own objectives. The list below includes the security enterprise architecture frameworks that can be considered to use in DOMINOES platform:

- Open Group Architecture Framework (TOGAF).
- Open Enterprise Security Architecture (O-ESA).
- ISO/IEC 27000 Family of Information Security Standards.
- Sherwood Applied Business Security Architecture Framework (SABSA).
- IBM Security Framework.
- Control Objectives for Information and Related Technology (COBIT).

In the DOMINOES project, we agreed to use the SABSA as the starting point for the DOMINOES Cybersecurity Architecture. This is due to the fact that the SABSA applies throughout the entire lifecycle of the project from the business view to security service management of the solutions delivered. The diagram in Figure 1 shows the SABSA operation of the controls.

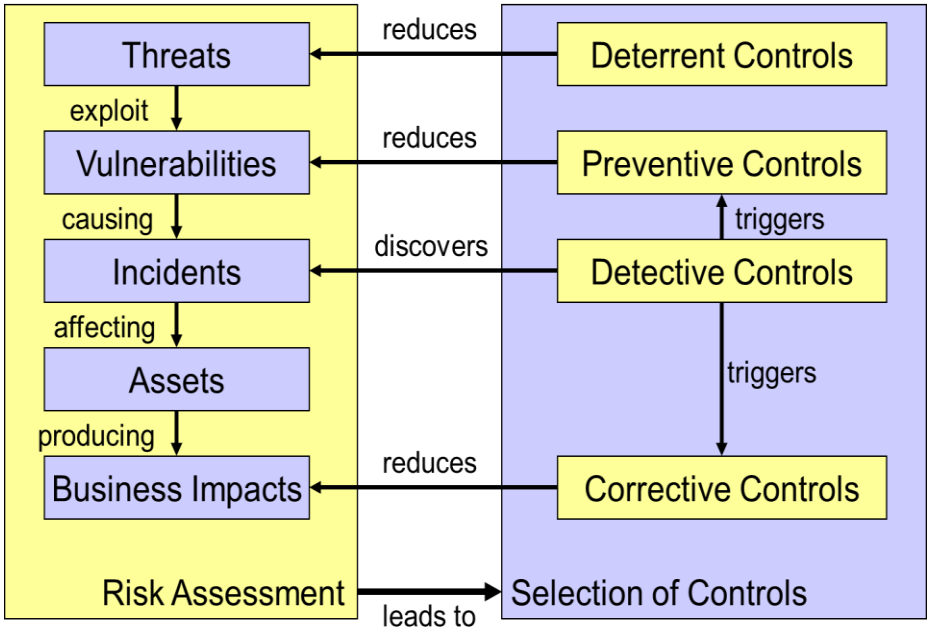

Figure 1 SABSA Operation of Controls by David Lynas [19]**.**

Moreover, SABSA is a free-use and open-source security architecture development and management method. Table 4 summarises the features and advantages of SABSA.

Table 4 Features and Advantages of SABSA [20]

FEATURE	ADVANTAGE
Business-driven	Value-assured
Risk-focused	Prioritised & proportional responses
Comprehensive	Scalable scope
Modular	Agility - ease of implementation & management
Open Source (protected)	Free use, open source, a global standard
Auditable	Demonstrates compliance
Transparent	Two-way traceability

In the next sections, we will define the DOMINOES security architecture by setting the data security and privacy objectives and data classification within the platform. We will also discuss the current and emerging vulnerabilities and threats to DOMINOES infrastructure. Finally, we define the SABSA security architecture layer.

3.1 Data Security and Privacy Objectives

Understanding data security and privacy objectives is the first requirement to successfully implement a security architecture. Ideally, the objectives should be broad, clear, and take into account business requirements, all the stakeholders involved, system functionalities and risk exposure. For the DOMINOES context, the following high-level objectives were conceptualised:

- Maintaining confidentiality of measurements, users' data and system parameters used in each operator.
- Protecting and segregating, appropriately, information from all stakeholders involved.
- Protecting the DOMINOES platform from current and future threats.
- Ensuring the good and consistent operation of the whole system.
- Maintaining the integrity of communication information between operators in the network.
- Preventing tampering and data manipulation.
- Ensuring the availability of data.

3.2 Data Classification

An effective and comprehensive design of a data security framework must begin with systematic identification and classification of the datasets that will be handled by the system or platform. In this way, efficient and adequate security controls can be defined for (applied to) each data set depending on the assigned classification. For the definition of the DOMINOES security framework, this classification should be based mainly on the importance of the data for each stakeholder and on the legal and regulatory requirements (GDPR specifically). Due to the mixing of individual and organisational stakeholders, the value that each one assigns to the data may range from keeping it private to a business (loss of revenue) cost. In other words, the value is either stressed by the sensitivity (privacy) of the data or its criticality (timeliness and accuracy).

At this stage, the following, extensively used classification levels, were selected to label the datasets, considering that privacy is the chief security objective:

- Public – information that can be made available freely to the public.
- Operational – information that is generally available to any registered user or platform manager.
- Restricted – information that is sensitive for any stakeholder (e.g. personal data like name, email, and address; data from which personal habits and preferences can be inferred; organisational data involving business transactions or data from which business options and strategies can be inferred).
- Confidential – information that is highly sensitive for any stakeholder (e.g. personal biometric data; IPR or business secrets).

Table 5 identifies and classifies the primary datasets that will be exchanged, stored, or shared by DOMINOES:

Table 5 Data Classification

Information exchanged			
ID	**Designation**	**Description**	**UC**
1.0	Account Settings	Credentials: username (email) and password Account id Invoice details: name, address, fiscal id TSO/DSO details: contract ids (meters ids) Forecast details: generation (unit id, unit type, power, location, installation, technology), consumption (load id, load type, power, operational restriction), timing details (resolution, interval)	Restricted
2.0	Production/ Consumption Forecasts	Production/Consumption: Forecast data (id, date-time, unit id, power)	Restricted

3.0	Procured/ Offered/ Demanded Provisioned Energy/Flexibility	Energy/Flexibility: Procured/Offered/Demanded/Provisioned program (date-time, session, power, price)	Restricted
4.0	Technical Validation	Network power flow profile (date-time, min power, max power)	Operational
5.0	Metering Data	Metering data (date-time, imported power, exported power)	Restricted
6.0	Market Data	Price (date-time, session, energy price, flexibility price) Aggregated analytics	Public
7.0	Settlement and Invoicing	Settlement: account id, deviation data (time, power, cost) Invoicing: account id, periodic financial results	Restricted
8.0	Get Auditing Data	System activity, network, and security logs	Operational

3.3 Cybersecurity Threat Landscape

In D1.2, a DOMINOES system architecture was introduced. Also, the data classification and information exchange processes were identified in the previous sections and also in D2.4. The next stage is to get an overall picture of the current and emerging vulnerabilities and threats to the DOMINOES infrastructure. Vulnerability is the weakness of an asset that is inherent in every smart grid infrastructure, application and service. A threat refers to everything that has the potential to cause serious harm or damage to the smart grid infrastructures, applications and services. An attack means the action taken to exploit the vulnerability or to create a threat to the smart grid infrastructures, applications and services. To summarise, a threat is a potential event that can adversely affect an asset, whereas a successful attack exploits vulnerabilities in your system [21].

We become more vulnerable over time; the more we get connected, the more vulnerable we become. Through analysis on the publicly known cybersecurity vulnerabilities databases such as the Common Vulnerabilities and Exposures index (CVE) and the National Vulnerability Database (NVD) by NIST, we found that there are more than 100,000 vulnerability entries, where an organisation's assets are vulnerable to cybersecurity breaches. Due to the large number of threats, only the most well-known threats will be discussed in this report. However, the systems will remain vulnerable to other types of cybersecurity threats, which may include those which are yet to be discovered by cybersecurity experts.

3.3.1 THREAT TYPES

Different categories of threats and vulnerabilities have been discussed. In the seventh series of the European Union Agency for Network and Information Security (ENISA) Yearly Report 2018 [22], a study was conducted on the most known cyber threats (see Figure 2). The top ten threats from their report are discussed below:

3.3.1.1 Malware

Malicious software ("malware") refers to software programs designed to harm or to perform unauthorised actions to the organisation's ICT assets. Malware application can perform a variety of security breaches, including copying, modifying or deleting sensitive data, controlling core computing functions and monitoring users' activity without their permission. Malware damages the target systems once it is delivered in some way into a target's devise [23]. This malware affects the smart grid environment, as all the services depend on the installed software, codes, and applications on the ICT infrastructure. Viruses, Worms, and Trojans may affect the operation of all the smart grid components by infecting devices with a virus, distributing worms using the network or other media, and enable unauthorised access to smart grid systems via Trojans. Also, Backdoor, which can be a hidden access facility to smart grid devices, made by vendors, without the company's knowledge and authorisation [24].

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	⊃	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	⊃	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	⊃	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 2 Overview and Comparison of the Current Threat Landscape in 2017 and 2018 [22].

3.3.1.2 Web-Based Attacks

Web-based attacks refer to the web services infrastructure attacker, use to exploit their target. Web-based threats are expected to increase as more exploitation techniques rely on it [22]. As a delivery mechanism, during the weaponisation, delivery, and exploitation phases on the kill chain model. Web-based attacks involve a variety of security breaches, including effects on the victims' availability, a breach of confidentiality and integrity of an organisation's data.

The P2P smart grid is widely dependent on web services to manage clients, services and functions. This will put the smart grid infrastructure under the attacker's reach by using a method such as browser exploits, drive-by downloads, malicious URLs, and water-holing, to attack the DOMINOES infrastructure [22].

3.3.1.3 Web Application Attacks

Web application attacks are a cybersecurity branch that deals specifically with security surrounding websites, web applications and web services such as Application Programming Interface (APIs). The Open Web Application Security Project (OWASP) [25] categorised the top 10 critical web application security risks that harm any organisation's smart grid infrastructure. The list includes:

- Injection.
- Broken authentication.
- Sensitive data exposure.
- XML External Entities (XXE).
- Broken access control.
- Security misconfiguration.
- Cross-Site Scripting (XSS).
- Insecure deserialization.
- Using components with known vulnerabilities.
- Insufficient logging and monitoring.

3.3.1.4 Phishing

Phishing is a type of social engineering attacks that attempt to obtain sensitive information such as usernames and passwords by masking as a truthful entity in electronic communication. Typically, this will be as an attachment file or URL delivered to the victim's machines via spoofing email, social media, SMS, or instant messaging. Once the user opens the malicious attachment or malicious URL, it will direct the request to legitimate-looking phishing pages, to steal the user's credentials, without the user's knowledge [26] . For the smart grid, phishing is one way of committing fraud, by tricking DOMINOES customers via emails in order to extract login credentials or account

information. Cybercriminals will then try to rip-off the customer and steal money or power balance [27].

3.3.1.5 Denial of Service

Denial of Services (DoS) and Distributed DoS attacks (DDoS) are one of the most known attacks, that target the availability factor of the main security goals. Attackers attempt to prevent legitimate users from accessing a specific resource or service. DoS attacks are usually accomplished by flooding the target victim with superfluous traffic, originating from one source for a DoS attack, but from different internet sources for a DDoS attack [28]. In the P2P smart grids, availability of information is a key aspect for allowing energy trading. Attackers can isolate some of the connected components from the network, including smart meters, networking devices, communication links, and utility business servers [29], which may result in the instability of the smart grid.

3.3.1.6 Spam attack

Spam attacks are usually unwelcome commercial messages in the form of e-mails, text messages, social networks, and internet postings, sent to a large number of addressees or posted in a large number of places. Email spam could include a link to a fake website that appears legitimate. For the P2P smart grids, this type of attacks may affect messages between the clients, and between the server providers and clients. Also, Spam could be a serious security threat to the DOMINOES platform as it can be used to deliver malwares, viruses, phishing attacks, Trojan horses and worms [30].

3.3.1.7 Botnets

A botnet refers to several devices connected over the internet such as computers, smartphones or IoT devices, and controlled remotely via command and control (C&C) software. Attackers can use a botnet to perform a DDoS attack, send spam, or allows the attacker to access the device (bot) and its connection to steal data [31]. Newer botnet architectures operates over a P2P network to communicate between C&C and bots [31]. A P2P smart grid infrastructure could be a target for hackers to install their bots and use smart grid infrastructure to launch their malicious activities. Figure 3 illustrates how the botnet works.

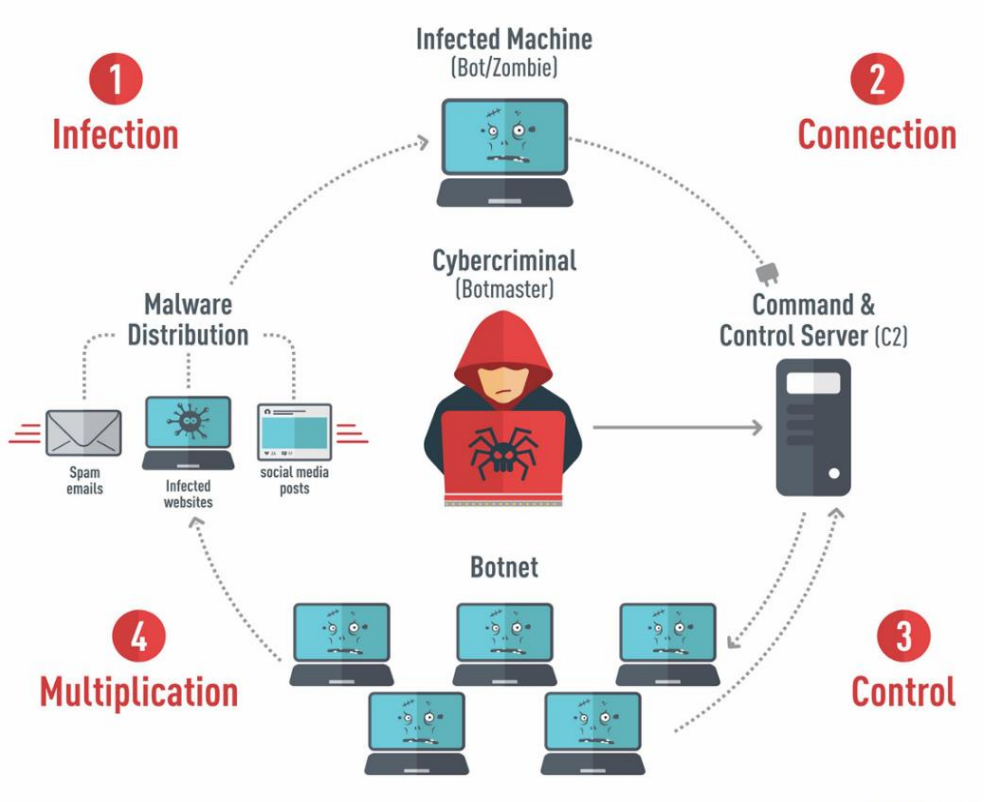

Figure 3: How the Botnet Works [32]

3.3.1.8 Data Breaches

A data breach is not a type of cybersecurity attack. However, it is a security incident which relates to the outcomes from other cybersecurity threats, and is still a malicious attempt [22]. A data breach will lead to confidential data, such as intellectual property or personal data, being exposed or leaked to an unauthorised party. In the DOMINOES environment, data breaches could have a direct impact on our own intellectual property and a client's personal data, if the procedures and the mitigation actions of the other cyber threats are not followed.

3.3.1.9 Insider Threat

Insider Threat refers to any malicious or unintentional activities that cause damage to an organisation's IT and network infrastructure, applications, or services. Those responsible identities may include employees (current or former), contractors, subcontractors, suppliers, or trusted business partners and anyone who has or has had authorised access to the organisation's IT assets. Moreover, it poses a significant negative impact on the information security elements (confidentiality, integrity, and availability) of the organisation [33]. Insider attacks could impact a smart grid in many ways based on insider categories such as: insider IT sabotage, insider IT fraud, insider theft of intellectual property, insider social engineering, unintentional insider threat incidents and an insider in cloud computing.

3.3.1.10 Physical Manipulation/Damage/Theft/Loss

A physical attacks is a cybersecurity threat whereby the attacker has physical access to the victim. However, the number of physical attacks is considered small, when compared with other types of attacks. Physical attacks can affect the smart grid at different levels. From the smart meter device within the client premises, where the client has physical access to the device, the client can analyse the smart device and possibly read out the firmware, the system configuration, credentials and key material. Using gathered information, the attacker can gain access to remote systems over the PLC network to the primary services hosted on DOMINOES platforms sites [34].

3.3.2 THREAT AGENTS

In the DOMINOES platform, it is essential to recognise which threats emerge from which threat agent group, as this will help us to understand the motivation and assess the capabilities of actors. The term “threat agents” is used to indicate an individual, group, organisation, or government from which a threat can manifest. Moreover, threat agent categories cover unintended incidents, accidents and natural disasters, which are compared with the term “attacker” which suggests malicious intent only. Table 6 shows the classification of threat agents, including descriptions.

Table 6 Threat Agent Classification [22]

Threat Agent	Description
Cybercriminals	This threat agent is the most active group in cyberspace; cybercriminals are usually individuals or groups of highly skilled people who commit malicious cyber activities for their financial gain.
Insiders	An individual who has authorised access to an organisation's assets to use their access for unauthorised purposes. This could be malicious or unintentionally insider.
Nation States	Nation State Actors (cyber army) work for a governmental organisation to cyberespionage, interrupt, or cause harm to the target governments, organisations or individuals.
Corporations	This type of actor is more organised as it is run by organisations that have technology and experts to launch cyber-attacks for financial gain or to obtain competitive knowledge from competitors.
Cyber- terrorists	Are individuals or groups motivated by religious, ideological or political inspiration, with various skill levels, resulting in harm to their victims including countries, critical infrastructures, organisations, and individuals.

3.3.3 Attack Vectors

The P2P smart grid will be implemented over the current public network (internet), to connect clients. This will have a potential cybersecurity risk to the DOMINOES platform and its customers, as the number of attack vectors is increased. An attack vector is a route that threat agents use to exploit victims' vulnerabilities. Attack vectors include exploiting kits, malicious e-mail attachments or URLs, pop-up windows and social media messaging services. Figure 4 shows the different routes a threat agent can use to exploit the target victim [25]. Also, Table 7 shows the threat types and their attack vectors.

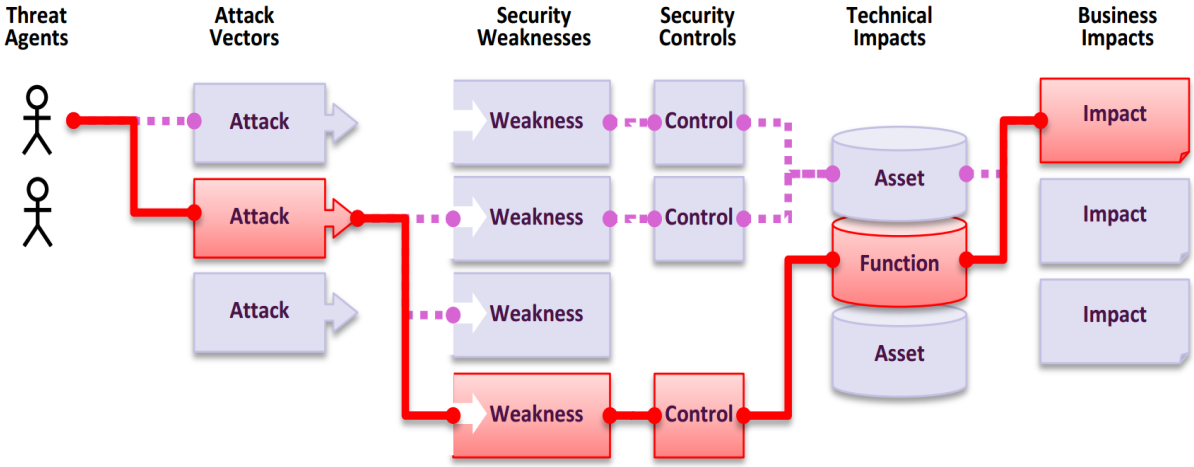

Figure 4 Exploitation Path [25]

Table 7 Threats and their Attack Vectors [22]

Threat	Attack Vectors
Malware	Email compromise, exploit kits, malvertising, drive-by downloads and strategic website compromise.
Web-Based Attacks	Browser exploits, drive-by downloads, malicious URLs, water-holing.
Web-Application Attacks	SQLite attacks still, Local File Inclusion (LFI), Cross-site Scripting (XSS), Cross-site request forgery, and other.
Phishing	Email compromise, mobile APP.
Denial of Service	User Datagram Protocol (UDP) Attack, Transmission Control Protocol Synchronized Packet (TCP SYN) Attack, Internet Control Mechanism Protocol (ICMP) Attack, Network Time Protocol (NTP) Amplification Attack, and others.

Spam	Email compromise.
Botnets	Exploit kit.
Data Breaches	SQL Injections Attack, phishing attacks, insider threat, and physical theft and loss.
Insider Threat	An authorised user (employee, contractor, and clients), and human errors.
Physical manipulation/ damage/ theft/loss	Physical actions (physical loss, physical theft).

3.4 DOMINOES Security Architecture

The main goal of this section is to define a security architecture robust enough to ensure the achievement of established security objectives, but sufficiently generic to encompass variations in the application architecture itself. In order to meet this purpose, the adopted methodology was developed, very much in line with the SABSA [20], whose main components include:

Table 8 Sherwood Applied Business Security Architecture

Point of View	Security Architecture Layer
Business	Contextual
Architect	Conceptual
Designer	Logical
Constructor	Physical
Technician	Component
Manager	Management (Operational)

Dividing in layers helps to propagate security objectives top-down across different stakeholder realms, starting with business requirements (context) down to security operations.

3.4.1 Contextual Layer

Contextual layer or the business view is the initial phase for the implementation of the DOMINOES architecture. This phase includes business objectives, goals and strategies. This phase aims to answer the following questions from the SABSA Matrix[3] [20]:

- Assets: What type of systems platform and its purpose? (Business Decisions)
- Motivation: Why using the selected platform? (Business Risk)
- Process: How will it be used? (Business Processes)
- People: Who will use it? (Business Governance)
- Location: Where will it be used? (Business Geography)
- Time: When will it be used? (Business Time Dependence)

The contextual layer provides background and high-level functional objectives that ought to be considered when designing security controls. Ultimately, the goal of the architecture is to ensure that both business and security objectives are met.

As the functional aspects are not the focus of this deliverable and considering that they have already been discussed thoroughly in previous sections, the following stage is to identify the risks associated with the application architecture, and how those could be mapped to business requirements to shape the model's next layer (conceptual).

3.4.2 Conceptual Layer and Critical System Components

When defining the system security architecture, the conceptual layer establishes concepts and principles that will be used in the following steps. Assessing risk in the DOMINOES application architecture begins with a high-level identification of critical components for service delivery. From the modules identified and represented in Figure 5, three main groups can be distinguished in terms of potential disruptive impact.

- Wholesale Market Module, Local Market Module, Contract & Tariff Management and Data Management: As they represent the core of system operations, any disruption would mean real-time impact for system availability. Furthermore, all the information exchange is governed by the data management module and is stored in the global database. It is therefore essential to impose strict security requirements to meet the privacy and data protection objectives.
- User Interface Modules: These components have the highest level of exposure, as they are the interface between the system and the real world. Thus, associated

[3] The SABSA Matrix showing the vertical analysis of each horizontal layer by applying the six critical questions: What? Why? How? Who? Where? When?

risks are directly related to the integrity of information – ideally, they would have to be tamper-proof, to ensure that requests from users are trustworthy and reliable.

- DOMINOES API: Providing a "communication bus" which connects all the components, the API itself is critical to module interaction, and must be then considered as an additional layer of the security architecture.

These high-level risks will have to be considered later as groundwork when working in lower layers (logical, physical, component) to define specific security requirements for devices and networks.

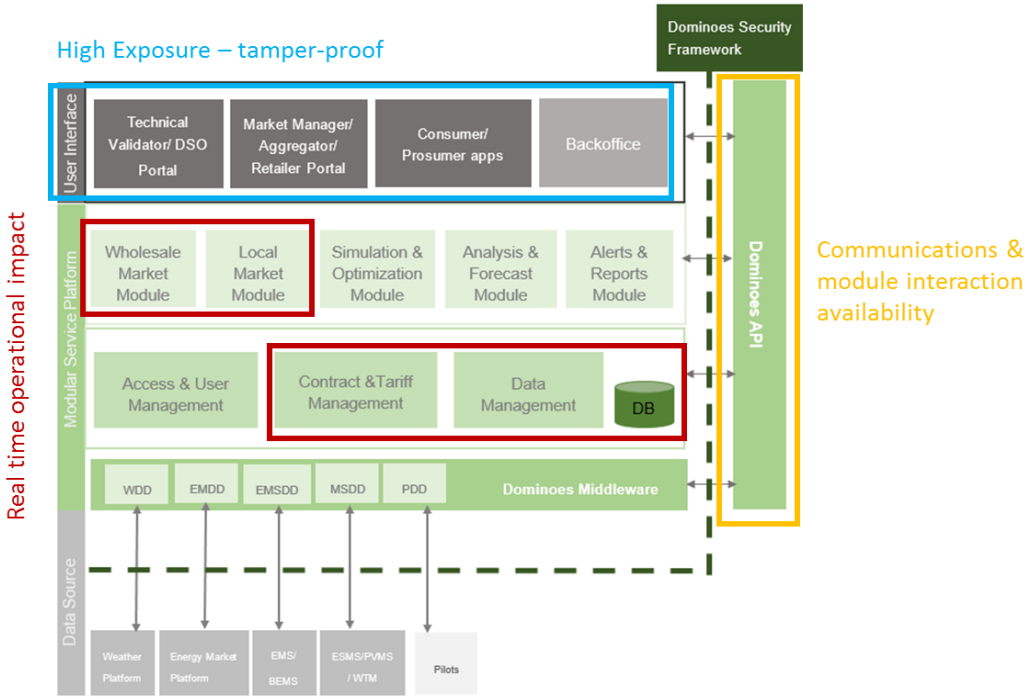

Figure 5: DOMINOES Application Architecture

At this moment, major transversal programmes must be defined, such as:

- Governance: roles and responsibilities regarding cybersecurity across different modules.
- Incident Response Monitoring and Plan.
- Business Continuity Plan.
- Awareness and Training Practices.
- Guidelines for developing documentation and standards.
- Compliance and Regulations (contextualised in section 2.1).

The purpose of those elements is to provide a broad overview of how security is going to be managed from a non-technical perspective – defining requirements for people and processes is as important as designing and implementing the cybersecurity systems from the platform.

3.4.3 Logical Layer

The logical layer works as a blueprint and translates the generic concepts established previously into security systems and subsystems. The ultimate goal is to create a more concrete vision of relevant high-level security domains and interactions between them. Some of the key elements include:

- Access Control Policies: rules to define access and modification rights, following the Principle of Minimum Privilege.
- Third-party and Vendor Security: Third party agreements, monitoring third parties' services and validating solutions against predefined acceptance criteria. This is especially critical considering the multiplicity of players involved in the DOMINOES context and consequently, the range of different supply chains.
- Secure Software Development: Guidelines to implement and develop software securely (e.g., OWASP), according to internal requirements.
- Data classification (as defined in section 3.1).

3.4.4 Physical Layer

The physical layer consists of technical requirements that will be implemented in order to mitigate the main risks identified in previous steps, according to the established management structures and policies. In summary, it uses the blueprint from the logical layer to define a technology model. Examples of the components considered on this step can be platforms, hardware, network devices, and operating systems, among others. The output of such analysis would be a set of requirements for every device to be used in building the application and security architectures in a real scenario. From this point, security measures will be more concrete, and frequently will be associated with tools, products or technologies. From the critical components identified previously, the essential controls to be considered for DOMINOES are listed below. It is implied that all the adopted technologies and systems would have to support the suggested features.

- User and Access Control: AAA (Authentication, Authorisation and Accounting) should be technically implemented, enforcing all policies defined in the conceptual layer. Remote access requirements should also be established. The

most critical use of this security control would be for the data management module and database access.

- Data Encryption: Both for data at rest and data in transit, encryption measures should be considered wherever suitable.

- Communications Security: The use of secure protocols should be considered for every communication interface (Web, H2M, M2M) – HTTPS, TLS, SSH, etc.

- Network Segmentation: Multiple systems, interfaces and interactions should be correctly split into different networks to enhance security and isolate systems (ex. air gapping). Regarding this topic, a very important consideration is segregation between IT and OT environments, if there are real-time interfaces between critical control systems and conventional IT systems.

- Penetration Testing: Deployed software should always be verified for vulnerabilities before going online, mainly if it affects the user interface (DevSecOps).

3.4.5 Component Layer

Finally, the component layer implements the individual requirements and the technology model with security solutions available on the market (or tailor-made solutions). The complexity here arises from building the puzzle with all the required pieces in a cost-effective way, with as little functional overlap as possible. As the lowest layer in the model, it should also be the one closest to the architecture's physical realization and security systems from multiple vendors.

3.4.6 Operational Layer

The purpose of the operational layer is to the help managers keep track of the architecture's functional level and its performance. It includes the guidelines for managing all the controls and policies implemented in higher layers, such as:

- Logging, Auditing and Monitoring.
- Change Management.
- Patch Management.

3.4.7 The Matrix

For each of the described layers, a set of questions has to be asked and answered, similarly to what was stated in 3.4.1.1. The combination of those elements results in a very visual representation of the security architecture, also known as the SABSA Matrix. By addressing and completing all the cells, one can ensure that all the relevant aspects

of the design have been considered. The previous sections provided guidelines to address each design step, and what is essential for the specific DOMINOES solution. Starting from the business layer (3.4.1.1), where it is crucial to understand the application functional requirements and its purpose, we drill down to several security layers, ranging from strategy and governance (3.4.1.2), to device security requirements (3.4.1.5) and security operations (3.4.1.6). A comprehensive architecture would take everything into account and should be clearly communicated to all stakeholders involved.

Table 9 SABSA Matrix [17]

	Assets (what)	Motivation (why)	Process (how)	People (who)	Location (where)	Time (when)
Contextual	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, Including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions etc.	Time Dependencies of Business Objectives
Conceptual	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives, Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians & Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-life Risk Management Framework
Logical	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable

	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; SOA	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain Associations & Inter-actions	Start Times, Lifetimes & Deadlines
Physical	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications, Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms & Networks Layout	Timing & Sequencing of Processes & Sessions
Component	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Management Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, Data Repositories & Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring, Reporting & Treatment	Tools & Protocols for Process Delivery	Identities, Job Descriptions; Roles; Functions; Actions & ACLs	Nodes, Addresses & Other Locators	Time Schedules; Clocks; Timers & Interrupts
Service	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management

4 DOMINOES Cybersecurity Recommendations and Requirements

4.1 Recommendations Mapping to Dominos Security Architecture

In this section, we map a set of recommendations, including the Smart Grid Task Force Expert Group 2 [7] and NISTIR 7628 “Guidelines for Smart Grid Cybersecurity” [9] and Security Controls Matrix [35], to the DOMINOES cybersecurity architecture. These recommendations should be considered by all DOMINOES partners involved in the platform design stages and the others who will maintain and run the system in real demonstration sites. However, before doing all of this, partners involved in the validation sites should comply with the ethical requirements, by following the procedures for data collection, storage, protection, retention, and destruction, that are reported in D8.1 of DOMINOES, which comply with EU legislation and national regulations of each demonstrations site. This will ensure that we follow the EU GDPR recommendations, in terms of the data protection by design and the data protection by default at the earliest stages of the DOMINOES project and throughout its lifecycle. Also, it will help us to achieve the DOMINOES data security and privacy objectives listed in the previous sections.

Table 10 shows a list of recommendations that map to each of the DOMINOES security architecture layers. However, each partner has to decide what kind of recommendation they need to use, based on their internal organisation cybersecurity policy, and the objectives of the DOMINOES components that they will develop.

Table 10 DOMINOES Cybersecurity Recommendations in SABSA Security Architecture Layers

Security Architecture Layer	Recommendations
Contextual (The Business View)	• To have clear business opportunities, strategy, requirements, and capability, for the overall DOMINOES platform. • To create a technology strategy, capability, and technology architecture for the overall platform and each component in the DOMINOES environment.
Conceptual (The Architect’s Vision)	Cyber Threats, Education and Awareness, Policies, Standards, Guidelines, and DPIA)

Logical
(The Designer's View)
	• Network Security:
	  ○ Application Control
	  ○ Content Security (Email Inspection and Control, Web Inspection and Control)
	  ○ Data Centre Segregation (Firewall, IDS/ Intrusion Protection Systems (IPS), UTM/Next Gen, Deep Packet Inspection)
	  ○ Network Access Control
	  ○ Geolocation
	  ○ Network Time (NTP)
	  ○ Wireless (Application Control (App FW), Pre-Authentication (802.1x), Guest Network, Encryption)
	  ○ Monitoring (Network Behaviour Analysis/Network Anomaly Detection, Network Forensics, Logging and Monitoring)
	  ○ Network Encryption (Layer 2 Encryption, Transport Layer Security, Virtual Private Networking VPN)
	• Endpoint Security:
	  ○ Endpoint Defense (Anti Malware, Host Firewall, and HIPS)
	  ○ Disk Encryption
	  ○ Remote Access/VPN
	  ○ Secure Config Baselines
	  ○ Sandboxing
	• Physical Security:
	  ○ Physical Access Control
	  ○ Physical Asset Control
	  ○ Security Passes – Identity
	  ○ CCTV/Monitoring
	• Web Services Security:
	  ○ Direct Authentication
	  ○ Brokered Authentication
	  ○ Data Confidentiality
	  ○ Data Origin Authentication
	  ○ Logging and Monitoring
	• Data Security:
	  ○ Databases Security (Database Encryption, Database Assessment, Database Activity Monitoring)
	  ○ Data Loss Prevention (Storage, Database, Network, Endpoint, Email, and Web Gateway DLP, Physical Media Control, and Content Discovery)
	  ○ Encryptions (Files, Emails, SAN, and Applications)

    - Access Management (Entitlement and File Activity Management)
    - Logging and Monitoring
- Identity and Access Management:
    - Authentication (Web, Enterprise, Certificates, Remote Access Authentication, Biometrics, Mobile Device, and Network Authentications (802.1x, PPAP, CHAP etc.))
    - Authorisation
    - Privileged User Management
    - Provisioning (Joiners, Leavers and Movers, Device Identities, Managing Generic Accounts)
- Security Management:
    - Security Operations (SIEM, Log Management, Security Operations Center, Response and Investigation, Dashboard and Compliance reporting, Cyber Intelligence)
    - Vulnerability Management (Penetration Testing, Vulnerability Assessment)
    - Crypto Management
    - System Management (Patching and Configuration Management)
    - Security Incident Management
    - Forensics Management (Digital and Malware Forensics)
    - Business Continuity (Disaster Recovery, Business Continuity and Service Continuity plans)
- Cloud Security:
    - Cloud-based hardware security module (HSM)
    - VPN Gateway
    - API Gateway
    - DDoS Protection
    - Cloud Firewall Appliances
    - Threat Detection
    - Disk Encryption
    - Just in Time Access
    - Logging and Monitoring
    - Cloud Security Access Broker (Authentication, Data Tokenisation, Encryption, DLP, Logging, Single Sign-On, Access Control etc.)
- Application Security Controls:
    - Auditing (Business, Operational, and Components Activity Logging)

	○ Access Control – Authorisation (File system, Database, and client ACL. Role Based Access Control, and Least Privilege Controls) ○ User and Application Authentication (Browser-based Federation (SAML, ADFS), Bespoke Authentication, Directory (LDAP), Single Sign-On, Unsuccessful Login Controls, and Previous Logon Notification) ○ Encryption within the Application ○ Session Management ○ Integrity Controls (Tamper Resistance and Detection, Memory Protection, and Code Control) • Security Testing and Code Validation: ○ Secure Development (Code Repository Tooling, Code Control Tooling, Automated Code Packaging and Deployment Tooling) ○ Web Application Assessment (Web Vulnerability Scanning, and Web Application Testing)
Physical **(The Builder's View)**	• Cloud Monitoring • Data Loss Prevention • Build Compliance • Vulnerability Scanning • Incident Management • Privileged User Management • Patch Management • Remote Access Management • Anti-Malware Management • Business Continuity Management • Key Management • Cloud Security Insight • Certificate Management • Security Testing
Component **(The Tradesman's View)**	• Secure by Design • Operational Risk Management • Security Risk Management • Education and Awareness • Security Requirements for Devices and Systems • Security Policy, Standards, and Guidelines Governance and Compliance Management (ISO 27000, GDPR, NIST, COBIT, PCI, TLS, IEC, and others)
Management	• Software Version Management • Asset and Configuration Management

(The Service Manager's View)	• Backup and Recovery • Network Management • Licence Management • Change and Release Management • Problem Management • Service Level Management • Service Continuity Management • Deployment Compliance • Release and Deployment Management • Cloud Monitoring and Management • Testing • Release Management

4.2 Requirements

There are a number of security techniques that can be used to mitigate the risks associated with the cybersecurity in the smart grid. The following subsections describe which technique should be used regarding each one of the major identified security risks.

4.2.1 Authentication Protection

In basic terms, to shield systems against this type of attack, every access gate to the system (i.e., web interface, console, API or similar) should be protected by an authentication technique, exposing the minimal information or services to unauthorised users or systems. The authentication system should use a robust cryptographic technique to avoid the transport of sensitive authentication information over the network in a way that it can be intercepted and used by an attacker (i.e., no clear text information should be exchanged if possible). Depending on the possibilities of the system components, the most common forms of authentication to be used can be from a simple username and password pair to a certificate-based method. Weaker methods such as network address-based authentication (IP address or MAC) can also be used to reinforce the authentication but should not be used in a standalone mode. In complex distributed systems such as in a smart grid environment, to avoid the certificate/password management hassle, centralized identity management tools can be used. Example techniques for this purpose are Shibboleth (https://www.shibboleth.net/) or Microsoft's Active Directory.

In summary, to prevent authentication attack risk, the following techniques should be used:

- Authentication is required for every access:
  - Web interface.
  - Console.

  - API.
  - Other interconnection protocols.

- Usage of secure and robust authentication methods:
  - Avoid clear text-sensitive information to be transferred.
  - Avoid authentication by easily forgeable mechanisms.

- In complex systems, usage of centralised identity management systems:
  - Shibboleth.
  - Microsoft Active Directory.

4.2.2 Authorisation Protection

To protect systems against unauthorised access, user profiles should be used to segment the access to data and system privileges. In conjunction with authentication methods, every authenticated user or system (for instance, in the case of APIs) should have an associated user profile which clearly delimits the access rights to the available resources. To avoid unnecessary system exposure, the user profiles should be designed with the objective of providing only the essential privileges the user needs to perform the operations he needs in the system. In order to prevent privilege escalation risk (a user gaining access to resources that should be not accessible) by the exploitation of an eventual system's security flaw, all the system's components should have the vendor's security patches and updates applied as soon as they are released.

In summary, the available authorisation techniques are:

- Usage of user profiles:
  - Design the profiles to limit the accessible resources and data to the essential.
- Limit the vulnerabilities of the system that might permit privilege escalation:
  - Apply the vendor's security patches and updates on a regular basis.

4.2.3 Breaking into a System's Protection

A first security measure is to secure the physical access to the systems to the authorised personnel only, avoiding the exposure to direct/physical attacks on the system. Usually, this is achieved by restricting the access to the data centre itself and to the network elements, which should not be accessible (e.g., protected by a key-locked locker). Additionally, it is recommended to have an access log to the facility, permitting the auditing of any physical access to the system on the event of an attack. The network access is as important as the physical access, so every system component's network (and the component itself if possible) should be protected by a network firewall, IDS and IPS. Also, the networks (wired/wireless) should be protected against unauthorised

access by the usage of network layer protection mechanisms, such as 802.1x. These measures should be applied to minimise the surface area exposed to unwanted threats.

Cryptographic methods should also be used, where possible, between the system components to ensure the confidentiality and integrity of the data travelling between them. When using the public internet to interconnect distributed components, the usage of these methods should be mandatory. In some cases, the use of a VPN technique can help to ensure confidentiality of data transport over public networks, as it makes use of methods of authentication (e.g., Internet Key Exchange (IKE)), data confidentiality (encryption) and integrity assurance, such as IPsec. Alternatively, depending on the network layer, there are several techniques that can also be used to ensure data security.

In summary, to prevent this type of risk, the following techniques should be used:

- Physical access:
  - Access to every element of the system (servers, network elements, devices) should be protected by key lock, key card or similar methods.

- Network/Electronic access:
  - Network firewalls/ IPS.
  - IDS.
  - VPNs or similar cryptographic methods to interconnect system components over public networks.
  - Link layer protection methods.

4.2.4 Confidentiality Protection

The preferred methods to guard against confidentiality attacks require the encryption of the information (e.g. messages, data). There is a vast array of encryption algorithms (symmetric, public-key, and hybrid) and key distribution mechanisms (key servers, PKI, and distributed key management).

4.2.5 Cybersecurity Evaluation

On the other hand, there are also some methods that can be used to evaluate the current vulnerabilities of the network. These methods can range from a simple port scanner to identify what is exposed to the possible attackers, to complex methods with a database of the currently known vulnerabilities of the operating systems and network components (e.g. network switches and routers), which can identify which ones are present in the system. Some of these methods include:

- Port scanning:
  - NMAP (Network Mapper) Security Scanner.

- Security auditing:

- OpenVAS (Open Vulnerability Assessment System).
- Nessus.

There are some all-in-one distributions that contain the most popular set of security auditing methods. One of these distributions is, for instance, Kali Linux[4], which contain, not only security auditing tools, but also penetration test tools that can be used to test the robustness of the system against attacks.

[4] https://www.kali.org/

5 Conclusions

In this deliverable, we presented the cybersecurity architecture for the DOMINOES project. The architecture is based on the already well-known open-source security architecture development and management method called Sherwood Applied Business Security Architecture Framework (SABSA). Specifically, it is divided into six layers, which helps to increase security objectives top-down across different stakeholder realms, starting with business requirements (context) down to security operations (Management). We have mapped each of the SABSA layers to the DOMINOES application architecture.

The architecture design allowed us to be able to identify and classify the main datasets that will be exchanged, stored, or shared by the DOMINOES platform. Also, it provides full details with regard to the cybersecurity threat landscape, that includes the discussion of the types of different categories of threats and vulnerabilities that we expect to have in the DOMINOES platform. Moreover, the classification of threat agents (actors) and attack vectors were considered in this deliverable. At this point, we also provided a list of cybersecurity recommendations and requirements mapped to the proposed architecture, which intend to be used for securing the DOMINOES platform. Moreover, this deliverable covered the current smart grid cybersecurity regulations, standards and approaches and discussed the challenges that DOMINOES cybersecurity might face.

The deliverable provides a comprehensive insight which could be of huge benefit to the DOMINOES project, to implement a secure and trusted P2P energy trading platform. The next cybersecurity tasks in the DOMINOES project will focus on implementing an anomaly detection component in T3.6 and the validation of securing data handling platform in T4.1.1 to address some of Dominoes cybersecurity challenges discussed previously in section 2.3.

References

Internal Documents (http://dominoesproject.eu/)

D1.2 ICT platform and connected energy network reference architecture design

D1.4 Implementation plan for the validation environment

D6.9 Standardization proposals Year 1

External Documents

[1] J. Abdella and K. Shuaib, “Peer to peer distributed energy trading in smart grids: A survey,” *Energies*, vol. 11, no. 6, 2018.

[2] European Union, “Regulation 2016/679 of the European parliament and the Council of the European Union,” *Off. J. Eur. Communities*, vol. 2014, no. March 2014, pp. 1–88, 2016.

[3] European Parliament and Council of The European Union, “Directive (EU) 2016/1148 of the European Parliament and of the Council - Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union,” *Off. J. Eur. Union*, vol. 194, no. July, pp. 1–30, 2016.

[4] “Guide to the General Data Protection Regulation (GDPR),” *Information Commissioners Office*, 2018. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/. [Accessed: 26-Jul-2019].

[5] “Smart Grid Task Force 2012 - 14 Expert Group 2 Expert Group for Regulatory Recommendations for Privacy, Data Protection and Cyber-security in the Smart Grid Environment, : Regulatory Recommendations for Privacy , Data Protection and Cyber-Security in the,” 2014. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf.

[6] The European Commission, “Commission recommendation on preparations for the roll-out of smart metering systems,” *Off. J. Eur. Union*, no. 2011, pp. 9–22, 2012.

[7] “Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection Recommendation to the European Commission,” 2011. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations regulatory requirements v1.pdf. [Accessed: 26-Jul-2019].

[8] Smart Grids Task Force, “Proposal for a list of security measures for smart grids,” 2013. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/20140409_enisa.pdf. [Accessed: 26-Jul-2019].

[9] “Guidelines for smart grid cybersecurity,” *NISTIR*, 27-Sep-2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf. [Accessed: 26-Jul-2019].

[10] S. La Porta, R. Griffin, and R. Chabukswar, “High-level design documentation and deployment architecture for Multi-Attribute SCADA Intrusion Detection System,” *Sparks*, 2015. [Online]. Available: https://project-sparks.eu/wp-content/uploads/2014/04/SPARKS_D4_1_Multi-Attribute_SCADA_Intrusion_Detection_System.pdf. [Accessed: 26-Jul-2019].

[11] E. Bilbao Hernández *et al.*, “Security for smart Electricity GRIDs, How to address the security challenges in Smart Grids,” *SEGRID*, 2017. [Online]. Available: https://segrid.eu/wp-content/uploads/2017/07/Whitepaper-SEGRID.pdf. [Accessed: 26-Jul-2019].

[12] E. Piatkowska, A. Bajraktari, D. Chhajed, and P. Smith, “Tool Support for Data Protection Impact Assessment im Smart Grid,” *Elektrotechnik und Informationstechnik*, vol. 134, no. 1, pp. 26–29, 2017.

[13] Y. Tong, J. Deyton, J. Sun, and F. Li, “A Secure Data Sharing Mechanism for Situational Awareness in The Power Grid,” *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1751–1759, Dec. 2013.

[14] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao, “Scalable solutions of Markov games for smart-grid infrastructure protection,” *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 47–55, 2013.

[15] D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, “Security for industrial communication systems,” *Proc. IEEE*, vol. 93, no. 6, pp. 1152–1177, 2005.

[16] X. Fan and G. Gong, “Security Challenges in Smart-Grid Metering and Control Systems,” *Technol. Innov. Manag. Rev.*, vol. 3, no. 7, pp. 42–49, 2018.

[17] B. Shakerighadi, A. Anvari-Moghaddam, J. C. Vasquez, and J. M. Guerrero, “Internet of things for modern energy systems: State-of-the-art, challenges, and open issues,” *Energies*, vol. 11, no. 5, 2018.

[18] W. L. Chin, W. Li, and H. H. Chen, “Energy Big Data Security Threats in IoT-Based Smart Grid Communications,” *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, 2017.

[19] D. Lynas, “An Overview of the SABSA Methodology,” *SABSA*, 2016. [Online]. Available: https://www.slideshare.net/SABSAcourses/sabsa-overview. [Accessed: 26-Jul-2019].

[20] J. Sherwood, A. Clark, and D. Lynas, *Enterprise Security Architecture A Business-Driven Approach*. Taylor & Francis, 2005.

[21] J. D. Meier *et al.*, *Improving Web Services Security: Scenarios and Implementation Guidance for WCF Contributors*. Microsoft Corporation, 2008.

[22] L. Marinos and M. Lourenço, “ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends,” *ENISA*, 2019. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018. [Accessed: 26-Jul-2019].

[23] I. Nai Fovino, A. Carcano, M. Masera, and A. Trombetta, “An experimental investigation of malware attacks on SCADA systems,” *Int. J. Crit. Infrastruct. Prot.*, vol. 2, no. 4, pp. 139–145, 2009.

[24] G. Elbez, H. B. Keller, and V. Hagenmeyer, “A New Classification of Attacks against the Cyber-Physical Security of Smart Grids,” in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1–6.

[25] “OWASP Top 10 web vulnerability,” *OWASP*, 2017. [Online]. Available: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. [Accessed: 26-Jul-2019].

[26] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, “Smart Grid Security: Threats, Vulnerabilities and Solutions,” *Int. J. Smart Grid Clean Energy*, pp. 1–6, 2013.

[27] B. Li, R. Lu, G. Xiao, Z. Su, and A. Ghorbani, “PAMA: A Proactive Approach to Mitigate False Data Injection Attacks in Smart Grids,” *2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc.*, pp. 1–6, 2019.

[28] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, “Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods,” *IEEE Access*, pp. 1–1, 2019.

[29] Yilin Mo *et al.*, “Cyber–Physical Security of a Smart Grid Infrastructure,” *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[30] A. Viswanathan, N. B. Sai Shibu, S. N. Rao, and M. V. Ramesh, “Security Challenges in the Integration of IoT with WSN for Smart Grid Applications,” *2017 IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC 2017*, pp. 1–4, 2018.

[31] S. Haas, S. Karuppayah, S. Manickam, M. Mühlhäuser, and M. Fischer, “On the resilience of P2P-based botnet graphs,” *2016 IEEE Conf. Commun. Netw. Secur. CNS 2016*, no. Mm, pp. 225–233, 2017.

[32] Haylee, “Botnets: Dawn of the connected dead.” [Online]. Available: https://blog.emsisoft.com/en/27233/what-is-a-botnet/. [Accessed: 26-Jul-2019].

[33] N. Elmrabit, S.-H. Yang, and L. Yang, “Insider threats in information security categories and approaches,” in *2015 21st International Conference on Automation and Computing (ICAC)*, 2015, pp. 1–6.

[34] L. Langer and M. Kammerstetter, *The Evolution of the Smart Grid Threat Landscape and Cross-Domain Risk Assessment*. Elsevier Inc., 2015.

[35] R. Campbell, “Enterprise Security Architecture - Security Controls Matrix,” 2019. [Online]. Available: https://www.assuredcontrol.com/index.html. [Accessed: 26-Jul-2019].