SDN-µSense

Project No. 833955
Project acronym: SDN-microSENSE
Project title:
SDN - microgrid reSilient Electrical eNergy SystEm

Deliverable D9.4

Market Analysis, Roadmap and Business Modelling Report

Programme: H2020-SU-DS-2018
Start date of project: 01.05.2019
Duration: 36 **months**

Editor: Eight Bells
Due date of deliverable: 31/07/2020 **Actual submission date:** 31/07/2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833955

Deliverable Description:

Deliverable Name	Market Analysis, Roadmap and Business Modelling Report
Deliverable Number	D9.4
Work Package	WP 9
Associated Task	T9.2
Covered Period	M01-M15
Due Date	31/07/2020
Completion Date	M15
Submission Date	31/07/2020
Deliverable Lead Partner	Eight Bells
Deliverable Author(s)	8BELLS, INC, 0INF, SID, IPTO, PPC, IEIT, EPESA, SINTEF, CW, ATOS, UBITECH, REAL, ALKYONIS, MoA
Version	**1.0**

Dissemination Level		
PU	Public	**X**
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)	

CHANGE CONTROL

DOCUMENT HISTORY

Version	Date	Change History	Author(s)	Organisation
0.1	04/05/2020	Finalization of ToC	Vasilis Machamint	8BELLS
0.2	05/06/2020	Contribution to Section 2 – Methodology Approach and Tools	Vasiliss Machamint, Ioannis Giannoulakis, Christos Markou, Panos Markou	8BELLS
0.3	11/06/2020	Contribution to Section 5 - SWOT Analysis	Achilleas Sesis, Yannis Spyridis; Vasilis Machamint, Christos Markou;	0INF; 8BELLS
0.4	15/06/2020	Contribution to Section 3 - PESTLE Analysis	Vasilis Machamint, Panos Markou; Giannis Ledakis, Sofianna Menesidou	8BELLS; UBITECH
0.41	16/06/2020	Contribution to Use Case 6 Analysis (Section 7.6)	Vasilis Machamint; Achilleas Sesis, Yannis Spyridis; Mats Åström	8BELLS; 0INF; CW
0.45	17/06/2020	Contribution to Section 4 - Porter's Five Forves Analysis	Vasilis Machamint, Ioannis Giannoulakis; Elisavet Grigoriou, Maria Poveda	8BELLS; SID

0.5	18/06/2020	Contribution to Use Case 1 Analysis (Section 7.1)	Hans Christian Bolstad; Vasilis Machamint; Theodoros Rokkas, Ioannis Neokosmidis; Nikola Paunovic	SINTEF; 8BELLS; INC; REAL
0.51	20/06/2020	Contribution to Use Case 2 Analysis (Section 7.2)	Maria Atanasova; Vasilis Machamint; Giannis Ledakis, Sofianna Menesidou	IEIT; 8BELLS; UBITECH
0.52	25/06/2020	Contribution to Use Case 3 Analysis (Section 7.3)	Panagiotis Famelis, Ioli Apostolopoulou; Vasilis Machamint, Christos Markou; Christos Dalamagkas , Papadopoulos Anastasios;	IPTO; 8BELLS; PPC
0.53	27/06/2020	Contribution to Use Case 5 analysis (Section 7.5)	Christos Dalamagkas , Papadopoulos Anastasios; Vasilis Machamint; Panopoulos Apostolos; Nikolaos Siaxampanis; Elisavet Grigoriou, Maria Poveda	PPC; 8BELLS; MoA; ALKYONIS; SID
0.6	01/07/2020	Contribution to Use Case 4 Analysis (Section 7.4)	Vasilis Machamint; Chloe Coral; Elena Gonzalez	8BELLS; EPESA; ATOS
0.7	02/07/2020	Contribution to SDN fuzzy AHP Sections (Section 6 and Section 2.4)	Theodoros Rokkas, Ioannis Neokosmidis	INC
0.71	07/07/2020	Contribution to Section 1- (Introduction) and Section 8 (Conclusions)	Ioannis Giannoulakis, Vasilis Machamint, Christos Markou, Panos Markou	8BELLS
0.72	08/07/2020	Executive Summary	Vasilis Machamint	8BELLS
0.95	27/7/2020	Addressing internal reviewer's comment	Vasilis Machamint, Ioannis Giannoulakis, Christos Markou, Panos Markou	8BELLS
1.0	31/7/2020	Finalization of Document	Vasilis Machamint	8BELLS

DISTRIBUTION LIST

Date	Issue	Group
15/07/2020	Revision	SAB, NTNU, INCITES and all the involved partners
30/07/2020	Acceptance	SAB, NTNU, INCITES, QM and all the involved partners
31/07/2020	Submission	8BELLS, AYESA

SAB APPROVAL

NAME	INSTITUTION	DATE
Dr Marc Stauch	LUH	13/07/2020

Academic and Industrial partner revision

NAME	INSTITUTION	DATE
Ajay Nehra	Academic partner: NTNU	14/07/2020
Theodoros Rokkas	Industrial partner: INCITES	14/07/2020

Table of contents

List of figures

List of tables

Acronyms

Acronym	Explanation
AC	Alternating Current
AGC	Automatic Generation Control
AHP	Analytic Hierarchy Process
B2B	Business-to-Business
B2C	Business-to-Consumer
BMC	Business Model Canvas
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
COBIT	Control Objectives for Information Technologies
CR	Consistency Ratio
CSP	Cloud Service Provider
CSR	Corporate and Social Responsibility
DC	Dirrect Current
DoS	Denial of Service
DR	Demand Response
DSO	Distribution System Operator
EEA	European Economic Area
EMS	Energy Management System
EPCIP	European Programme for Critical Infrastructure Protection
EPES	Electrical Power and Energy System
ERM	Enterprise Risk Management
EU	European Union
FACTS	Flexible AC Transmission Systems
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
HIL	Hardware-in-the-loop
HMI	Human Machine Interfaces
HSM	Hardware Security Module
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IED	Intelligent Electronic Device
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
kW	kilowatt
MAC	Media Access Control

MitM	Man-in-the-middle
NIST	National Institute of Standards and Technology
PCC	Point of Common Coupling
PESTLE	Political, Economic, Sociological, Technological, Legal, Environmental
PII	Personally identifiable information
PLC	Programmable logic controller
PTP	Precision Time Protocol
PV	Photovoltaic
R&D	Research and Development
RCP	Rapid Control Prototyping
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SDN	Software-Defined Networking
SIEM	Security information and event management
SWOT	Strengths, Weaknesses, Opportunities and Threats
TSO	Transmission System Operator
UK	United Kingdom
VM	Virtual Machine

Executive Summary

This Deliverable D9.4 - Market Analysis, Roadmap and Business Modelling Report, has the goal to present the efforts towards understanding the market potential of the SDN-microSENSE solution. Apart from the market characteristics, it illustrates the factors that will affect the market adoption of SDN-microSENSE solution and business models. Furthermore, the deliverable is related to the activities of the T9.2 - Market Analysis and Business models, which explores the means to deliver SDN-microSENSE outcomes to the market.

The deliverable provides the necessary market concept that is required to be clear for the implementation of the SDN-microSENSE solution. The report offers a clear picture of the SDN-microSENSE market by conducting a market analysis using a variety of tools. A PESTLE analysis is conducted to assess if market conditions are favourable for launching SDN-microSENSE in the market. Furthermore, the Five Forces of Porter Framework is analysed for the SDN-microSENSE project in order to assess the market conditions, the industry's attractiveness and the industry status. Moreover, a SWOT analysis is conducted to estimate the level of the strategic advantage for the SDN-microSENSE solution.

A business roadmapping is also conducted, providing deeper knowledge of the factors that affect SDN-microSENSE market adoption and evolution using the Fuzzy Analytic Hierarchy Process (AHP). A conducted survey reveals experts' vision regarding critical factors that can influence the introduction and acceptance of the SDN-microSENSE as a technology solution.

The report also focuses on the six project use cases, offering a value proposition, a Business Canvas and a Business plan activity map for each one of them in order to describe better the consortium's strategy towards bringing the SDN-microSENSE solution to the market.

The results of this report will be used to guide the activities of T9.2 and WP9, serving as a guideline for the project exploitation activities and the future commercialization aspects.

1. Introduction

1.1 Purpose of this document

This deliverable provides a definition of the SDN-microSENSE market with special focus in the project use cases and identifies the key stakeholders taking part in each of them. The report considers the different market possibilities and tools that will make the SDN-microSENSE product(s) sustainable and at a time ensure the services will be adaptable and feasible in the energy security market segment.

The specific objectives of the deliverable are the following:

- Provide a clear picture of the SDN-microSENSE market based on the specific information that stems from each use case of the project.
- Conduct a business roadmap analysis to provide a deeper knowledge of the factors affecting SDN-microSENSE market adoption and evolution, by using multi-criteria decision-making methods
- Analyse the specific market of the project, including its definition, segmentation, target market and competitors.
- Analyse the key stakeholders for each use case identifying their characteristics, relations and inter-relations.
- Extract the value chain of each use case, as a result of the market and stakeholder analysis.

For our analysis, we will be considering the EU market as our target market. Thus, we will be assessing the market dynamic and the competitive framework of the EU market environment. Once the above assessment is complete, we will elaborate on how the SDN-microSENSE project can create value in that market and which business plan can lead to the optimal value creation. Finally, we will be assessing our business model's competitive advantage and sustainability against our competition.

1.2 Focus Area and Analysis Tools

This section presents a summary of the focus areas and the analysis tools that are used in this document. Further analysis of the tools and methodologies used can be found in Section 2 of the report.

First, a market environment analysis is conducted, offering insights into the micro and macro environments of the SDN-microSENSE project. This market analysis is conducted using three frameworks:

1. **PESTLE analysis:** a framework used to analyse and monitor the macro-environmental factors that may have a profound impact on an organization's performance. This tool is especially useful when starting a new business or entering a foreign market. PESTLE offers general insights into the nature of the elements that affect businesses and generally have an indirect impact on the company.
2. **Porter's Five Force Framework**: a tool used to analyse the company's micro-environment or its competitive environment. It offers a 'horizontal' competition analysis by examining the threat of substitute products or services, the threat of established rivals, and the threat of new entrants. Porter's 5 Forces Model also analyses the 'vertical' competition by examining the bargaining power of suppliers and the bargaining power of customers. The tool aims to determine the competitive intensity of an industry and to gain insights into the industry's attractiveness and profitability
3. **SWOT Analysis:** a strategic planning technique that offers insights into internal and external factors that a company is expected to face in the market. It is a brainstorming technique that provides a compilation of a company's strengths, weaknesses, opportunities and threats.

Following the market environment analysis, the business roadmapping and value creation analysis of SDN-microSENSE is conducted using three frameworks:

1. **Fuzzy AHP:** The Fuzzy analytic hierarchy process (AHP) is an approach that is suitable for dealing with complex systems related to making a choice among several alternatives. The fundamental principle of the analysis is the possibility of connecting information, based on knowledge, to make decisions or previsions.
2. **Business Model Canvas**: a one-page overview that enables management to have structured conversations around strategy by laying out the crucial activities and challenges involved with the identified initiative and how the elements relate to each other.
3. **Activity map**: a framework for analyzing competitive advantage through listing the value-creating activities as core competencies a business offers, as well as the advantages created through delivering the unique mix of these competencies. The activity mapping identifies an organization's core operational activities, its key functional strengths and the customer perceived value of a product or service.

1.3 Document Overview

This deliverable is structured in 8 Chapters.

In Chapter 1, an introduction regarding the scopes of the Deliverable, the focus areas and the tools that are used for the market analysis and the business modelling is presented.

Chapter 2 provides a Literature survey of the tools and methodologies that are used for the analysis.

In Chapter 3, the Porter's Five Forces analysis for SDN-microSENSE is presented.

Chapter 4 describes the PESTLE analysis of SDN-microSENSE.

Chapter 5 presents the SDN-microSENSE SWOT Analysis.

Chapter 6 provides the detailed approach of the SDN Fuzzy Analytical Hierarchy Process and its results.

In Chapter 7, the business analysis of the six SDN-microSENSE use cases is carried out.

Finally, Chapter 8 concludes the deliverable.

2. Methodology Approach and Tools

This section provides a literature survey of the tools and methodologies that will be used for the market analysis, the business roadmapping and the business modelling analysis of the deliverable.

2.1 PESTLE Analysis

PESTLE analysis is a marketing tool used to determine the influence that the macro-environment can have on a company. The study of this macro-environment makes it possible to identify the factors specific to a situation (geographical area, market, company, sector of activity etc) and thus to be able to measure the impact of these factors on an organization [1].

The PESTLE analysis (shown in Figure 1) is usually part of the strategic analysis and should lead to the identification of the most influencing factors in the market, company or industry studied [2]. As part of a strategic approach, this tool is used in conjunction with the SWOT analysis to assess the macro-environmental effects on a company.

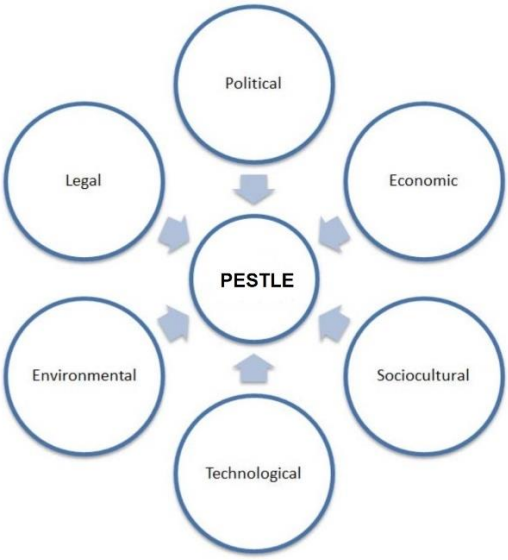


Figure 1: The PESTLE Framework [3]

The PESTLE analysis divides the external environment into the following six main categories of factors of influence on an organization [4]:

Political Environment: It operates at several levels, from regional to international, in terms of fiscal and monetary policies. In addition, it also includes everything relating to civic engagement and the political behaviour of society.

Economic Environment: It includes all the variables and all the factors that play a significant role not only on the purchasing power and consumption expenditure of the customers and suppliers, but also on the representation of socio-economic factors such as the distribution of wealth.

Social or Sociocultural environment: It includes the different characteristics of the population (size, age pyramid, family structure, culture, traditions, etc.) as well as access to education, information, or even the fashions and trends that may influence the obtaining or acquisition of services or products.

Technological Environment: This corresponds to the research and development forces and their financial support, which create new technologies, new products or which directly or indirectly influence the capacity of companies to innovate.

Legal Environment: It directly influences the organization through at least these complementary mechanisms: laws, regulations and standards, controls and a judicial system. However, we must not forget that it also influences individuals, and therefore the organization in an indirect form.

Environmental or Ecological context: It defines all the factors linked to nature, sustainable development and its policies, which influence the activity of your organization. Some directly influence your organization's output, such as energy shortages, while others are reactions to economic development, such as regulations or subsidies.

The PESTLE analysis is fundamental when creating a business model, assisting in determining the feasibility and viability of the various alternatives that may arise. The PESTLE analysis of SDN-microSENSE is provided in Section 3.

2.2 Porter's Five Forces Framework

Porter's Five Forces is a tool created by strategy professor Michael Porter, which allows for a company to perform an in-depth analysis of the competitors and every threat that can affect the profitability of its business in any market [7]. Porter's Five Forces Analysis can be particularly useful for businesses that plan to enter a market or implement a strategy to strengthen their market positioning. In addition to the competitive environment, this tool gives you the possibility of defining with great precision the opportunities and threats that weigh on a business.

Porter's five forces make it possible to assess competition in a market, through the analysis of different elements (as seen in Figure 2) : the bargaining power of suppliers, the bargaining power of buyers, the threat of new entrants, the threat of substitute products and the industry rivalry [8]. The configuration, hierarchy and dynamics of these forces make it possible to identify the key success factors, that is to say the strategic elements, that should be mastered to allow companies gain a competitive advantage.

Figure 2: Porter's Five Forces of Competition Framework [9]

By definition, Porter's five forces model characterizes a competitive environment and not a particular firm. Thus, for all the competitors involved, the analysis is the same, and the key success factors are identical [10]. The five forces determining the competitive structure of a goods or services industry are further elaborated below.

Bargaining power of suppliers: The bargaining power of suppliers can have significant impacts on prices and influence the profitability of a company [11]. The influence of suppliers depends on their negotiating power, that is to say on their ability to impose their conditions on the firms involved (in terms of cost or quality). A low number of suppliers, a strong brand, highly differentiated products are all factors that increase the cost of changing suppliers and, therefore their power. Suppliers have high power when:

- they are concentrated and few in number;
- the competitors (their customers) are numerous and dispersed;
- the transfer cost (the cost that a customer must bear to change supplier) is high;
- there is a threat of downstream integration from suppliers.

Bargaining power of buyers: The influence of buyers in a market depends on their negotiating power [12]. Their influence on the price and the conditions of sale (payment terms, services) determines the profitability of the market. The level of concentration of clients gives them more or less power; few customers facing multiple producers have greater negotiation possibilities (eg large distribution). Buyers have high bargaining power when:

- they are few in number (oligopsony);
- there are alternative sources of supply;
- the transfer cost (cost that customers must bear to change supplier) is low or high and predictable (which means that the offer is standardized);
- there is a threat of upstream integration (customers can produce the offer themselves).

Threat of new entrants: The difficulties that new entrants face when entering an industry make it possible to determine the level of competition within the market. If the barriers to entry are few, new players can easily position themselves in an industry and lead to a rapid multiplication of competitors [13]. Otherwise, competition is generally weak and it is easier to acquire customers.

The emergence of new competitors can be hampered by the existence of barriers to entry : the initial investments and the time required to make them profitable (also called “capital intensity”), the patents already in place, technical norms and standards, protectionist measures , the brand image of already established companies, cultural barriers, etc. All these means make entry more difficult for a new competitor. Competitors already in place usually try to strengthen these barriers to entry.

Threat of substitutes: This Porter's force makes it possible to determine the level of threat posed by substitute products in the face of offers already on the market [13]. Substitute products represent an alternative to the offer of the firms involved and they pose a threat when their value for money is higher than that of the established offer. If they provide greater value for the same or only slightly higher price, the threat is strong. If, on the other hand, the additional value is proportional - or even lower - to the additional price, the threat is low.

When faced with a new item or service that may present itself as an excellent alternative to its offer, a company can react in different ways. To maintain the appeal of its product, it can apply lower prices or add functionality to provide more value to its customers. On the other hand, it can decide to switch to a substitute product or to withdraw from the market.

Industry Rivalry: Industry rivalry is determined, among other things, by the number of competitors and the opportunities that arise for companies, suppliers and buyers [14]. Industry rivalry is qualified as fierce when a market is growing and dominated by a small number of firms, but also when consumers have the possibility of switching easily from one product to another.

Competitors are struggling within the industry to increase or simply maintain their position. There are more or less intense power relations between competitors, depending on the strategic nature of the sector, the attractiveness of the market, its development prospects, the existence of barriers to entry and exit, the number of companies, the size and diversity of competitors, the importance of fixed costs, the possibility of achieving economies of scale etc. When rivalry is strong, players generally engage in price wars, which can have negative impacts on their profitability.

2.3 SWOT Analysis

The SWOT analysis is an established method for assisting the formulation of strategy [15]. It is a business strategy tool for determining the options offered in a strategic business area [16]. It aims to specify the objectives of the company or the project and to identify the internal and external factors that are favourable and unfavourable to the achievement of these objectives. SWOT has been described as a proven tool for strategic analysis. Strengths and weaknesses are often internal, while opportunities and threats generally focus on the external environment.

The name is an acronym for the four parameters examined by the technique[17]:

- **Strengths**: Characteristics of the company or project that give it an advantage over others.
- **Weaknesses**: Company features that disadvantage the company or the project to the other.
- **Opportunities**: elements of the environment that the company or the project could exploit to its advantage.
- **Threats**: elements of the environment that could cause problems for the business or project.

Conducting a SWOT analysis involves performing two diagnoses:

1) **an external analysis**, which identifies the opportunities and threats present in the environment [18]. These can be determined using a series of strategic analysis models, such as the PESTLE analysis, the five competitive forces model proposed by Michael Porter, or even scenario analysis. This could, for example, involve the emergence of new competitors, the appearance of new technology, the emergence of new regulations, the opening of new markets, etc. By definition, the results of the external analysis are the same for all the competitors involved;
2) **an internal analysis**, which identifies the strengths and weaknesses of the strategic business area [18]. These can be determined using a series of models of strategic analysis, such as the value chain analysis. It can be, for example, the technological portfolio, the geographic presence, the network of partners, the corporate governance structure, etc. By definition, the results of the internal analysis are specific to the organization studied.

The expected result of a SWOT analysis is typically presented in the form of a table with a grid made up of four large boxes (see Figure 3):

- Vertically: two columns.
  - The column on the left collects the list of elements having a positive or favorable impact on the area of the studied strategic activity.
  - The column on the right collects the list of elements having a negative or unfavorable impact on the area of the studied strategic activity.
- Horizontally: two lines.
  - The elements that are related to internal factors are reported in the upper line. These elements - whose causes are internal - can be modified by the organization.
  - In the lower line, the elements that are related to external causes (and are therefore, in general, common to all competitors) are reported. These elements - whose cause or causes are external - are imposed on the leaders of organizations, who have no power over them.

Figure 3: SWOT Analysis [19]

The operation of the power grid is of high strategic importance, and there have been several use cases of SWOT analysis for these types of problems in the literature. Jaber et al. [20], Okello et al. [21] and Terrados et al. [22] utilized a SWOT analysis to conduct energy planning and formulate strategic goals. It is generally accepted as one of the most reliable strategic planning tools, including in the energy sector, assisting in implementation of innovative technologies and development of action plans.

2.4 Fuzzy Analytical Hierarchy Process

The AHP was proposed and developed by Thomas Saaty [24], in the early 1970s, mainly for military purposes, such that AHP can be considered to be a multi-criteria decision-making methodology. AHP has been extensively used over the years to cover various application areas, such as education [25], engineering [26], industry [27], manufacturing [28] and resource allocation [29]. Recently, AHP has also been widely used for selecting and ranking alternatives in the field of Information and Communications Technology (ICT) [30]-[33].

AHP is a structured technique for dealing with complex decisions, based upon a rational and comprehensive framework for decomposing an unstructured complex problem into a multi-level hierarchy of interrelated criteria, sub-criteria and decision alternatives. By incorporating judgments on qualitative and quantitative criteria, AHP manages to quantify decision-makers' preferences. The relative priorities of the criteria, sub-criteria and alternatives are finally reached by a mathematical combining of all these various judgments.

Figure 4 illustrates the required steps of AHP. In the first step, the problem that will be investigated is framed (i.e., its formation articulated), while the criteria and sub-criteria contributing to the objective's satisfaction are determined through interviews and/or group discussions with experts. The multi-level hierarchy is then constructed (Figure 5), consisting of three levels. In the first level, the objective under investigation is shown. In the next level, the criteria, C_{rk} with k=1,2,…,N and N the total number of criteria, participating in the decision-making process are determined. The criteria should be general enough to incorporate several features resulting in a rough description of the objective. In the lower level, criteria are further analyzed into their sub-criteria SC_{rjk}, where j=1,2,…,M_k and M_k is the number of sub-criteria under criterion k. Sub-criteria represent a specific feature characterizing a criterion. The identification of criteria and sub-criteria is accomplished based on the focus of their preferential independence.

Figure 4: Steps for analytic hierarchy process

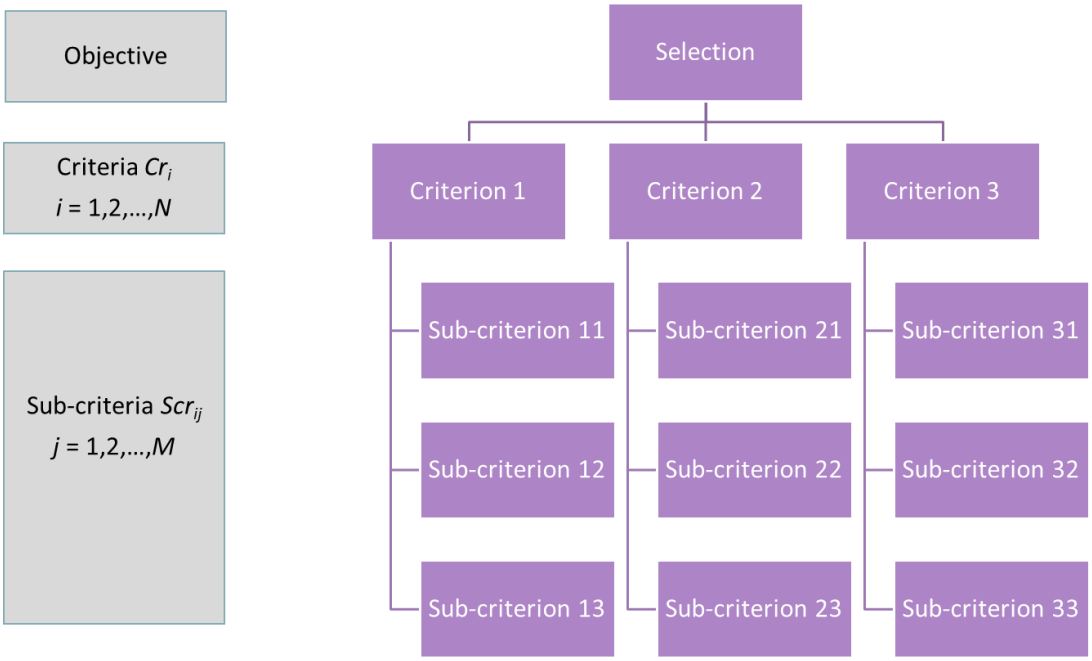


Figure 5: multi-level hierarchy

Once the hierarchical structure has been constructed and the criteria and sub-criteria determined, appropriate questionnaires are created and distributed to experts (step 2) for them to fill in. The procedure here is based upon systematic pairwise judgments of the experts from the second to the lowest level of the hierarchy: In each level, the criteria (sub-criteria) are compared pair-wisely according to their degree of influence and based on the specified criteria in the higher level. The described comparisons are performed using the standardized nine levels scale shown in Table 1.

Table 1: The Saaty Rating Scale

Intensity of importance	Definition	Explanation
1	Equal importance	The two criteria contribute equally
3	Moderate importance	Experience and judgment favour one of the criteria
5	Strong importance	A criterion is strongly favoured
7	Very strong importance	A criterion is very strong dominant
9	Extreme importance	A criterion is favoured by at least an order of magnitude
2, 4, 6, 8	Intermediate values	Used to compromise between two of the above numbers

The set of pairwise comparisons on the N criteria results in an N x N evaluation matrix $A=[A_{ij}]$ in which the elements A_{ij} (>0) represent the relative importance of criterion Cr_i as compared to Cr_j. It should be noted that $A_{ii}=1$ for all i, while the matrix $\boldsymbol{A}$ is symmetrical across the main diagonal, that is $A_{ji}=1/A_{ij}$. The same steps are followed regarding the sub-criteria of each criterion k, and the results are summarized in a similar matrix to $\boldsymbol{A}$, called $\boldsymbol{A_k}$.

The last step (step 3) towards the evaluation of the objectives is the estimation of the criteria and sub-criteria weights, w_k and s_{jk} respectively. This requires the calculation of the principal eigenvector $\mathbf{v}=[v_k]$ (or $\boldsymbol{u_k}=[u_{ik}]$) that is the eigenvector corresponding to the maximum eigenvalue λ_{max} (principal eigenvalue) of matrix $\mathbf{A}$ (or $\boldsymbol{A_k}$). The weights of the criterion k and of each of its sub-criterion j are given by:

$$w_k = \frac{v_k}{\sum_{i=1}^{N} v_i} \quad (1)$$

$$s_{jk} = \frac{u_{jk}}{\sum_{i=1}^{M_k} u_{ik}} \quad (2)$$

where N and M_k is the number of criteria and sub-criteria of criterion k respectively.

It is well recognised that AHP can be highly subjective and inaccurate, mainly due to its inability to adequately handle the inherent uncertainty and imprecision associated with the mapping of a decision-maker's perception to exact numbers. In this case, the Fuzzy Analytic Hierarchy Process (FAHP), an extension/improvement of the AHP methodology, has been proposed [34]-[36] as a means to address this uncertainty. Fuzzy numbers are used in order to model the relative importance of criteria and sub-criteria.

Let $\tilde{A}$ represent a fuzzified reciprocal *N*x*N*-judgment matrix containing all pairwise comparisons between elements *i* and *j* for all *i*, *j* ∈ (1,2,…,*N*).

$$\tilde{A} = \begin{bmatrix} (1,1,1) & \tilde{a}_{12} & \cdots & \tilde{a}_{1N} \\ \tilde{a}_{21} & (1,1,1) & \cdots & \tilde{a}_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{a}_{N1} & \tilde{a}_{N2} & \cdots & (1,1,1) \end{bmatrix} \quad (3)$$

where $\tilde{a}_{ji} = \tilde{a}_{ji}^{-1}$ and all $\tilde{a}_{ij}$ are fuzzy numbers. The use of fuzzy numbers as answers (vague comparisons), although increasing the processing complexity, provides for more accurate and meaningful results. A fuzzy weight for each criterion and sub-criterion is evaluated, while crisp weights can also be obtained through the defuzzification process.

Fuzzy numbers are a part of the fuzzy sets theory, introduced by Zadeh [37] as a modelling tool for complex systems under uncertainty. In fuzzy sets, grades of membership in [0, 1] are assigned to objects through a membership function $\mu_A(x)$. As shown in Figure 6, in the special case of triangular fuzzy numbers, the membership is defined by three real numbers, (*l*, *m*, *u*), where *l* is the lower limit, *m* the most promising and *u* the upper limit value. In the limit, *l* = *m* = *u*, fuzzy numbers become crisp numbers. Eq. (4) describes the membership function of triangular fuzzy numbers.

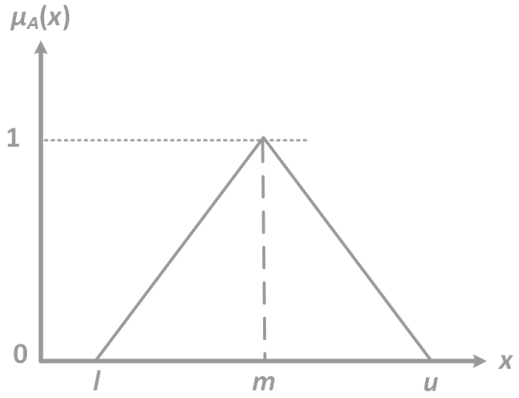


Figure 6: Triangular fuzzy numbers membership function.

$$\mu_A(x) = \begin{cases} \dfrac{x-l}{m-l}, & x \in [l,m] \\ \dfrac{u-x}{u-m}, & x \in [m,u] \\ 0, & otherwise \end{cases} \quad (4)$$

Assuming that $M_1=(l_1, m_1, u_1)$ and $M_2=(l_2, m_2, u_2)$ are triangular fuzzy numbers, the operations on them can be:

$$\text{Addition: } M_1 \oplus M_2 = (l_1 + l_2, m_1 + m_2, u_1 + u_2) \quad (5)$$

$$\text{Multiplication: } M_1 \otimes M_2 = (l_1 \cdot l_2, m_1 \cdot m_2, u_1 \cdot u_2) \quad (6)$$

$$\text{Inverse: } M_1^{-1} = (l_1, m_1, u_1)^{-1} = \left(\frac{1}{u_1}, \frac{1}{m_1}, \frac{1}{l_1}\right) \quad (7)$$

After collecting the fuzzy judgment matrices from all decision makers, these matrices are then aggregated. An approach is to combine the fuzzy pairwise comparisons using the following algorithm [36],[38]:

$$l_{ij} = \min(l_{ijk}),\ m_{ij} = \left(\prod_{k=1}^{K} m_{ijk}\right)^{1/K},\ u_{ij} = \max(u_{ijk}) \quad (8)$$

where (l_{ijk}, m_{ijk}, u_{ijk}) is the fuzzy evaluation of the sample members k (k = 1, 2, … , K). In the case of a wide range of upper and lower bandwidths (inhomogeneous evaluations), min and max operations are not appropriate, usually leading to a very large span of fuzzy numbers and allowing the aggregated fuzzy weights to exceed the predefined borders.

Therefore, the fuzzy geometric mean method [39]-[41] is used. In this case, the aggregated triangular fuzzy number of K decision makers' judgment in a certain case (l_{ij}, mij, u_{ij}) is given by:

$$l_{ij} = \left(\prod_{k=1}^{K} l_{ijk}\right)^{1/K},\ m_{ij} = \left(\prod_{k=1}^{K} m_{ijk}\right)^{1/K},\ u_{ij} = \left(\prod_{k=1}^{K} u_{ijk}\right)^{1/K} \quad (9)$$

Geometric mean operations are also used within the application of the AHP for aggregating group decisions [42].

In order to evaluate the final weights of the decision elements (criteria and sub-criteria) the popular Fuzzy Extent Analysis, proposed by Chang [34] is used. The first step towards weights evaluation is to calculate the value of the fuzzy synthetic extent with respect to the i^{th} object using the fuzzy arithmetic operations of eqs. 5-7:

$$\tilde{S}_i = \sum_{j=1}^{N} \tilde{a}_{ij} \otimes \left[\sum_{i=1}^{N}\sum_{j=1}^{N} \tilde{a}_{ij}\right]^{-1} \quad (10)$$

According to Chang's method, the possibility of $\tilde{S}_1 \geq \tilde{S}_2$ can be expressed as:

$$V\left(\tilde{S}_1 \geq \tilde{S}_2\right) = \begin{cases} 1, & m_1 \geq m_2 \\ 0, & l_2 \geq u_1 \\ \dfrac{l_2 - u_1}{(m_1 - u_1) - (m_2 - l_2)}, & otherwise \end{cases} \quad (11)$$

To compare $\tilde{S}_1$ and $\tilde{S}_2$, it is necessary to evaluate both values of $V\left(\tilde{S}_1 \geq \tilde{S}_2\right)$ and $V\left(\tilde{S}_2 \geq \tilde{S}_1\right)$. The possibility for a convex fuzzy number to be greater than *k* convex fuzzy numbers S_i, (i=1,2,…,*k*) is defined by:

$$\begin{aligned} V\left(\tilde{S} \geq \tilde{S}_1, \tilde{S}_2, \ldots, \tilde{S}_k\right) &= V\left[\left(\tilde{S} \geq \tilde{S}_1\right) and \ \left(\tilde{S} \geq \tilde{S}_2\right) and \ldots . and \ \left(\tilde{S} \geq \tilde{S}_k\right)\right] \\ &= \min V\left(\tilde{S} \geq \tilde{S}_i\right), \ i = 1,2,\ldots,k \end{aligned} \quad (12)$$

Through normalization, one can calculate the non-fuzzy (crisp) weight vector *W*, given by:

$$W = \left(\min V\left(\tilde{S}_1 \geq \tilde{S}_k\right), \ \min V\left(\tilde{S}_2 \geq \tilde{S}_k\right), \ldots, \min V\left(\tilde{S}_N \geq \tilde{S}_k\right)\right)^T \quad (13)$$

Another approach that can be implemented in order to estimate the final weights is the use of the geometric means method of Buckley [40],[41], where:

$$\tilde{r}_i = \left(\prod_{j=1}^{N} \tilde{a}_{ij}\right)^{1/N} \quad (14)$$

And

$$\tilde{w}_i = \tilde{r}_i \otimes \left(\sum_{i=1}^{N} \tilde{r}_i\right)^{-1}, \ i = 1, 2, \ldots, N \quad (15)$$

Finally, a simple centroid method can also be used to defuzzify the fuzzy weights $\tilde{w}_i$:

$$w_i = l_i + \frac{(m_i - l_i) + (u_i - l_i)}{3} = \frac{l_i + m_i + u_i}{3}, \ i = 1, 2, \ldots, N \quad (16)$$

Consistency of pairwise comparison matrices

In order to maintain a certain quality level of a decision, the consistency of the data should also be investigated during the analysis. It should be noted that the rank of the matrix ***A*** (or $\boldsymbol{A_k}$) equals to 1 and $\lambda_{max}=N$ (or M_k) if the pairwise comparisons are completely consistent. In this case, weights can be estimated by normalizing any of the columns or rows of ***A*** ($\boldsymbol{A_k}$). A consistency index (*CI*) was introduced by Saaty in 1977:

$$CI = \frac{\lambda_{\max} - N}{N - 1} \quad (17)$$

where λ_{max} is the largest (maximum) eigenvalue and *N* is the number of criteria. The final consistency ratio (*CR*), showing how consistent the judgments have been relative to large samples of purely random judgments, is given by:

$$CR = \frac{CI}{RI} \tag{18}$$

where *RI* is the random index calculated as the average *CI* across a large number of randomly filled matrices using the scale described earlier in this section. The random indices for several values of *N* were calculated by Saaty [43] and are given in Table 2. The consistency ratio should be less than 0.1. A *CR* larger than the tolerable level of 0.1 demonstrates the need to exclude the pairwise comparison matrix of this respondent for further analysis so as not to affect the overall accuracy of the results.

Table 2: RI values for different values of n

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

In the case of fuzzy pairwise comparison matrices, there are authors in the literature who do not even verify their consistency at all [44]-[46]. Buckley [40] proposed that $\tilde{A} = \left[\tilde{a}_{ij}\right]$ is consistent if and only if:

$$\tilde{a}_{ij} \otimes \tilde{a}_{jk} \approx \tilde{a}_{ik} \tag{19}$$

where $\otimes$ is the fuzzy multiplication symbol. In order to reduce the complexity, and without loss of generality, authors usually verify the consistency only for crisp matrices whose elements are the middle significant values of the triangular fuzzy numbers from the corresponding fuzzy pairwise comparison matrix [47][49]. This approach will also be used in this deliverable in order to assess the consistency of the pairwise comparison matrices. In a similar manner [53], the consistency ratio CR is calculated for the crisp matrix $N_{\tilde{A}} = \left\{n_{ij}\right\}_{i,j}^{p}$ where:

$$n_{ij} = \frac{a_{ijl} + 4a_{ijm} + a_{iju}}{6},\ i, j = 1,\ldots, p \tag{20}$$

2.5 Business Model Canvas

Business Model Canvas (BMC), as presented in Figure 7, is a strategic management template for developing new business models or documenting existing ones, developed by Osterwalder and Paigneur [54]. It is a graphical approach that describes nine elements and represents how an organization creates, delivers and captures value from a product or a service [55]. The nine elements that should be described to provide a holistic view of a business' key drivers are the following:

1. **Customer Segments**: The Customer Segments Building Block defines the different groups of people or organizations an enterprise aims to reach and serve [56].
2. **Value Propositions**: The Value Propositions Building Block describes the bundle of products and services that create value for a specific Customer Segment [54].

3. **Channels**: Value propositions are delivered to customers through communication, distribution, and sales channels. The Channels Building Block describes how a company communicates with and reaches its Customer Segments to deliver a Value Proposition [56].
4. **Customer Relationships**: Customer relationships are established and maintained with each Customer Segment. The Customer Relationships Building Block describes the types of relationships a company establishes with specific Customer Segments [58].
5. **Revenue Streams**: Revenue streams result from value propositions successfully offered to customers [59].
6. **Key Resources**: Key resources are the assets required to offer and deliver the previously described elements [59].
7. **Key Activities**: The Key Activities Building Block describes the most important things a company must do to make its business model work [54].
8. **Key Partnerships**: Some activities are outsourced and some resources are acquired outside the enterprise. The Key Partnerships Building Block describes the network of suppliers and partners that make the business model work [57].
9. **Cost Structure**: The business model elements result in the cost structure. The Cost Structure describes all costs incurred to operate a business model [57].

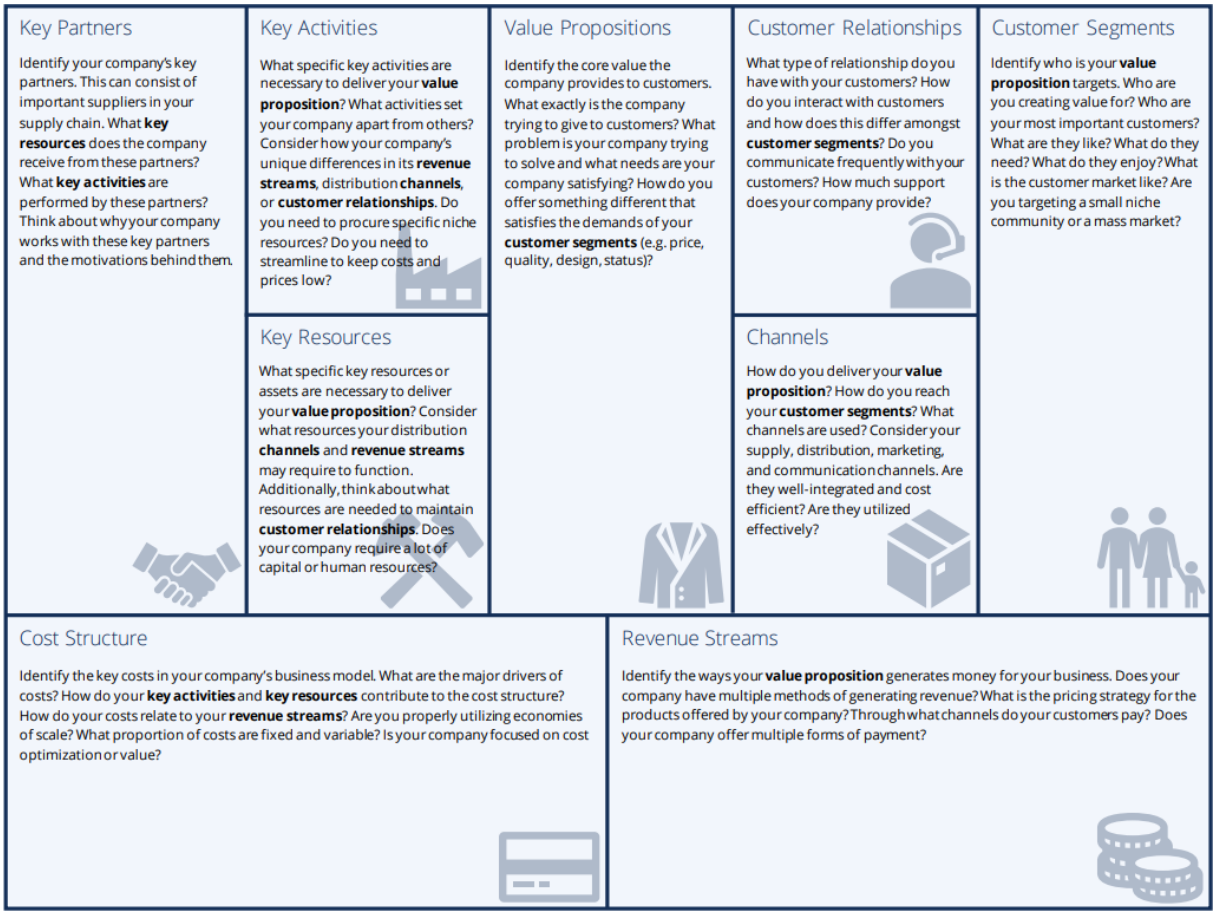


Figure 7: Business Model Canvas [57]

The BMC facilitates the process of devising and improving business strategies. It has been used to deliver and analyse business models in various sectors, including the energy sector (Li et al. [58]). A separate business model canvas analysis for each use case of the SDN-microSENSE is presented in Section 7.

2.6 Business plan activity map

An activity map is a diagnostic tool to identify an organisations competitive advantage. It connects an organisation's value proposition to the activities of the organisation that enable it to deliver its value proposition better than any competitors [60]. Activity-system maps show how a company's strategic position is contained in a set of tailored activities designed to deliver it. In companies with a clear strategic position, a number of higher-order strategic themes can be identified and implemented through clusters of tightly linked activities.

Activity-system maps can be useful for examining and strengthening the strategic fit. A set of basic questions should guide the process. An activity map can be used to:

- Make incremental decisions about whether a new idea or opportunity fits the strategy. If the new opportunity does not undermine any other aspect of the activity.
- Communicate how every function and policy contributes to the organisation strategy; it can also be used to cascade KPIs down the organisation[61].
- Identify activities that undermine any part of the activity map[61].
- Make decisions about the boundary of the organisation. It is a strategic risk to outsource anything on your activity map since this is the core of your competitive advantage. Anything not on this map is context and can be outsourced and managed for cost-effectiveness [62].
- To make organisation decisions for new ventures or acquisitions. If the activity maps of the businesses are very different, combing them in the same organisation will create trade-offs, and they are better off separate, even if this increases the cost base [62].

3. SDN-microSENSE PESTLE analysis

The general environment of an industry is one that affects all companies in a certain sector equally. For this, it is necessary to take into account the political, economic, social, technological, legal and social environment. To carry out this analysis, PESTLE analysis is used, which was presented in previous section. It is used to assess the current situation of the company, identifying the main external forces that affect the business and also helps in planning the strategy.

In the next sections, the PESTLE analysis of the SDN-microSENSE is presented in detail.

3.1 Political analysis

Political stability and local political conditions: The European Union (EU) is a political and economic union of 27 member states [63]. All member states of the EU are stable democracies with democratically elected governments. Moreover, member states that participate in the economic union enjoy a degree of economic protection, which is a factor favouring their local political stability. Additionally, region political stability is increasing with extremist group attacks reducing from 2015 to 2018 .

Government regulations: Although each EU member state enforces their local regulations regarding labor, trade and production of goods and services, all members have to align with the general directions of the EU high standards. Thus, within EU borders, businesses have access to a high-quality labor force, a fair and clear trade regulatory framework and a properly organized supplier and buyer network with high-quality standards. This creates a solid ground for sustainable business growth. Another important point is that the EU greatly facilitates trade between members states since they do not impose quotas, tariffs and additional taxes on goods and services traded between them.

In the field of energy, governments in the European Union are working towards the establishment of a modern, interconnected and secure energy grid across Europe. The EU has adopted a comprehensive European Union Energy policy based on Article 194 of the Treaty on the Functioning of the European Union [64], where provisions on a common EU energy policy were introduced. This policy, also known as the Energy Community Treaty [65], defines the rules for the operation of the energy market, the security of energy supply, the energy efficiency, the integration of renewable energy sources and, last but not least, the interconnection of the electricity networks of Europe. This adopted policy is favourable for launching the SDN-microSENSE product, which addresses the issues of secure energy supply and grid resilience.

In the field of Critical Infrastructure Protection (CIP), the European Commission has developed the European Programme for Critical Infrastructure Protection (EPCIP) [67] action plan and policy framework, which aims to improve the protection of critical infrastructure and pays special attention to the security of communication networks and information systems. From this perspective, the EU has adopted the Policy on Critical Information Infrastructure Protection (CIIP) [68] that focuses on the protection of Europe from cyber threats and aims to strengthen cybersecurity capacity of the member states. These initiatives aim to align the EU's complex cybersecurity landscape and national government planning [69] on cybersecurity strategies aiming to develop a truly unified EU Cybersecurity Strategy. A foundation for strategic cooperation level has already been set, and it is widely accepted that coordination among EU institutions and Member states will ensure policy alignments and generate synergies among the member states. The stability and homogeneity of the regulatory framework in the EU can provide a solid ground for launching our product.

Furthermore, there are upcoming regulations regarding data exchange, data protection and cybersecurity. Although most of them will promote the usage of privacy-preserving systems and secure by design, it is difficult to foresee what these new regulations will dictate. This creates uncertainty on how technologies should be built to be compliant with future regulations. For example, a proposal for the ePrivacy Regulation [70], which is a regulation that has been discussed for many years, has just been recently released. Furthermore, the European Commission supports the development of European Cybersecurity standards and aspires to promote a Single Market for Cybersecurity products in the EU. These evolutions in the cybersecurity Market create a positive environment for the deployment of the SDN-microSENSE solution, which will be compliant with the evolving EU regulations and legislation.

Procurement regulations: All EU members have to align with the current EU policy regarding procurement regulations. Suppliers have to abide by the respected restrictions to ensure the quality of the products or services rendered.

Final verdict: Opportunities for the deployment of the SDN-microSENSE solution have arisen, based on the aspect that our product is regulatory-compliant. Overall, The EU political situation can be assessed as favorable for launching our product.

3.2 Economic analysis

Local economic conditions and stability: Yearly forecasts indicated an increase in EU growth rate for 2020, reaching an average growth rate of 1.4% [71]. However, due to the ongoing COVID-19 pandemic, the EU economy is now expected to contract by 8.3% in 2020 and grow at a rate of 5.8% in 2021 [72]. The growth rates of the EU are not high since the vast majority of member states are already developed economies. Still the EU manages to sustain a positive average metric overtime. Thus, the market space is expanding. Moreover, EU member states are aligned to a low-interest rate policy creating a favorable environment for creating new businesses and launching new projects.

To achieve those low and harmonized interest rates the EU members have agreed upon harmonizing their inflation rates. As a result of those policies, inflation rates in the EU zone are now estimated at 1.4% (2019) [73], and they are expected to remain at that level for 2020. Low and stable inflation favors stable prices in goods and services, thus facilitating the generation of more stable revenue models. Thus, the economic stability of the EU can be characterized as high.

Saving Costs: The SDN-microSENSE solution supports the stability and security of the European power grid. It follows a proactive approach against cyber-threats, detecting, preventing and protecting from cyber-attacks, thus saving an organization from the high costs of a cyber-attack recovery Furthermore, the SDN-microSENSE solution, which can balance demand and supply in a microgrid or in a specific substation area, can be utilized by TSOs to defer grid investments and thus reduce their operational costs. Furthermore, the SDN-microSENSE will be compliant with the future implementation of the European Single Market in Electricity [74], where energy trading across European countries will play a key role, substantially lowering electricity prices and making electricity production less profitable if the electricity is fed to the electricity market. The SDN-microSENSE solution offers a unique energy-trading approach that supports the energy communities approach, optimizes self-consumption and maximizes the profitability of RES installations

Foreign exchange fluctuations: The majority of the members of the EU along with candidate countries for future membership, are using the Euro as a common currency for their transactions. Thus, the risk

of exposure to foreign exchange fluctuations is significantly reduced thus making profitability forecasts more dependable.

Subject to sales tax: Our products and solutions are subject to sales taxes with a range of 10%-27% depending on the country of sale.

Final verdict: The economic environment for launching of new products can be assessed as favorable. More specifically, the compatibility of our solution with the future operation of the single European electricity market renders our product competitive and innovative.

3.3 Social analysis

Social factors are all those factor that affect the attitudes, interests and opinions of society, influencing their purchasing decisions. The most relevant are:

Demographic factors / Population growth: The population of the EU is estimated to be 513 million [75] which categorizes it as the fourth biggest market in the world. Moreover, the EU population is expected to increase in the forthcoming decades reaching an all-time high of 525 million in 2044 [76]

Labor Market: The EU employment rate has shown an upward trend in the past years. For example, in 2018, EU employment rate reached 73.2% [66]. Due to the effects of the COVID-19 pandemic, the unemployment rate has risen for the past few months. The EU unemployment rate was estimated at 6.6 % in April 2020, up from 6.4 % in March 2020.

Free Movement: The free movement of workers is a fundamental right guaranteed by the Treaty on the Functioning of the European Union (EU). Therefore, EU citizens are entitled to: look for a job in another EU country; work there without needing a work permit; reside there for that purpose; stay there even after employment has finished; and enjoy equal treatment with nationals in access to employment, working conditions and all other social and tax advantages. Moreover, the border-free Schengen Area guarantees free movement to more than 400 million EU citizens

Business sustainability: EU policies aim towards creating a ground for healthy and sustainable business development. The core of those policies is taking form under the Sustainable Development Goals [77] that the EU has created. In 2018 a plan was put into place, introducing seventeen goals to be implemented by member states. By following a sustainable growth policy, EU member states become an ideal environment for nurturing new business models.

Final verdict: Social factors can directly or indirectly influence a company's operating environment. EU is estimated to face a shortage of 800,000 qualified Information Technology (IT) workers in 2020 [78], thus influencing the availability of workforce for IT companies. On the other hand, the low unemployment rate indicates economic and social stability. For these reasons, the social environment can be considered as neutral for our product.

3.4 Technological analysis

Technological factors are all those related to the state of technological development and its presence in business activity.

Technological development level of European Union: European Union is one of the top world-leaders in technological development. Regarding technological skills, in Europe there are highly-skilled power engineers, and developers, which is an important factor for the process of selection and recruitment of employees for a company. In professional skills, Europe has an important percentage of experts in the domains of Cybersecurity and Grid operation.

Rapid advances in technology: SDN-microSENSE implements a set of solutions and tools that are based on novel technologies, such as information security, privacy-preserving and decentralized technologies. Information security tools protect end-users from unwanted intruders, theft of assets, identity theft, loss of privacy and confidentiality. Privacy preservation focuses on the protection of user's privacy and sensitive data protection. Furthermore, Blockchain is a new general-purpose decentralised technology to revolutionize business activities and interactions in the future, considering its economic, political, humanitarian, and legal system benefits.

This ever-changing technological ecosystem can also have negative consequences. Some technologies, tools and even platforms can go obsolete fast. Besides, there are some concerns about the security of these innovative systems and tools. Advances in artificial intelligence, computing, and wireless networks have made technology faster and more reliable, but these solutions could potentially cause new cyberthreats. This environment is considered as favorable for the deployment of the SDN-microSENSE's privacy-enabled and resilient to cyberattacks tools

Protection of critical infrastructure: New ways and concepts of dealing with security concerns are always on high demand, with the European Union currently paying special attention in the protection of critical infrastructure, like the power grid, from cyber threats. Moreover, the smart grid cybersecurity market is expected to reach 12.3 billion dollars by 2026 [79], providing unique growth opportunities to projects like SDN-microSENSE. Another important indicator of the market trend is the increasing global market value of cybersecurity, which is expected to reach 259 billion dollars by 2025 [80].

Cybercrime has recently shifted from attacking big corporations to attacking critical infrastructure, like the electricity sector. This trend has been rising for the past decade, with cybercriminals conducting sophisticated cyber-attacks against electricity networks. Most notably, the 2015 cyberattack against the Ukrainian power grid was the first successful cyber-attack that caused a widespread power outage [81]. A big issue regarding the protection of the power grid is that, today, electrical switches and circuit breakers are electronic and can be programmed to perform various functions, while the operation of the entire electrical network depends on them. However, each electronic component, sensor or IoT device represents a possible entry point for a cyber-physical attack. Thus, vital protective measures must be implemented in order to minimize the risk of future cyber-attacks against the power grid.

Information security standards: The introduction of information security standards in the EU similar to the NIST framework [82], COBIT [83] or ISO/IEC 27002:2005 [84] would greatly facilitate the launch of SDN-microSENSE.

Increase of connectivity: The data, along with the devices themselves, are creating the Internet of Things (IoT) – a connected infrastructure of smart grid components, Supervisory control and data acquisition (SCADA) systems, sensors, IoT devices, software applications and electrical systems. The IoT in the smart grid era is rapidly transforming the traditional power grid roles, stakeholders and relationships. The technological advancements, the introduction of the two-way-communication between energy operators and consumers, and the use of IoT devices modernizes the grid operation, minimizes costs and enables remote operation and reliable grid monitoring.

R&D activity: There' been increasing interest from a market perspective for more cybersecurity solutions on the ICT of the Power Grid. From a European Union perspective, the EU is interested in positioning the continent as the leaders in smart grid technologies, funding several H2020 projects on the subject. The same can be said about cybersecurity. From a market perspective, various consultancy firms have reported that there is an increasing interest from companies on solutions that enhance the security and resilience of ICT Systems for the power grid.

Final verdict: The technological aspects in the EU are considered to be favorable for launching our product.

3.5 Legal analysis

GDPR Regulations: The General Data Protection Regulation (GDPR) [85] harmonizes the national legislations of the EU member states, deriving from the Directive 95/46 on data protection. The GDPR was adopted in May 2016 and, after a 2-year adjustment period, is now applicable since 25 May 2018. Since that date, all entities concerned must comply with the new rules when processing personal data. There are 99 articles – or, the actual enforceable laws –, in the EU GDPR, grouped into 11 chapters. Within these chapters, issues such as rights of the data subject, controllers, processors, provisions etc. are being described thoroughly.

The harmonization that the GDPR offers creates a common framework for all EU member states thus making it easier for companies to align the architecture of their services and products with that framework to avoid legal consequences.

One of the biggest changes that has come from GDPR is the definition of personally identifiable information (PII) [86]. Under article 4, the definition of PII in the GDPR is "any information relating to an identified or identifiable natural person ('data subject')". Therefore, metadata that is related to an individual, such as a MAC address or even smart grid data is also considered PII, adding an extra layer of complexity. This is a favorable situation, because as privacy legislation tightens, the necessity of secure and privacy-preserving tools for data exchange and management increases.

Moreover, GDPR has stated that all system should be created by Privacy-by-Design and default, as stated in article 25. This implies that data protection should be a major concern in every organization that is either processing data (such as storage, usage, exchange, *interalia)*. Consequently, in order to be compliant with the GDPR, all-digital system that work with personally identifiable data should consider data protection and security pivotal for their systems.

In addition to the GDPR, there have been discussions on replacing the ePrivacy directive with the Regulation on Privacy and Electronic Communications (ePrivacy Regulation). It is still unclear when the ePrivacy regulation will enter into force, as it is still being discussed in the EU bodies. The ePrivacy

regulation comes in hand with the GDPR, to align the privacy rules and as part of the strategy of the EU Digital Single Market. The new regulation will affect a broader set of players, will apply stronger rules, have more effective enforcement, among other elements.

In the absence of an agreement between the European Economic Area (EEA) and the United Kingdom (UK) (no-deal Brexit), the UK will become a third country, and this will surely affect all the use cases, from data processing, exchange, storage, usage and others. Since there is still great uncertainty over the specifics of Brexit, the impact of this element should be considered as neutral.

Finally, although the GDPR provides a common legal framework for all EU member states it is a relatively new regulation with little to none legal precedent in most countries. This creates a certain level of uncertainty regarding the proper alignment of products and services with GDPR and the legal implications in case of failure to align. The impact of this element can be considered as neutral.

Data protection by design: It means that a company should take data protection into account at the early stages of planning a new way of processing personal data. In accordance with this principle, a data controller must take all necessary technical and organizational steps to implement the data protection principles and protect the rights of individuals. These steps could include, for example, using pseudonymization.

Data protection by default: It refers to the fact that only personal data that is strictly necessary for the purpose of treatment is subject to treatment. In other words, regardless of the data set collected by the data controller, the data controller must compartmentalize the dataset and limit access to personal data only when it is strictly necessary.

Data protection legislation supports the development of security as a service. However, different legislations in the EU versus non-EU countries might apply, affecting global interoperability for different technical solutions and services. As the development of the SDN-microSENSE platform will take part within an EU setting it will be GDPR compliant by design. The GDPR operates in a wide scope, protecting any data that can be used to directly or indirectly identify a living person (PII). In this sense, there will be much higher legal demands in developing a new product or service in the present context. However, the need to protect any PII will ensure interoperability in multiple settings and reduce the risk of unnecessary privacy breaches and legal fines.

Final verdict: SDN-microSENSE provides a set of secure, privacy-enabled tools that are GDPR compliant. The developed solution will adopt a privacy (and data protection) by design and default approach. Concluding, the legal environment can be considered as favourable for the launch of SDN-microSENSE.

3.6 Environmental analysis

Sustainable Energy: The EU, under the Kyoto Protocol [87], has set itself the target of reducing greenhouse gas emissions by 8% in 2012 and 20% in 2020 compared to 1990 [88]. SDN-microSENSE solution facilitates the integration of Renewable Energy Sources both to microgrids and to the main grid, assisting in EU's target of decarbonisation of energy sector, and optimizes the overall grid operation. The installation of new infrastructure must however, be carefully studied to avoid consequences in terms of environmental pollution (i.e., use of materials that cause environmental pollution).

The SDN-microSENSE solution aspires to have a positive impact on the environment by:

- Promoting the transition towards distributed generation, thus modifying the existing balances between centralized and decentralized electricity generation significantly;
- Utilizing IoT components and control devices that are capable of giving great flexibility to the electricity supply and demand.
- Optimizing the use of distribution networks, thanks to grid intelligence at distributed points of the network (e.g. in the microgrid's Point of Common Coupling (PCC) to the main grid);
- Improving the quality of electrical energy distribution;
- Facilitating the integration and management of distributed energy resources (Photovoltaic (PV) generation, wind energy, minimization of fossil fuels etc.)
- Managing local congestion in distribution networks;
- Enabling Demand side management through supplier-prosumer interaction

Sustainable green cloud: On May 16th 2019, the Commission's Information Technology and Cybersecurity Board approved the new Cloud Strategy of the European Commission [89]. This is a major step forward in Commission's cloud journey which started already in 2014. This strategy includes Energy-efficiency in line with the overall EU priority of lowering carbon footprint and with green public procurement policy.

As many of our digital activities will be cloud-based in the future, it is essential that cloud computing becomes as sustainable as possible. That is why cloud service providers should take their responsibility and continue to work on improving production processes, for example by making their cooling systems for data centers more efficient

Corporate and Social responsibility/ Responsible Business Conduct: EU citizens rightly expect that companies understand their positive and negative impacts on society and the environment. And, therefore, prevent, manage and mitigate any negative impact that they may cause, including within their global supply chain. The EU has an essential role in supporting and encouraging companies to conduct their business responsibly. The EU Commission adopts a strategy for corporate and social responsibility (CSR) that is to be followed by all EU member states. The impact of this strategy can be considered as positive since the EU provides benefits for companies abiding by the CSR regulations and although restrictions exist, they foster a ground for sustainable business development

Final verdict: The environment in the EU is considered to be favorable for launching our product.

4. SDN-microSENSE Porter's Five Forces Analysis

The objective of this section is to carry out an analysis of the business environment of the SDN-microSENSE solution using the Competitiveness Model proposed by Michael Porter. This analysis demonstrates how the five forces directly affect the internal operation of companies, frequently conditioning their strategies and, therefore, influencing their results. The internal dynamics of the company and the speed and way in which the environment moves, have to be treated as a whole when carrying out this analysis, which will reveal the strategies to follow in order to create a viable product in an increasingly competitive market.

An overview of the conducted Porter's five forces analysis on SDN-microSENSE is presented in Figure 8. The detailed SDN-microSENSE Porter's Five Forces analysis is presented in the following subsections.

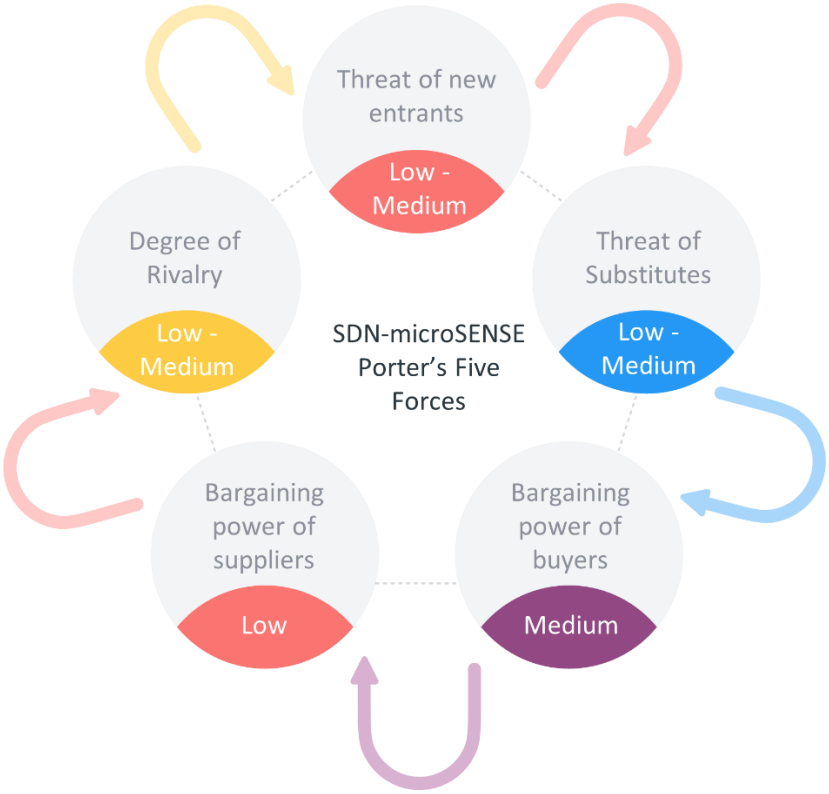


Figure 8: SDN-microSENSE Porter's Five forces Analysis

4.1 Bargaining power of suppliers

Sensory equipment, hardware and software are very important for the protection of the Electrical and Power Energy Systems in the era of the Smart Grid and the Internet of Things. With the appearance of IoT, operating systems and sensors are required to improve the functionality of the grid. All these technologies are owned by certain companies that have very high bargaining power since the manufacturers are not experts in the field. Furthermore, if the supplier is highly dependent on a company in order to be able to sell its products, the latter will have very little bargaining power. We can take the example of ENEL, EDF or Engie, which are some of the biggest electric companies in the world and place a large number of orders for various grid components. Due to their order volume, the supplier has very little negotiating power in the sense that if he loses the contract with these companies, this could negatively affect his business.

List of suppliers (hardware, services, software etc.):

- **Cybersecurity service providers**. In the EU market, there are around 1000 large and medium-size enterprises of which around 10 of them are the key players. Hence, there is a strong competitor's ecosystem.
- **Cloud service providers (CSP)**: They must be European. As a processor, the CSP is legally subject to and accountable for specific obligations (Articles 28, 29 and 30 of the GDPR).
- **Smart Grid ICT Application Providers** (i.e. IT service providers, IT product developers, Third-party consulting services, Smart Grid vendors, IoT devices developers and ethical hacking service providers): There are many cybersecurity companies, but this is a very critical aspect for trust and reliability.
- **Hardware suppliers:** We require the usage of computers for the creation of the service for the Use Cases, as well as the acquisition of sensors and specialized equipment for the implementation and testing of the SDN-microSENSE solution (HIL equipment, SDN controllers ect.) These hardware requirements can be easily found in the market, which is already a competitive market.
- **Blockchain technology:** Every blockchain technology has its own programming language and thus, mastering a platform requires resources and time to adapt. There might be potentially some evolutions in the blockchain technology that may affect the costs. For example, currently the Hyperledger technology is free to use, yet this might change in the future (although it is unlikely). In this case it might be necessary to adopt another blockchain ecosystem. This implies that the adopted blockchain technology in SDN microSENSE has certain power over our Use Cases; however, there are other alternatives in the market to migrate.
- **Communication Providers:** Telco providers must provide communications that guarantee a secure and private European network for the SDN-microSENSE Platform.

Verdict: The **supplier power** is determined from the list of different suppliers that range from cloud services providers and smart grid vendors to common computational hardware needed to run the SDN-microSENSE platform. The whole project relies on many suppliers, and there is low-medium completion among them. However, by using long term supply contracts, it's possible to mitigate risks and power of suppliers is subject to the price of fluctuations. Since there are several suppliers for these services and components, their bargaining power is **low.**

4.2 Bargaining power of buyers

The relationship with customers is an aspect of the sector that must be taken into account since the attractiveness of the sector and the profitability potential is widely related to the dominance of the relationship by the buyers. The Internet has facilitated access to information by the byers, which has the effect of increasing the buyers' negotiating power vis-à-vis the organization, favored by the availability of all the necessary information at the time of purchase of products or services. Therefore, the improved information acquisition by the clients has led to greater negotiation capacity and, as a consequence, a decline in expected profit margin for current and potential organizations in the sector of cybersecurity.

Since at the moment there are few, if any, solutions in the Electrical Power and Energy System (EPES) cybersecurity field, buyers will not have much bargaining power. In the case that two competitors offer two different variants of the same product, the buyer will somehow have bargaining power over the

price of the product. In the upcoming years, the cybersecurity for the Smart Grid market is expected to become highly competitive. The more companies that manufacture/ offer a similar product, the more the buyer will have strong bargaining power since he will be able to make a choice among multiple solution providers. A list of buyers that are targeted by SDN-microSENSE solution is provided below:

- **Distributoion System Operators (DSOs):** SDN-microSENSE should aim to enter the market through direct sales. In general, switching costs (training the personnel) for the DSO is high. SDN-microSENSE could target for 15-year contracts, with the DSOs having bargain power regarding the specifications, but little on the prices of the products. Overall, the bargaining power is medium, since there is a limited number of available solutions on the market.
- **Transmission System Operators (TSOs):** Entering the market through public tenders. Bargaining power is high due to the limited number of TSOs in Europe (43 TSOs across 36 countries of Europe). Furthermore, new products have to be compliant with GDPR directives into force.
- **Energy providers/suppliers:** Entering the market through direct sales. Switching costs (training the personnel) for an energy provider is high. SDN-microSENSE could target making long-term agreements with energy providers. Overall, the bargaining power is low, since there is also a limited number of available solutions in the market.
- **Demand Response aggregators:** SDN-microSENSE should enter the market through direct sales. Energy Aggregators are organizations who utilize the bargaining power of their customers in order to negotiate lower energy costs and achieve better agreements. The bargaining power is expected to be high, since the energy aggregators will have low switching costs and will, more probably, negotiate agreements collectively.
- **Energy communities:** It is still unclear when the energy communities will emerge as a key player in the energy mix. SDN-microSENSE should enter this market through direct sales. It could target making long-term agreements with the energy communities. The bargaining power of the energy communities is medium, since there is a limited number of energy communities and a limited number of alternative products on the market.
- **Microgrid operators (i.e. Critical Infrastructure, Army Bases, Universities):** SDN-microSENSE should enter the market through direct sales or, where applicable, through public tenders. In general, switching costs (training the personnel) for a microgrid of Critical Infrastructure is moderate. SDN-microSENSE should target for long-term contracts with this type of customers. The bargaining power is low, since they are expected to purchase cybersecurity products in low amounts. Additionally, there is not a wide variety of alternative products that would result in competitive pricing strategies.

The SDN-microSENSE solution is unique, combines a variety of tools, and currently, it is difficult to find another specific supplier in the market. In addition, and as already specify in substitution competition, the cost of migrating a whole system to another is expensive, meaning there will be incurred costs in case of switching between the alternatives.

However, the product is price sensitive. These organizations currently do not allocate a big portion of their budget on cybersecurity. In fact, the budget tends to be limited, as it is difficult to see the direct results of the implementation. Furthermore, cybersecurity tools tend to be costly. In addition, there are various cybersecurity tools out in the market, making it a highly competitive market. Although SDN-

microSENSE is very different from other technologies out in the market (as it is a dedicated solution for Electrical Power and Energy Systems), it is still important to understand that there will be competition by other cybersecurity tools.

Verdict: Purchasing power is related to the lack of buyers in any given market. In the case of the energy sector, the number of potential buyers is sensitive to the price change. Potential buyers are willing to spend much in order to be protected. However, it's not feasible for the buyers to compare the different alternatives with the information on the web, but extensive research is needed. As more options arise, margins will decrease in this industry. Thus, **buyer power** can be assessed as **medium**.

4.3 Threat of new entrants

Considering ***threats of new entries***, the barriers are set quite high since the technology behind SDN-microSENSE is quite advanced and each developed tool is a result of top-notch research and development activities. Hence, there is a prerequisite for both financial, technical and intellectual requirements to enter this market. Additionally, the diversity of the SDN-microSENSE consortium partners brings great access to different channels of distribution through each partner's present contacts and network.

The possible threat of new competitors may be due to any of the following factors: the current attractiveness of the sector, the reaction from established competitors in the sector and the existence (or not) of entry barriers.

Barriers to entry, if they are absolute, will be impossible to overcome. On the contrary, if these barriers are relative, they can be overcome with the application of ICT technologies. Indicatively, as an example of a relative barrier to entry, the introduction of ICT has modified the concept that only large companies, with economies of scale, could access the automation of production processes that require large financial outlays. Thanks to ICT, this concept has changed, thus reducing the barriers to entry.

On the other hand, entering the smart grid and cybersecurity market and cybersecurity has substantive capital requirements. The use of ICT implies the use of certain technology that involves an outlay which, on certain occasions, is significant. If an organization wants to become part of the cybersecurity market, it will need to make a certain economic investment to catch up with its competitors, which becomes a barrier to enter into the sector. Expertise in Smart Grid Systems and microgrid operation, as well as Blockchain knowledge, from an IT and Computer Science perspective, are still considered as niche knowledge, that demands high levels of specialization. Therefore, experienced personnel (developers, operators) with high employment cost is needed to perform the activities. Moreover, as cybersecurity in the smart grids and blockchain are considered as novel technologies, investment into R&D and the latest trends is necessary. This factor translates into low levels of threats of entry.

Furthermore, given that the targeted cybersecurity market is not yet fully developed in the specific sector of critical infrastructure, it is obvious that the first to succeed in reaching a comprehensive solution will have a definite advantage; in this case, we are talking about first-mover advantage. Indeed, the first entrant will often benefit from the recognition of the consumers who will trust him. It will be also easier to further develop its solution by analysing consumer expectations in particular.

However, other important elements also affect the threat level. The incumbency advantages are low. The major incumbency advantage comes from having experience in building cybersecurity systems.

There is a number of solutions on the market, including open-source solutions that provide open and free platforms. There is no necessity for raw material (except for some necessary equipment like sensors and hardware), apart from having access to IT systems, nor geographical advantages.

Even more, various governments in Europe and the European Union are fostering the development and implementation of measures that protect critical infrastructure. For example, the European Union has established an initiative on Critical Information Infrastructure Protection (CIIP), which aims to strengthen the security and resilience of vital ICT infrastructure, thus supporting research and projects related to the subject

In addition, the European Union has also decided to promote new ideas and research in cybersecurity. This has made the cybersecurity and the power grid market a fast-growing market that is appealing to investments. Thus, taking the incumbency advantage solely, government restrictions (or promotion in this case) and market growth, the level of threat of entry is high.

Switching costs can be high should there be a signed agreement between the vendor and the buyer. That would discourage buyers to switch from one product to another once they have adopted SDN-microSENSE solution. Thus SDN-microSENSE, being an early launcher, would possess an advantage against to-be-developed similar products.

Channels of Distribution: There is a difficulty accessing the channels of distribution as a new entrant, whereby the already established channels of access is limited to larger corporations and brand names, making it extremely difficult and costly to create these channels without prior connections.

Verdict: It is not easy to start a new business in this industry as much experience is needed; high levels of human capital and investment are needed. The buyer's switching cost is low, but the bargaining power of suppliers is increased. However, the power grid cybersecurity market is also a fast-growing and attractive industry with low customer loyalty for non-established companies, making it easy for buyers to switch to alternatives. Analyzing all the factors together, gives us a **low-medium threat of entry**.

4.4 Threat of substitute products

Substitute products are those that perform the same function for the same group of consumers, but are based on different technology. They are also considered as a force that determines the attractiveness of the industry. In this sense, these products constitute a permanent threat to the extent that the substitution can always be made. They represent a serious threat to the SDN-microSENSE solution if they meet the same needs at a lower price, with superior performance and quality. The entry of substitute products, depending on their quality, availability, costs and performance, regulates the price that the SDN-microSENSE solution can be charged before consumers opt for a substitute product.

As explained earlier, there is increasing competition in the field of cybersecurity. It is therefore necessary to analyze the SDN-microSENSE solution and its components in order to see if substitute products could emerge and become a threat to our solution. It is important to perceive that these threats can be aggravated when, under the impact of a technological change, the quality-price reality of the substitute product changes in relation to the quality-price of the market's reference product.

There are currently many solutions for cybersecurity, making buyers look at other options. However, the SDN-microSENSE platform diversifies from many other products by focusing on the field of Power systems and increasing the reliability, security and efficiency of critical system operations. Furthermore, the SDN-microSENSE solution brings together a variety of Cybersecurity and Smart Grid tools in one product, integrates blockchain technology and complies with the GDPR.

The value proposition of SDN-microSENSE, is that it solves cybersecurity and grid operation concerns, through the usage of novel technologies (i.e. honeypots, blockchain). Particularly, SDN-microSENSE provides a robust, distributed and effective IT cyber-defense system for large-scale EPES ecosystems that prevents and addresses disruptions to the SCADA and Industrial Control Systems (ICS) infrastructure and delivers at the same time an energy trading platform for secure and flexible trading management.

A list of competitors and their offered substitute products can be found on Table 3. None of those products provide the full list of services that SDN-microSENSE does but they provide similar services.

Table 3: SDN-microSENSE Competitive Products

Product Name	Company	Product Characteristics
IBM QRadar SIEM[90]	IBM	Security information and event management (SIEM) solution that offers: Log management; analytics; intrusion detection; data collection; risk modelling analytics to emulate attacks; insider threat detection; sense analytics
McAfee Enterprise Security Manager SIEM [91]	McAfee	SIEM solution that runs via active directory with the focus on system security. It compiles and correlates disparate data
ArcSight Enterprise Security Manager [92]	ArcSight	SIEM solution that can compile logs of big data. It also provides security orchestration, multi-tenancy & unified access matrix
AlienVault OSSIM [93]	At&T Cybersecurity (Open Source)	Probably the most popular Open Source SIEM platform. It includes key SIEM components, namely event collection, processing and normalization, and event correlation
Trustwave Enterprise SIEM [94]	TrustWave	SIEM solution that is suitable for diverse ICT infrastructure organizations. It provides automated analysis by a cloud engine, unified data storage of logs, events, alerts, findings and incidents as well as threat management
Kaspersky Endpoint Security[89]	Kaspersky	Endpoint security solution that eliminates vulnerabilities, helps in preventing loss or theft of confidential business data and uses encryption to prevent data being accessed by cybercriminals
IBM Security Guardium[96]	IBM	Security solution that simplifies organization's Data Security architecture and protects all types of data from growing threats across diverse on-premises, hybrid, and public cloud environments, by using data activity monitoring and alerting, encryption, blocking, masking and advanced data security analytics
LogicGate Risk Cloud [97]	LogicGate Inc	IT and Security Risk Management platform connecting IT risk Processes across an enterprise. Its process automation

		enables organizations to transform mission-critical risk and compliance activities by enhancing controls, increasing flexibility, and reducing risk
LogicManager ERM Software [98]	LogicManager	A successful IT risk management, security, and privacy solution consisting of an Enterprise Risk Management (ERM) program. It provides an effective Risk-based Approach for Governance Activities.
CURA ERM [99]	Cura Software Solutions	An ERM software offering solutions in the fields of project risk management, enterprise risk management, operational risk management and incident risk management. It enables organizations to better manage risks by embedding and integrating risk management in business processes, linking risk management directly to decision making and by monitoring organizational and individual performance against goals and objectives
BitSight Cyber Risk Management Solution [100]	BitSight	It is a cybersecurity Risk Management tool that focuses on external cyber risk management and optimizes an organization 's third-party risk management program. It offers a platform for quantifying the external cybersecurity posture of organizations using publicly accessible data. Furthermore, it can evaluate the performance of an organization's cybersecurity program through broad measurement, continuous monitoring, and detailed planning and forecasting in an effort to measurably reduce cyber risk
IBM Spectrum Protect Plus [101]	IBM	It is a data protection solution that provides near-instant recovery, replication, retention, and reuse for Virtual Machines (VMs), databases, and containers in hybrid multi-cloud environments
Rubrik Polaris Radar [102]	Rubrik	It leverages machine learning to detect anomalies, analyze threat impact, and accelerate recovery to minimize business impact in the event of an attack. It makes easier and faster to recover from security attacks while providing greater intelligence on how an incident impacted a company's global applications and data.
SolarWinds N-central [103]	SolarWinds	This Remote monitoring and management solution can manage devices in a complex environment. It automatizes several functionalities such as device setup, self-healing responses, ticket creation and management, etc. It supports multiple types of devices such as endpoints, servers, network devices, virtual machines, mobile and IoT devices, etc.

Verdict: The threat of substitutes concerns the availability of alternative products or methods to achieve a goal that exists in the market or may exist in the market. It is not easy to find many alternatives to cybersecurity tools and services for the energy sector in the market. The substitutes are

only available through selected vendors. This happens due to the consistently advancing technology. The risk of **substitute products** can be assessed as **low-medium**.

4.5 Industry rivalry

Industry rivalry refers to existing companies that provide a similar solution. Within Horizon2020 calls, six other projects develop solutions that address cybersecurity-related aspects in the power grid. More details on these projects are presented in Table 4. Even though synergetic activities are present, they must be considered as future competitors at later stages in the deployment of each of the projects' products, as we are expected to compete for similar market segments. Moreover, there is an abundance of cybersecurity companies that provide different tools to their customers. Big firms are fighting to gain the largest share of the market, while other companies expand their solutions within this market in view of the economic prospects that this could generate. The rivalry between these companies is therefore high as, on the one hand, there are numerous solution providers, while, on the other hand, there is a challenging R&D environment that aims to develop innovative products to penetrate the market.

Table 4: H2020 Projects Related to SDN-microSENSE

Project Acronym	Description	Comparison with SDN-microSENSE
EnergyShield [104]	EnergyShield is an H2020 project that implements an Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures.	SDN-microSENSE also integrates a bundle of tools in a holistic cybersecurity solution that includes monitoring, assessment and protection of critical infrastructure. Moreover, SDN-microSENSE with its tool facilitates the optimal and dynamic operation of the distribution grid and integrates innovative energy concepts such as energy trading, while it also follows a privacy by design approach
SPEAR [105]	SPEAR project aims at a) detecting and responding to cyber-attacks using new technologies and capabilities, b) detecting threat and anomalies timely, c) developing all-in-one security detection solutions, d) leveraging advanced forensics subject to privacy-preserving, e) confronting Advanced Persistent Threat (APT) and targeted attacks in smart grids, f) increasing the resilience of the smart grid innovation, g) alleviating the lack of trust in smart grid operators and h) empowering EU-wide consensus.	SDN-microSENSE leverages on the developed tools of SPEAR and moves one step forward by extending with novel tools and algorithms and integrating them in the SDN-microSENSE platform. Moreover, SDN-microSENSE inserts the concept of cybersecurity to flexible sources, expanding its applications and resulting in secure and flexible power infrastructure.
PHOENIX [106]	PHOENIX aims to offer a cyber-shield armour to European EPES infrastructure, enabling cooperative detection of large	Both projects aim to strengthen EPES cybersecurity preparedness and coordinate cyber-incident discovery, sharing and response. They utilize

	scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure	advanced ML-based techniques for the protection of critical infrastructure and they both follow a privacy-by-design approach. PHOENIX further investigates 5G communications, while SDN-microSENSE investigates a wider range of cybersecurity applications through its use cases.
SealedGRID [107]	SealedGRID aims to design, analyze, and implement a scalable, highly trusted and interoperable Smart Grid security platform, providing tools for the protection of Smart Meters, Aggregators and Utilities.	SDN-microSENSE also provides security solution for the smart grid components that are targeted by SealedGRID, and moves one step forward by protecting additional entities, like RES plants and power plants. Moreover SDN-microSENSE develops a more holistic solution for the protection of critical infrastructure.
UNITED-GRID [108]	UNITED-GRID aims to secure and optimise operations of the future electricity grid by developing integrated cyber-physical solutions for smart grids with high penetration of renewables.	Both projects use ML algorithms for the protection of the power grid and develop solutions for microgrid islanding and grid optimization. SDN-microSENSE demonstrates a wider variety of tools for grid protection, leveraging global system visibility for preventing and addressing disruptions in the grid and developing a risk assessment and management framework. Furthermore, it allows for secure and privacy-preserving information sharing among energy operators and actors.
FORESIGHT [109]	FORESIGHT develops a federated cyber-range solution that aims to enhance the preparedness (prevention, detection, reaction and mitigation) of cyber-security professionals in the aviation, power grid and naval industries.	FORESIGHT tests various cyber-security aspects by developing scenarios using simulated environments and devices, while SDN-microSENSE leverages on six real use cases to test and validate its solutions. Moreover, FORESIGHT is more focused on the training of cyber-security professionals in the power grid, while SDN-microSENSE is more focused on developing a holistic cyber-security solution for cyber-security professionals.

In order to enter this market, there is a great need for diversification of the intended product in order to avoid tough competition. From a power grid perspective, there are very few companies offering services related to cyber-security on the smart grid, such as the Thales-developed Hardware Security Modules (HSM). However, from a general perspective of cybersecurity, there are various industry rivals. Those rivals are concentrated and there is a wide variety of solutions available in the market, at a wide range of prices.

Our product differentiation is that, in comparison to other cybersecurity solutions, SDN-microSENSE deploys and implements risk assessment processes, self-healing capabilities, large-scale distributed detection and prevention mechanisms, as well as an overlay privacy protection framework. Furthermore, the use of blockchain technology and anonymous channels for EPES ensures the integrity and the confidentiality of communications

In the near future, the rivalry in the specific field among the companies is expected to become more intense as competitors of different sectors will expand their operations in the field of cybersecurity for the smart grid. The greater the competition, the more prices will fall; consumers will benefit at the expense of businesses, which will see their profits decrease. The intensity of this market is all the stronger since it is growing.

Verdict: Extremely high levels of competitiveness can negatively affect your business and industry. This makes it more difficult for a company to gain customers and increase its profitability. However, in the energy sector, these levels are low to medium due to the competitive market saturation and the consistently evolving industry. The competitiveness level is low to medium during the last years as a limited number of projects were funded from Horizon2020 in this field (i.e. Phoenix, EnergyShield). Moreover, there are currently no products or projects that provide the holistic approach and the bundle of services and tools that is offered by SDN-microSENSE. However, there is a great number of solutions on the wider cyber-security sector that are able to compete on a very high level and are well-established in the market. Thus, **industry rivalry** can be perceived as **medium**.

5. SWOT Analysis

This section presents the SWOT analysis for the SDN-microSENSE solution, describing the main strengths and weaknesses, as well as the emerging opportunities and worrisome threats that the solution might face,which are factors that must be considered when formulating a product strategy.

The result of the SDN-microSENSE SWOT analysis can be found on Tables 45 and 45.

Table 5: SDN-microSENSE SWOT analysis, internal factors

Internal Factors	
Strengths	**Weaknesses**
• Solution that offers a bundle of secure, privacy-enabled and resilient to cyberattacks tools that are not provided by competitors in the market • Human capital expertise in the technical and business domain. Technological know-how by the well-qualified and high-performing staff that are involved in the development of the SDN-microSENSE solution • Improved energy security and protection of the power grid by ensuring continuity of the critical business energy operations • Increased resilience against different levels of cyber and privacy attacks and data breaches (including personal data breaches) in the energy sector. • Advanced threat-detection and active prevention of attacks using state-of-the-art technologies • Cybersecurity solution with easy and robust deployment and deep integration capabilities • The cost items can be clearly identified and flexibly shared between the stakeholders, depending on the specifically issued ecosystem and business model. • The deployment of a use-case can be progressively carried-out in the possible scenarios and in a geo-localized perimeter for each of them (i.e. limited and well-estimated cost). • Solution that efficiently and flexibly uses network and computing resources.	• Technical complexities in the implementation of the solution might result in commercialization delays, leading to a late entry in a competitive market environment • High initial investment cost for the commercialization of the solution, with high estimated costs for the personnel payroll and marketing activities • Services offered by SDN-microSENSE are currently aimed at a specific market segment (power grid market) with its specific needs and characteristics

Table 6: SDN-microSENSE SWOT analysis, external factors

External factors	
Opportunities	**Threats**
• Prioritization of Electricity supply security and resilience in the EU favors the increase in the	• Stakeholders distrust towards novel solutions, due to the existence of traditional processes

market pull demand for solutions like SDN-microSENSE. • Positive trend of the EU and the member states towards the protection and security of critical infrastructure, is expected to lead to increased demand for the provision of information security and cybersecurity services. • Cybersecurity market in the power grid is still at a premature phase; thus it is relatively easy to penetrate this market as the level of the competition is not so high • Market expansion opportunities for the SDN-microSENSE solution, with the potential of a global expansion of the product • Industrial, academic, governmental, standardization and social stakeholders worldwide are strongly committed to develop and foster the adoption of novel technologies for improved efficiency, sustainability and security of power systems.	• Lingering policy harmonization of the member-states with EU cybersecurity strategy • Infrastructure upgrading costs • Rapid changes in the technological environment can shorten product life cycles, thus making the time-to-market critical for the success of the product • Electric power industry is critical infrastructure; hence it will be difficult to convince policy-makers to consider the adoption of major changes like SDN-microSENSE solution. • The level of bureaucracy required to obtain the permissions to launch SDN-microSENSE in a public sector organization is high.

As the SDN-microSENSE solution is mainly addressed towards the protection of public infrastructure, it is conditioned by legislations that are expected to be positively regulated for the introduction of our product in the market, but could also lead to potential delays or restrictions of deployment, thus affecting the profitability of our solution. Therefore, regulatory decisions can be seen as both an opportunity and a threat. Furthermore, the increased interest on the part of potential customers in cybersecurity services and products is identified as an opportunity, given the increasing use of IoT devices and the ongoing adoption of smart grid technologies in Europe and worldwide

One of the most important strengths is considered the introduction of a unified cybersecurity solution that provides security management, cyberthreats identification and protection, by utilizing a bundle of state-of-the-art tools, which are not offered by competitors in the market. Furthermore, another significant strength of SDN-microSENSE is the technical knowledge and expertise in the fields of cybersecurity and power grids that the consortium members possess. However, an identified weakness relates to unforeseen technical complexities that could delay the deployment and commercialization of the product, leading to late market entry and possibly resulting to value-adding product modifications in order to gain a unique and strong competitive advantage.

6. SDN Fuzzy Analytical Hierarchy Process

This section presents the SDN-microSENSE Fuzzy Analytical Hierarchy Process. The purpose of this activity is to identify the factors that would affect the adoption of SDN-microSENSE outcomes. In order to achieve this goal, a survey using the Fuzzy Analytic Hierarchy Process (AHP) method has been conducted. The survey reveals experts' vision regarding critical factors and their significance anticipated to influence the introduction and acceptance of SDN-microSENSE as a technology solution.

6.1 Set of criteria and sub-criteria

Initially, the most important factors that are related to the adoption of SDN-microSENSE were identified after discussions with partners taking into account a wide range of factors. The final list that was compiled contains the following set of criteria:

- **Performance**: aspects such as availability, usability and scalability
- **Technology / Features:** aspects such as islanding, reconfiguration, energy balance management, trading system
- **Security:** aspects related to compliance, privacy and accountability
- **Business aspects:** aspects related to cost, licensing, transition and continuity

For each of these criteria several sub-criteria were also defined, these are attributes that are closely related to each criterion. In more details:

For the performance criterion, four sub-criteria were identified:

- **Resilience and reliability**: the system will have high reliability and resilience
- **Usability:** the system will provide a comfortable experience to users
- **Availability:** the overall functionality supported by the SDN-microSENSE should always be available
- **Scalability:** the system should be able to expand its capabilities

Regarding the technology/features criterion, the following four sub-criteria were selected:

- **Islanding:** SDN-microSENSE will use islanding schemes as a countermeasure against cyber-attacks or improper grid operation
- **Network reconfiguration:** the SDN controller will be able to conduct network reconfiguration
- **Energy balance management:** the system will be able to conduct constant energy balancing actions to mitigate possible issues in case of attack or failures in the grid
- **Blockchain-based trading system:** SDN-microsSENSE will provide a safe peer-to-peer energy trading system among grid stakeholders

For the security criterion, four sub-criteria were selected:

- **Compliance with regulation:** SDN-microSENSE will be compliant with the latest regulations regarding security and data protection, like GDPR
- **Privacy protections (prosumers, consumers):** the system will protect prosumers and consumers against data breaches and will preserve their privacy

- **Privacy protections (energy providers):** the system will protect datasets containing personal identifiable information when exposing these to third parties
- **Accountability: a**ll cyber-attack access attempts and actions should be properly recorded

Finally, for the business criterion the following four sub-criteria were identified:

- **Cost / Sustainability:** the cost of adopting the SDN-microSENSE must be sustainable
- **Licensing:** the system will have an intellectual property modular design that will allow organizations to deploy the components that suit the licensing terms
- **Transition:** a smooth transition from the current state must be made when adopting the SDN-microSENSE solution
- **Continuity:** business continuity must be satisfied

A full list with all criteria and sub-criteria is illustrated in Figure 9.

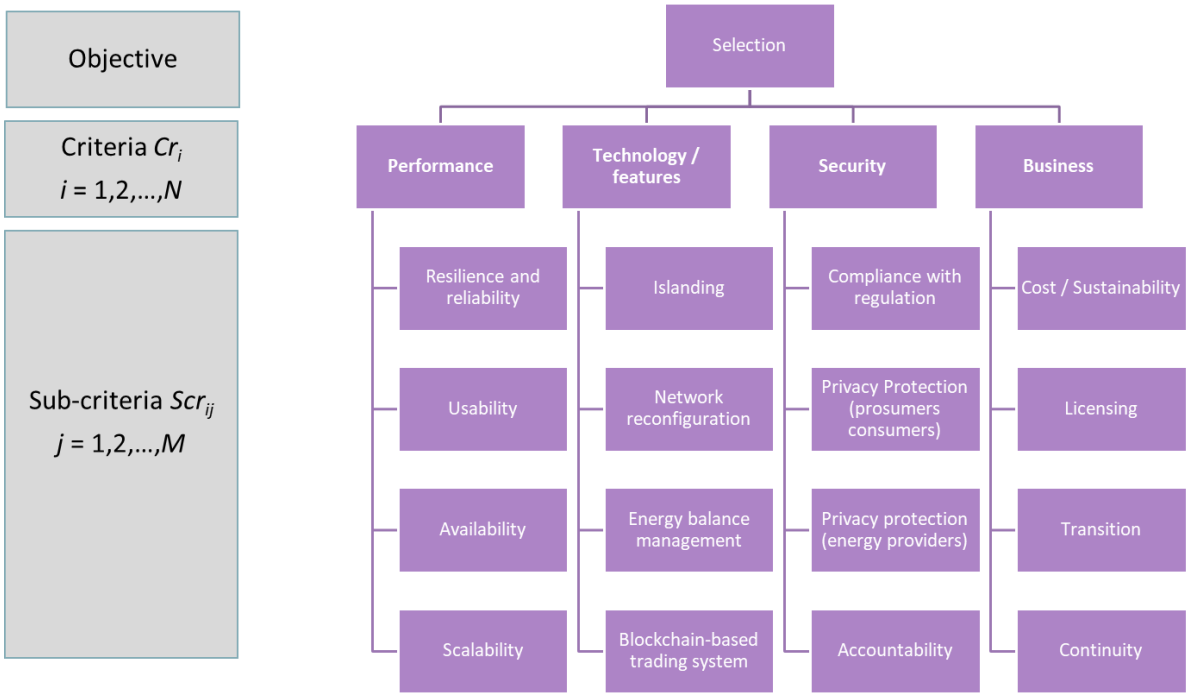


Figure 9: Multi-level hierarchy set of criteria and sub-criteria for SDN-microSENSE

6.2 Description of the Survey

In order to perform the required pairwise comparisons a web-based survey was created. All elements required by the fuzzy AHP were taken into account in order to implement the survey and as a result experts were asked to provide their input regarding the (sub)criterion of their preference and the upper and lower limits of the importance. The web-platform was implemented using LimeSurvey (https://www.limesurvey.org/), an open-source tool for web surveys that was deployed in the projects website.

Limesurvey does not have available modules for implementing a fuzzy logic AHP and performing the needed calculations, so the responses to the survey were extracted and imported to a tool

implemented in Matlab to estimate the weights that signify the importance of criteria and sub-criteria according to the methodology described in section 2.4.

An introductory page provided a short description of the project (Figure 10) along with details about the methodology that was used (Figure 11 and Figure 12). The same page also contained information about the funding of the project, links to the social media of the project and the data policy (Figure 13). The responses were strictly anonymous; no personal data was collected during the survey.

Figure 10: First page of survey with short description of SDN-microSENSE

Methodology

Please answer the questions using the following instructions:

Each criterion will be rated according to its degree of relative importance to the other criteria within the group using pair wise comparisons to rank them. The method is able to test the consistency of the replies. Please indicate your preference between two criteria by providing a range of values between 1 and 9 [lower bound, upper bound].

As shown in the table below when two criteria are of equal importance, they should take a score of 1. When one criterion is more important than another criterion, then it should take a score between 2 and 9, depending on how much more important it is compared to the other ctiterion, with 9 indicating that is much more important.

The scale used to find pair wise relative importance between the different criteria is a nine point scale as follows:

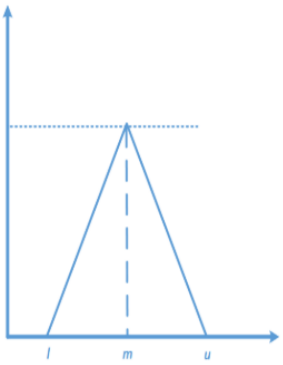
Importance	Definition	Explanation
1	Equal importance	The two criteria are of equal importance
3	Moderate importance	Experience and judgment favors one criterion
5	Strong importance	One criterion is strongly favored
7	Very strong importance	One criterion is dominant over the other
9	Extreme importance	One criterion is favored by at least an order of magnitude over the other
2,4,6,8	Intermediate values	Used as a compromise between two of the above numbers

To deal with the vagueness of human thought, the fuzzy set theory was introduced. A major contribution of the fuzzy set theory is its ability to represent vague data.

A fuzzy set is a class of objects with a membership function ranging between zero and one. It was specifically designed to mathematically represent uncertainty and vagueness. Fuzzy set theory implements groupings of data with boundaries that are not strictly defined, hence the name "fuzzy".

Figure 11: Description of the methodology

In this survey, triangular fuzzy numbers (TFN) are used in order to provide answers. This is the special class of fuzzy number whose membership is defined by three real numbers, expressed as (**l**, **m**, **u**) where **l** and **u** are the lower and the upper limits respectively and m is their mid point. This is illustrated in the next figure:



l and **u** define the limits of the answers: if you are uncertain about your choice the range must be higher. The smaller the range between u and l the biggest the certainty regarding your answer.

Examples:

If you are comparing criterion C1 with criterion C2 and you select C1 then:
- An answer of 8.7 - 9 shows that C1 has extreme importance over C2 and you have high confidence in this choice
- An answer of 4.3 - 8.9 shows that C1 has a stronger importance than C2 but you are not so certain about your choice
- An answer of 1 - 1.2 shows that C1 is almost equal to C2 with high confidence

Figure 12: Description of the methodology (b)

Figure 13: Data policy and acknowledgment

The next figure shows a screenshot of a question that was asked of the participants to answer and the sliders used to input the upper and lower limits of their selection.

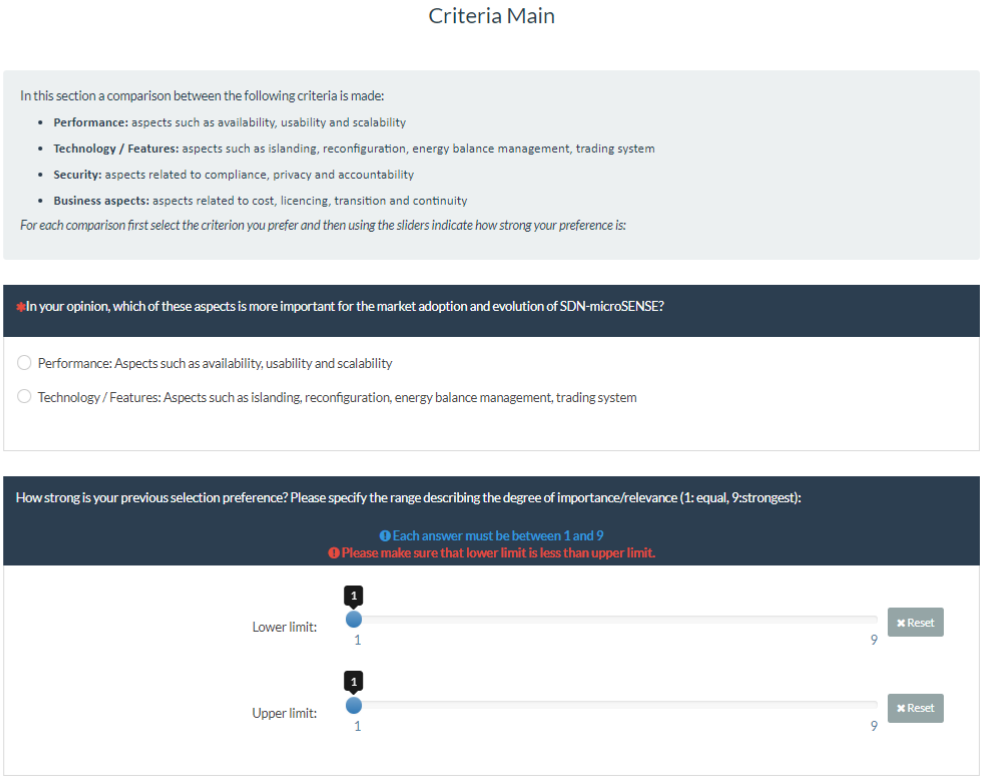


Figure 14: Structure of questions

6.3 Results

The link of the survey was distributed to partners within the SDN-microSENSE project. The questionnaires were conducted and completed during a period of two weeks (June 2020). From the thirty-three experts who participated in the survey, ten questionnaires were discarded as inconsistent, since their associated Consistency Ratio (CR) was >0.1.

Regarding the profile of the experts, all types of organizations that participate in the project are represented. Forty percent of the experts are researchers working in academia and research centers, 35% in SMEs, while 15% work on operators and 10% in industry. The results are presented in Figure 15.

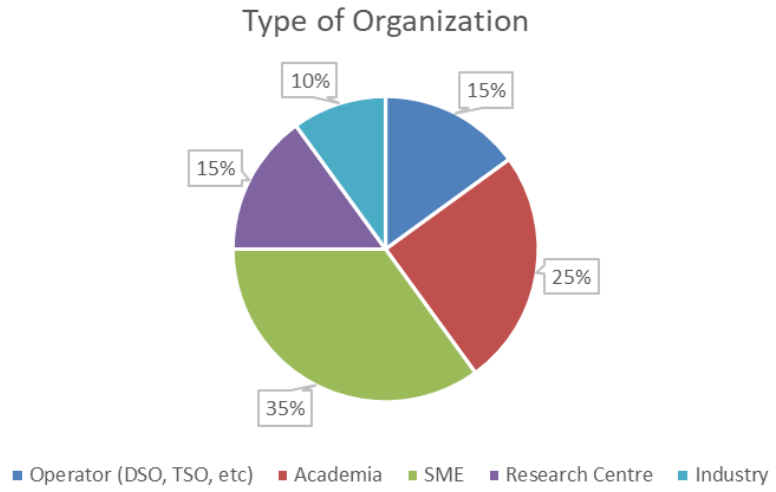


Figure 15: Type of organization

6.3.1 Weights of Criteria

The weights of criteria are shown in Table 7 and illustrated in Figure 16. According to experts' preferences the most important criterion is the Technology / Features with a weight equal to 0.33 (33%), followed by Security with a weight of 0.29 (29%). Performance ranks third with a weight equal to 0.20 (20%) while the criterion with the lowest weight is Business with 0.18 (18%).

Table 7: Fuzzy and Crisp Weights of criteria

Sub-criteria (SC_{ij})	Crisp Weight	Fuzzy Weight (lower; mean; upper;)
C_1: Performance	0.20	(0.20;0.29;0.42;)
C_2: Technology / Features	0.33	(0.20;0.30;0.45;)
C_3: Security	0.29	(0.21;0.31;0.45;)
C_4: Business	0.18	(0.07;0.10;0.15;)

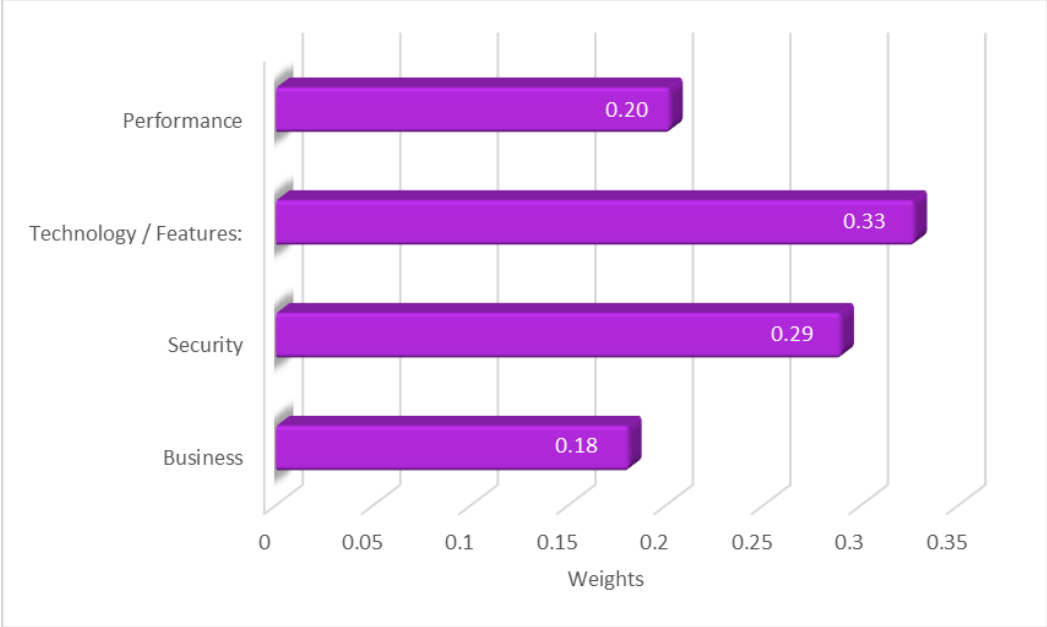


Figure 16: Relative weights of criteria

Technology and features of the developed solution is the most important factor among experts, who value the different features that the final product will have as the most critical ones. Security that is one of the main aspects of the SDN-microSENSE solution is ranked second, these features are important but not as the technology. Combined, these two criteria have a weight of 0.62, something that highlights the fact that these two factors are clearly the most important ones.

Performance follows at the third place followed by business in the last place. It seems that at this stage of the project with most of the components still in an early development phase, experts are more focused on criteria associated with the development. Business factor is more related to a product that is already close to commercialization.

A different interpretation of the results is that the decision making does not always imply a discrete choice between the alternatives, but could also refer to probabilities, possibilities or considerations concerning opportunities vs. risks. The usage of fuzzy numbers could then be taken to guarantee the minimum and maximum values. An α-cut can also be taken into account in order to define narrower lower and upper limits of the relevant weightings based on risk considerations.

In order to better understand that effect, the fuzzy weights are illustrated in Figure 17. Technology is the most important factor among the criteria, although it has high uncertainty, while there is a significant overlap with Security that also has high uncertainty. The other two criteria present lower uncertainties but are clearly the ones ranked at the last places.

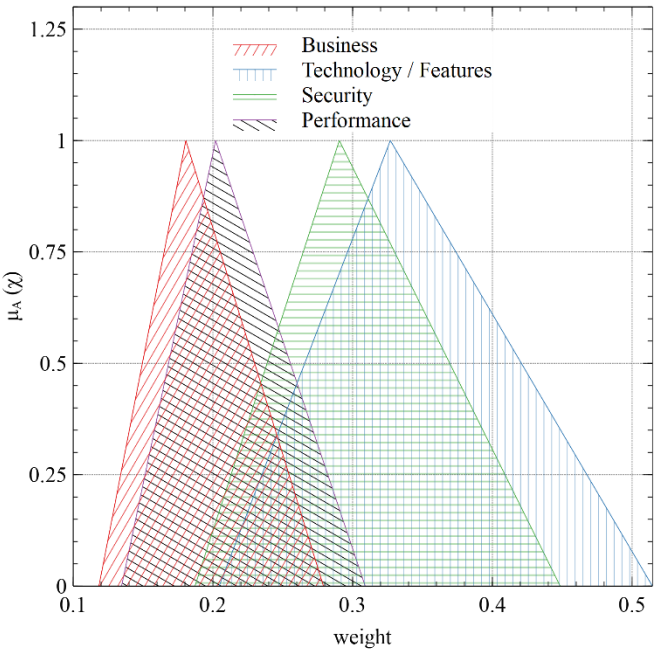


Figure 17: Fuzzy evaluation of criteria

6.3.2 Weights of sub-criteria

At the next step we examined the ranking among the different sub-criteria under each of the criteria. Regarding the Performance criterion we see in Table 8 the crisp weights that are also illustrated in Figure 19. Resilience and reliability has the highest weight of 0.40 (40%), followed by availability with a weight of 0.34. The other two sub-criteria have significant lowest weights: the usability 0.14, while scalability has 0.12

Table 8: Fuzzy and Crisp Weights of Performance Sub-criteria

Sub-criteria (SC_{ij})	Crisp Weight	Fuzzy Weight (lower; mean; upper;)
SC_{11}: Resilience and reliability	0.40	(0.28;0.40;0.57;)
SC_{12}: Usability	0.14	(0.10;0.14;0.20;)
SC_{13}: Availability	0.34	(0.24;0.34;0.48;)
SC_{14}: Scalability	0.12	(0.08;0.12;0.17;)

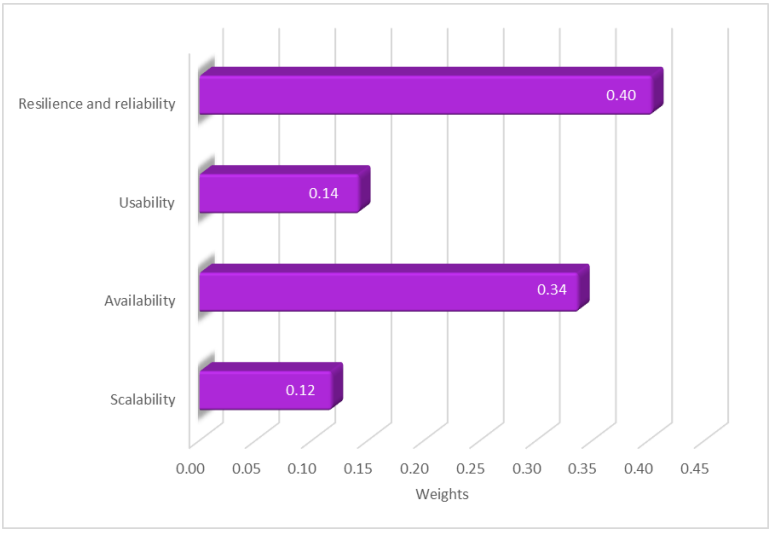


Figure 18: Relative weights of Performance criterion

Seeing the fuzzy weights that are illustrated in Figure 19, one can observe that resilience ranks first although it has a partial overlap with availability. It is interesting that experts have a clear preference on these two as there is no overlap with the other two sub-criteria. Experts highly valuate systems that have high resilience and availability and they prefer these two characteristics over usability and scalability. These two options come as additional features that are good to be present but the most important to have is a stable and available system.

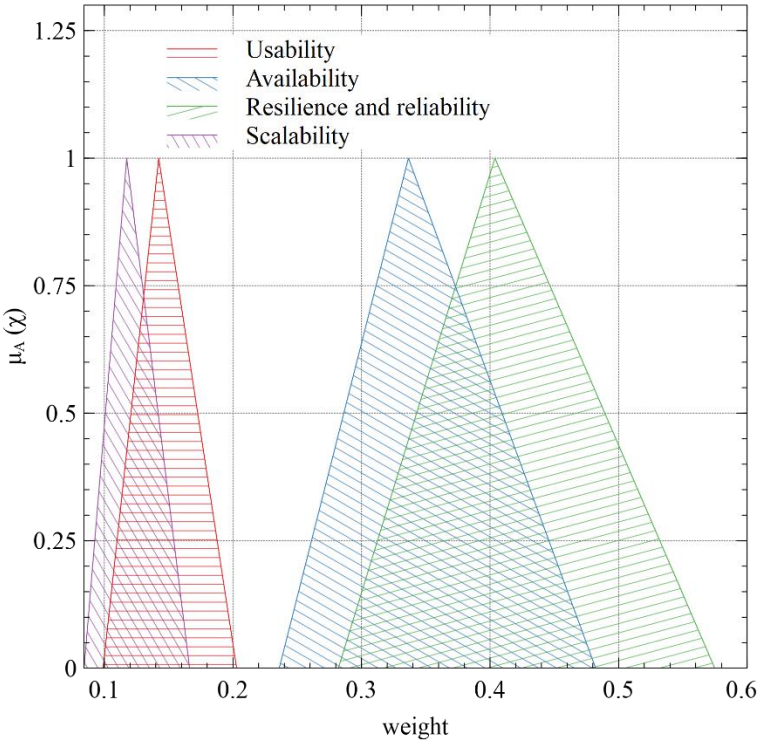


Figure 19: Fuzzy evaluation of performance criterion

For the technology criterion the ranking of the sub-criteria is presented in Table 9 and illustrated in Figure 20. Three out of the four sub-criteria present similar weights. Energy balance system ranks first with 0.31, followed by Network reconfiguration with 0.30 and Islanding with 0.29. The blockchain trading system has the lowest weight of 0.10.

Table 9: Fuzzy and Crisp Weights of Technology Sub-criteria

Sub-criteria (SC_{ij})	Crisp Weight	Fuzzy Weight (lower; mean; upper;)
SC_{21}: Islanding	0.29	(0.20;0.29;0.42;)
SC_{22}: Network reconfiguration	0.30	(0.20;0.30;0.45;)
SC_{23}: Energy balance management	0.31	(0.21;0.31;0.45;)
SC_{24}: Blockchain based trading system	0.10	(0.07;0.10;0.15;)

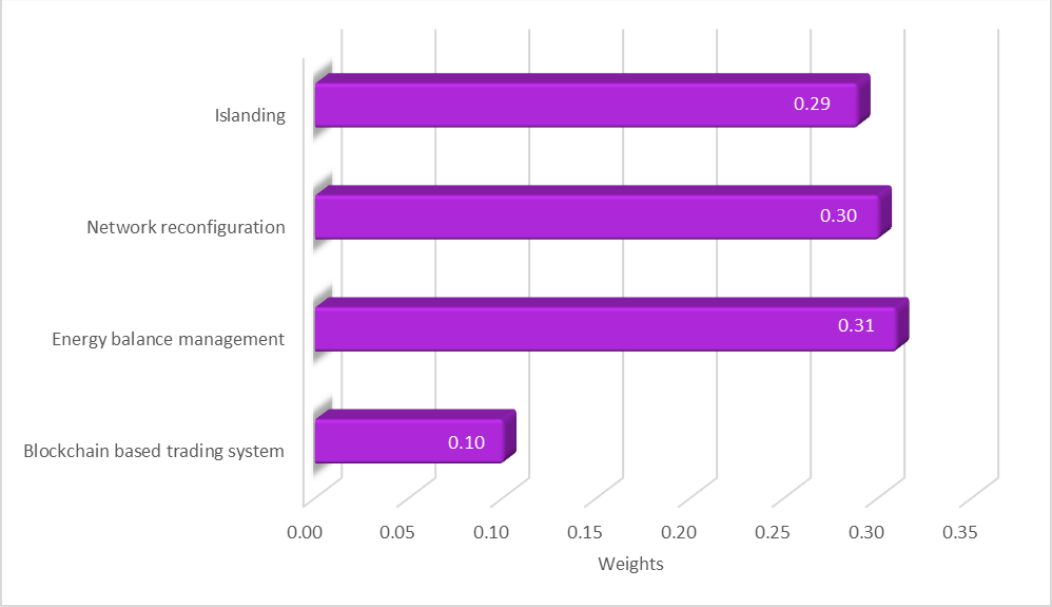


Figure 20: Relative weights of Technology criterion

Examining the fuzzy weights that are depicted in Figure 21 we see that the three sub-criteria present high overlap and similar uncertainties. It seems that all three characteristics are required and have similar importance according to experts. The trading system based on blockchain is clearly a characteristic of lower importance as experts have high certainty that this is the least preferable from the features regarding technology.

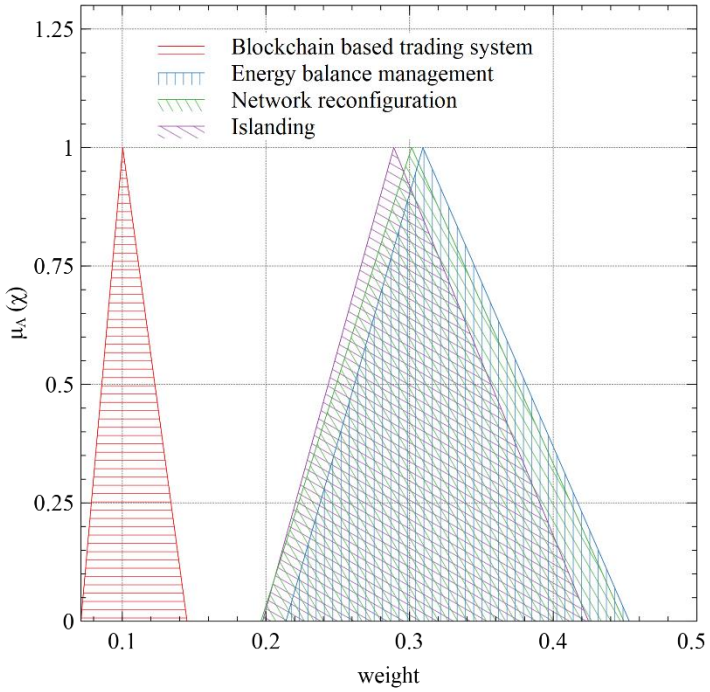


Figure 21: Fuzzy evaluation of technology criterion

Proceeding to the security criterion we see the weights in Table 10: Fuzzy and Crisp Weights of Security Sub-criteria and in Figure 22. Compliance with regulation has the highest weight of 0.33 while the other three options present similar weights. Privacy protection for consumers ranks second with a weight of 0.25, followed by privacy protection for energy providers with a weight of 0.22. Finally, accountability ranks last with a weight equal to 0.20.

Table 10: Fuzzy and Crisp Weights of Security Sub-criteria

Sub-criteria (SC_{ij})	Crisp Weight	Fuzzy Weight (lower; mean; upper;)
SC_{31}: Compliance with regulation	0.33	(0.23;0.33;0.47;)
SC_{32}: Privacy protections (prosumers, consumers)	0.25	(0.17;0.25;0.36;)
SC_{33}: Privacy protections (energy providers)	0.22	(0.16;0.23;0.32;)
SC_{34}: Accountability	0.20	(0.14;0.20;0.29;)

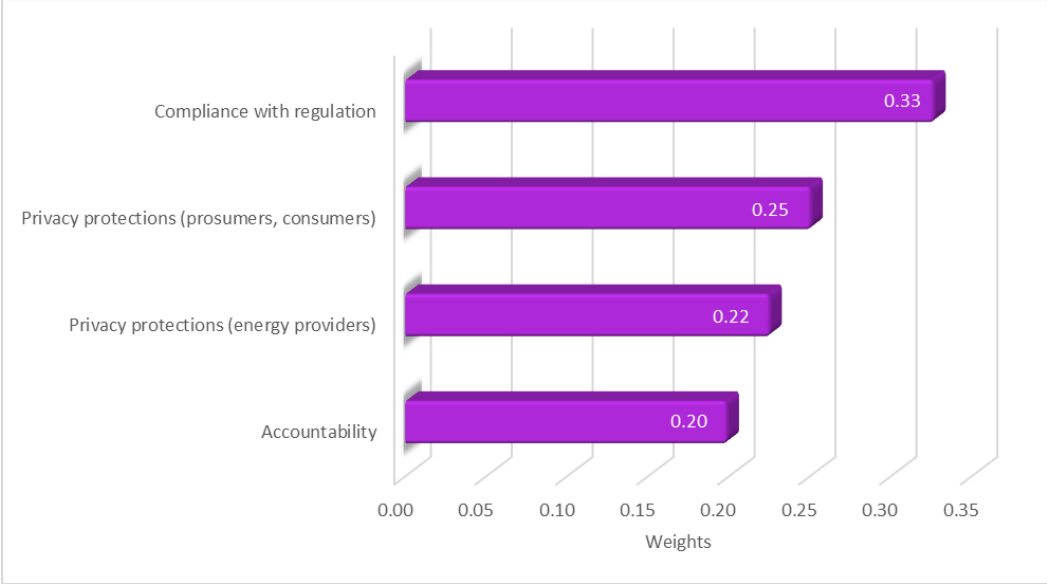


Figure 22: Relative weights of Security criterion

Examining the fuzzy weights that are presented in Figure 23 we see that compliance with regulation ranks first although there are overlaps with all the other options and has the highest uncertainty among all of them. The overlap is significant among the other three sub-criteria. All of these characteristics are valued almost equally by the experts.

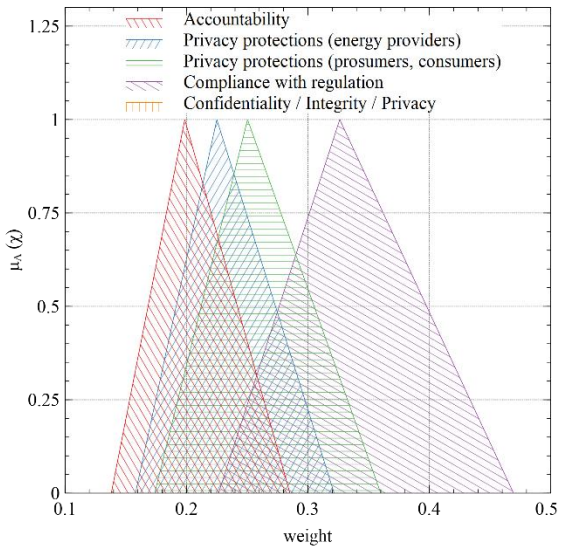


Figure 23: Fuzzy evaluation of security criterion

The weight of the sub-criteria of the business criterion are presented in Table 11 and illustrated in Figure 24. Cost has the highest weight (0.31) followed closely by continuity (0.30). Transition ranks third with a weight of 0.21 while licensing with a weight of 0.17 takes the last place.

Table 11: Fuzzy and Crisp Weights of Business Sub-criteria

Sub-criteria (SC_{ij})	Crisp Weight	Fuzzy Weight (lower; mean; upper;)
SC_{41}: Cost / Sustainability	0.31	(0.22;0.31;0.45;)
SC_{42}: Licensing	0.17	(0.12;0.17;0.24;)
SC_{43}: Transition	0.21	(0.15;0.21;0.31;)
SC_{44}: Continuity	0.30	(0.21;0.30;0.44;)

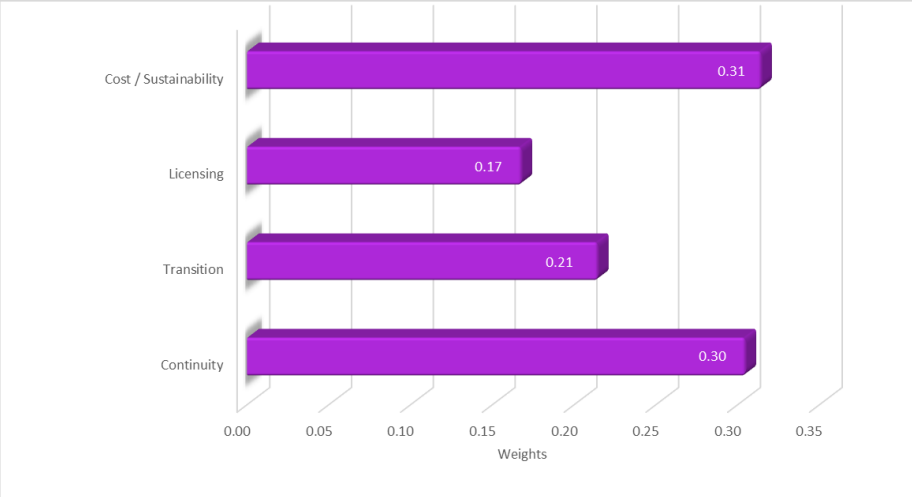


Figure 24: Relative weights of Business criterion

Examining the fuzzy weights (Figure 25) we see that the first two ranked factors have almost complete overlap, these are almost equally important factors according to experts. Transition ranks third although there is partial overlap with the two most high weight options.

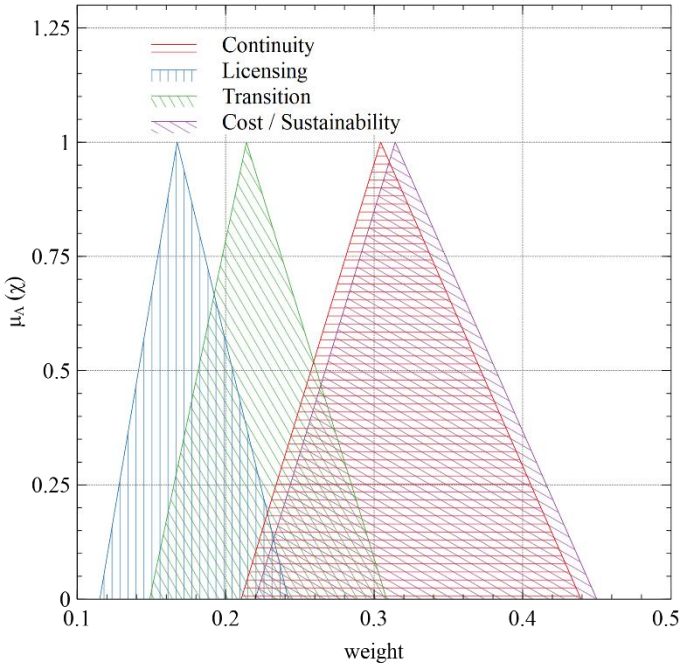


Figure 25: Fuzzy evaluation of business criterion

6.3.3 Global weights of sub-criteria

In order to capture a global view of the sub-criteria ranking, global weights must be calculated. The global weights are obtained by multiplying the sub-criteria weights by their parent's (criteria) weight. The global weights for all the sub-criteria add up once again to 1. Table 12 presents the global weights and the ranking for all the sub-criteria examined in the survey.

Table 12: Global Weights and ranking of Sub-criteria

Sub-criteria (SC_{ij})	Global weight	Global rank
SC_{11}: Resilience and reliability	0.101	1
SC_{12}: Usability	0.036	14
SC_{13}: Availability	0.084	2
SC_{14}: Scalability	0.029	15
SC_{21}: Islanding	0.072	8
SC_{22}: Network reconfiguration	0.075	7
SC_{23}: Energy balance management	0.077	5
SC_{24}: Blockchain based trading system	0.025	16
SC_{31}: Compliance with regulation	0.082	3
SC_{32}: Privacy protections (prosumers, consumers)	0.063	9
SC_{33}: Privacy protections (energy providers)	0.056	10
SC_{34}: Accountability	0.050	12
SC_{41}: Cost / Sustainability	0.078	4
SC_{42}: Licensing	0.042	13
SC_{43}: Transition	0.054	11
SC_{44}: Continuity	0.076	6

Resilience and reliability ranks first (with a weight of 0.101), followed by availability with weight of 0.084. Compliance with regulator (0.082) is in third place, Cost is in forth with weight of 0.078 while Energy balance system with weight of 0.077 concludes the top-5 list.

Regarding the criteria with the lowest weight, these are Accountability, Licensing, Usability, Scalability and Blockchain based trading system

7. Use Cases Business Analysis

This section focuses on the business modelling of the specific use cases offering a use case description, a business plan activity map and a Business Model Canvas (BMC) for the six use cases, aiming to better describe our strategy towards bringing the SDN-microSENSE product to the market.

Before proceeding with the various use case business models, we have identified the main buyers/ customers of the SDN-microSENSE solution (Table 13). Some of the customers are targeted by one or a few use cases, while other customers would be attracted by the demonstration and implementation results of various use cases.

Table 13: SDN-microSENSE Customer Segments

Customer Name	Characteristics
DSO	Distribution System Operators (DSOs) are the entities that securely operate and develop an active distribution system in an area. They are responsible for the network operation, maintenance, and development of the network.
TSO	A Transmission System Operator (TSO) is an organization that is entrusted with transporting energy at a national or regional level. It is responsible for the reliable transmission of power from the generation plants to the DSOs through the High voltage grid.
Electricity Generation company/ Energy Provider	It is an electric power company that generates/produces electricity in an efficient and profitable way. It uses coal, nuclear power, gas or renewable sources for electricity generation
Energy Community	Energy community is an emerging collective concept that aspires to provide active participation of citizens in the shaping of the energy mix and can cover various parts of the value chain (i.e. generation and distribution)
Energy Aggregator	It is a new type of energy service provider that aims to optimize financial or technical aspects of energy generation and consumption. It can increase or decrease electricity consumption and of a group of consumers.
Defence /Military Agency	Government agencies that are responsible for the defence of areas/regions, including the protection of Critical Infrastructure.
Power Plant operator	Power plant operators control, maintain and operate the various systems that generate electricity.
Prosumer	Prosumers are active energy consumers who can both generate and consume energy

It needs to be taken into account that the BMC analysis is done at an ideal generic business model level. Thus, the key actors, customers and roles that have been identified in each use case will be verified during the demonstration phase of the SDN-microSENSE pilots.

7.1 Use Case 1: Investigation of Versatile Cyberattack Scenarios and Methodologies Against EPES

7.1.1 Use Case Description

Investigating attack scenarios in a controlled but highly realistic laboratory environment is highly important since it is not always feasible to deploy real-life cyber-attack scenarios in running EPES infrastructure for safety reasons. As part of the simulation and validation effort, a laboratory environment consisting of a realistic (if scaled-down to the kW range) power system together with a realistic, scaled-down control system architecture are employed to act as a testbed for examining the effectiveness of attack scenarios as well as effectiveness and efficacy of detection and mitigation mechanisms, particularly also performance characteristics critical for mitigation. To this end, the Norwegian National Smart Grid laboratory is well equipped with different components and equipment for research related to smart grids and renewable generation. The laboratory is suitable for studying different grid configurations, hybrid ac/dc networks, microgrids, offshore grids and grid connection issues regarding small hydropower plants and wind generation. It includes a Grid emulator (200 kVA amplifier, DC to 5 kHz), a Real-Time Digital Simulators, hardware-in-the-loop (HIL) testing equipment and Rapid Control Prototyping (RCP) systems (OPAL-RT), Rotating machinery: Induction generators/motors, Synchronous generators/motors, Permanent magnet generators/motors and AC/DC converters: Voltage Source Converters and Multi-Level Converters.

The involved partners of this use case are NTNU and SINTEF. The scenario will provide insights on how the SDN-microSENSE platform confronts a variety of attack methodologies in the EPES infrastructure. This pilot is critical since it will pave the way for the real-world demonstrations to come. Three main methodologies will be followed, namely a) attack vectors via business / Human Machine Interfaces (HMI), b) Substation local networks and c) process control attack vectors. Key impact of the first methodology is the understanding of the type of communication arising during attacks as well as to obtain indicators of compromise from network traffic analysis. The second family of attack scenarios seeks to investigate attacks occurring at the station bus network where traditionally little or no network monitoring takes place. The third methodology differs from others in that: process bus networks should only ever be reachable from station bus networks by way of interaction among remote terminal units (RTU)s, programmable logic controllers (PLCs) and ultimately Intelligent Electronic Devices (IEDs). The use case will conduct tests that otherwise could not be done in an operating grid, while it will also serve for training/ educational purposes. It aims to demonstrate that it is possible to design a realistic laboratory platform for testing of cybersecurity aspects in a controlled environment, taking down both risks and costs.

This use case involves a number of different setup methodologies. First, a laboratory setup will be implemented for simulating an SDN-based network topology hosting a number of (virtual) systems replicating enterprise functionality and traffic as well as connectivity to the SCADA systems. Key impact is a better understanding of the types of attacks possible in modern network architectures and of attack signatures, particularly directed towards control systems.

The second setup involves a laboratory environment based on a selection of industry standard components that will be combined with co-emulated components primarily to represent IED units. The actual interconnection is to be affected by a combination of real and simulated network components, with attack scenarios being mostly monitored for the externally visible effects of attacks as interference with RTU/PLC units in the field is not desirable.

The third setup requires a lab-based environment owing to limits to the fidelity of existing simulation environments where multiple sensors must themselves be co-ordinated to ensure that timeliness and ordering is captured correctly. The principal impact for these scenarios is an enhanced understanding of the feasibility and impact of such attacks, as well as to identify, if any, early indicators of on-going attacks may be detectable in time for mitigation measures to be initiated.

A set of demonstrating attacks will take place against SCADA systems and applications such as the Enterprise Resource Planning systems and the office productivity applications, by launching target spear-phishing attacks via a web browser, email and document transfers, direct attacks against operating systems and applications relying on insecure or outdated configurations, and multi-stage attacks targeting systems across such networks, including eavesdropping on network traffic and Man-in-the-middle (MitM) attacks to secure credentials or interfere with legitimate communication between the enterprise network and the SCADA network, also deploying obfuscation and persistence mechanisms (root kits). Also, a set of attacks will be planned against HMI, data historian and engineering workstations, accompanied by supply chain attacks and indirect attacks, i.e., injection of malicious software updates, interference with the HMI and engineering systems interaction with the SCADA systems (DoS and MitM).

The second round of demonstration encloses attacks on network infrastructure and traffic among the SCADA system and RTU components, since this will normally have stringent requirements for performance such as timeliness and reliability. Hence, attack scenarios based on simple Denial of Service (DoS) may well already be effective in addition to more complex attacks such as MitM or command (and response) injection attacks or de-synchronisation attacks. Attack scenarios will concentrate on standard protocols over Industrial Ethernet (IEEE 802.3) including, in particular, IEC 60870-5-104 [110], IEC 61850 [111] MMS (Manufacturing Message Specification) and GOOSE (Generic Object Oriented Substation Event), also taking into account their relative performance requirement characteristics.

In the third set of attack demonstration, measurements from hard real-time components, such as SDU and aggregators, will be involved alongside with real-time communication protocols including IEC 61850 GOOSE and SV. These protocols are particularly susceptible to attacks on availability such as relatively straightforward and difficult to defend DoS attacks, including low-rate attacks e.g., targeting state machines for connection- or transaction-oriented semantics. Attacks and detection scenarios are also to consider indirect attack vectors such as manipulation of support protocols including e.g., the network time protocol or time synchronisation at higher precision levels including PTP or the manipulation of GNSS reference clocks.

7.1.2 Business Model Canvas

Table 14: Use Case 1 Business Model Canvas

<table>
<tr>
<td rowspan="2">Key Partners
- Consortium Partners
- Universities</td>
<td>Key Activities
- Protection from a variety of attack methodologies in the EPES infrastructure
- Security of supply
- Conduction of on–demand attack simulations that can assist in detecting vulnerability exposures and evaluating the level of protection from cyber-threats
- Research and Education</td>
<td rowspan="2">Value Proposition
- Testing and verifying a cybersecurity power grid domain prior to development and deployment
- Strengthening EPES Resilience against Data breaches by conducting tests in a realistic sand box environment
- Examining the effectiveness of cyber-attack scenarios and the effectiveness of detection and mitigation mechanisms for the protection of EPES systems, at a simulated environment, with reduced costs and risks in comparison to testing on live power systems
- Replicate the communication between the components in a future energy system including cyber-security, compatibility, cyber-physical system activity.</td>
<td>Customer Relationships
- B2C: Transactional relationships with customers for the provision of secure lab testing environment and privacy-enabled services. Possibility of building long-term relationships if some of the customers interact on a recurring basis</td>
<td rowspan="2">Customer Segments
- Energy Utilities
- TSOs and DSOs
- Electrical component manufacturers /solution providers / integrators
- Educational institutions (including partners in projects e.g. supported by EU instruments)</td>
</tr>
<tr>
<td>Key Resources
- Highly integrated laboratory with electrical components and RT-simulations including communication structure
- Cloud Services and state-of-the-art technologies and equipment</td>
<td>Channels
- Testing results to be promoted in NTNU’s and SINTEF’s web site, and social media.
- Research results to be published in open-access repositories such as Zenodo
- Stories and information in technical magazines for the power sector</td>
</tr>
<tr>
<td colspan="2">Cost Structure
- Rental fees and equipment depreciation costs
- Maintenance
- Personnel costs</td>
<td colspan="3">Revenue Streams
Hour based or contract-based fee – including extended R&D activity</td>
</tr>
</table>

Table 14 presents the business model canvas of use case 1.

Key partners involved in the use case are the Consortium partners who develop the technologies and the solution of SDN-microSENSE. Furthermore, universities that will form potential synergies with NTNU and technological partners of SDN-microSENSE in order to exploit the infrastructure and the capabilities of the lab-based environment can be considered as partners.

The **key activities** of use case 1 are related to protection from a variety of attack methodologies in the EPES infrastructure and the demonstration of the offered Security of supply of the SDN-microSENSE solution in a simulated environment. Another key activity is the conduction of on–demand attack simulations that can assist in detecting vulnerability exposures and evaluating the level of protection from cyber-threats. Moreover, this use case contributes to Research and Education purposes of an academic partner of the consortium (NTNU).

In regard to the **Value Proposition** of the use case, a lab test environment is provided to customers who are interested in testing and verifying a cybersecurity power grid domain prior to development and deployment. Tests are conducted for critical infrastructure in a realistic sand box environment , with the aim of strengthening EPES Resilience against data breaches. The effectiveness of cyber-attack scenarios and the effectiveness of detection and mitigation mechanisms for the protection of EPES systems are examined at a simulated environment, with reduced costs and risks in comparison to testing on live power systems. Moreover, the use case replicates the communication between the components in the future energy system including cyber-security, compatibility, cyber-physical system activity.

Customer Relationships are mainly transactional relationships with the customers for the provision of secure lab testing environment and privacy-enabled services and the promotion of the SDN-microSENSE solution and tools. There will be also a possibility of building long-term relationships if some of the customers will interact on a recurring basis (i.e. continuous testing and verification of power grid domains prior to development and deployment).

The main **customer segments** are: Energy Utilities, TSOs and DSOs, electrical component manufacturers /solution providers/integrators, research and educational institutions (including partners in projects e.g. supported by EU instruments)

The **key resources** for the use case are the highly integrated laboratory with electrical components and RT simulations including communication structure. Moreover, our envisioned services rely on cloud Services, realized through the use of state-of-the-art technologies (Hardware-in-the-loop testing)
Concerning the communication **channels**, testing results will be promoted in NTNU's and SINTEF's web site, and social media pages in order to be disseminated to the academia and power grid domains. Furthermore, Research results will be published in open-access repositories such as Zenodo, while story-telling and provision of information in technical magazines for the power sector will also be utilized.

The **key costs** in our business model are the rental fees, the equipment depreciation costs, as well as maintenance costs and personnel costs (salaries).

Our values proposition's main **revenue streams** stem from clients who utilize the equipment for testing and verifying their cybersecurity power grid domain prior to development and deployment. The pricing strategy is based on an hour-based or contract-based fee for service provision – including extended R&D activity.

7.1.3 Activity map

In a succinct overview of the business model activity map, as shown in Figure 26, the relations between core activities and value-adding activities are depicted. The two darker circles represent the foundations of the overall core activities. All of the other activities support or add value to the core activities of the use case. The activity map consists of two main core activities and four value-adding activities. The main core activities are protection from cyber-attacks and security of supply.

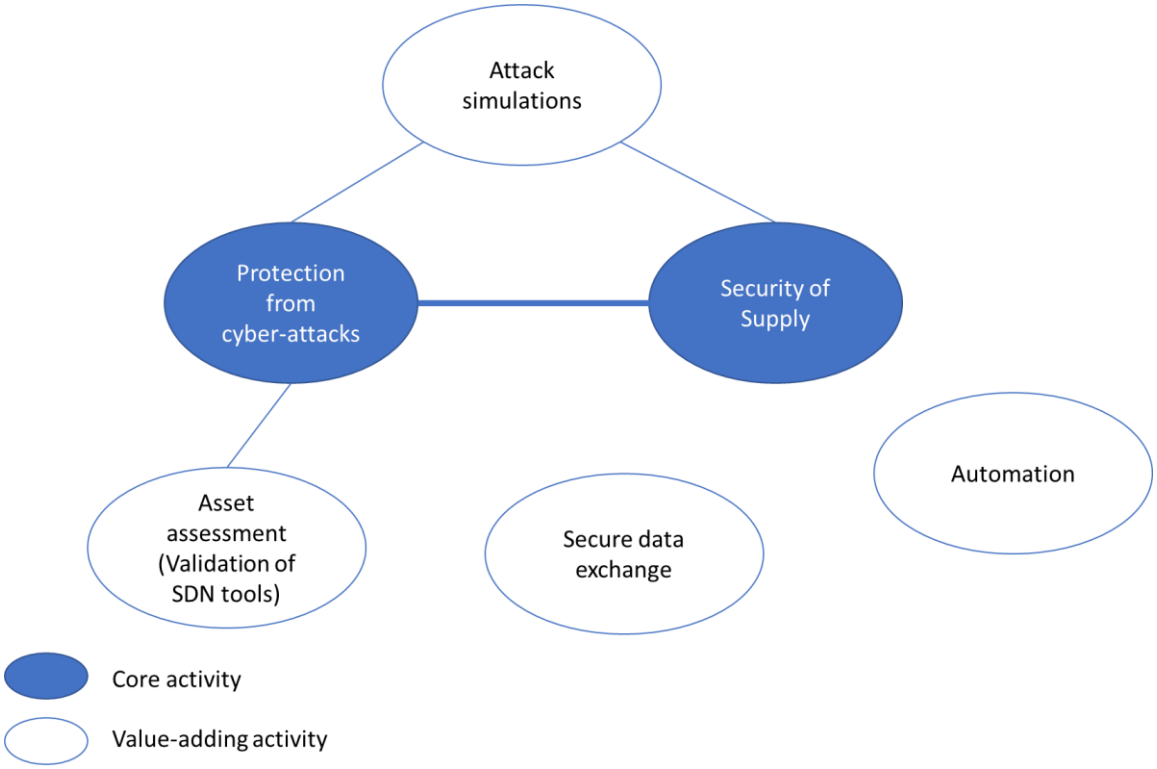


Figure 26: Use Case 1 Activity Map

The value-adding activities of the use case include the asset assessment (such as the validation of SDN tools), secure data exchange and automation capabilities, and the conduction of on-demand attack simulations that can assist in detecting vulnerability exposures and evaluating the level of protection from cyber-threats.

7.2 Use Case 2: Massive False Data Injection Cyberattack Against State Operation and Automatic Generation Control

7.2.1 Use Case Description

Management and automation systems are becoming increasingly important to meet the demands of the energy distribution infrastructure. On transmission and distribution levels, Distribution Management Systems (controlled from both TSOs and DSOs) typically incorporates a few unique power applications, including forecasting, state estimation, fault management, Volt/VAR control, and automatic feeder restoration. Moreover, Energy Management Systems (EMS) focuses on the bulk power system generation and transmission domain. EMS systems have historically utilized real-time communications for control and monitoring, with applications such as Automatic Generation Control (AGC), State Estimation, and Flexible AC Transmission Systems (FACTS). Smart grid initiatives look to expand current EMS solutions through improved algorithms for operational applications. These attributes are especially important due to the criticality of the applications controlling the bulk power system. Additionally, strong authentication should be supported for all grid-related communications, especially remote field devices, such as IEDs and PLCs.

The use case 2 will include a massive false data injection in a whole energy value chain sandboxing environment using a HIL simulation platform. A cybersecurity tool will be developed subject to massive false data injection attacks and tested in a HIL simulation platform. A validation procedure will follow in dry-run scenarios by the Bulgarian grid operators. The secure system should ideally involve a defense-in-depth approach combining infrastructure and application-level security mechanisms. The dry-run scenario will include indicative grid assets substations at the transmission and distribution level, a hydroelectric power plant and an office building acting as energy-efficient prosumer (producer + consumer).

The main actors of this use case are TSO (ESO), DSO (CEZ), Hydroelectric Power Plant (VETS), End-User (DIEL) and a Technology Provider (IEIT). IEIT will coordinate the use-case 2 deployment, i.e. the Hardware-In-the-Loop demonstration and the field testing, ESO will provide the TSO substation and National Dispatching Centre, CEZ will provide the DSO substation, VETS will provide the hydroelectric power plant acting as Distributed Energy Resource (DER), and DIEL will provide the Smart Building acting as prosumer. The SDN-microSENSE tools will be deployed in all the aforementioned five domains.

7.2.2 Business Model Canvas

Table 15: Use Case 2 Business Model Canvas

<table>
<tr>
<td rowspan="3">Key Partners
• Consortium partners
• Hardware and equipment providers</td>
<td>Key Activities
• Provision of enhanced controllability and visibility up to the lower level of the grid, resulting in effective Stability area monitoring and grid balancing of demand and supply
• Risk assessment analysis conducted in all domains of the energy value chain, contributing to security of supply of the power grid
• Secure energy trading and real-time energy data exchange to achieve energy grid management and optimization
• Accurate, efficient and effective anomaly detection and implementation of a defence-in-depth approach for the protection of the system</td>
<td rowspan="3">Value Proposition
• Use case 2 demonstrates how the SDN-microSENSE solution can address a massive false data injection attack in a whole energy value chain sandboxing environment using a HIL simulation platform, as well as with a field application in dry-run scenarios</td>
<td>Customer Relationships
• B2B: Long-term relationships that will be achieved mainly through contacts with industrial energy partners, alongside with participation in targeted exhibitions and venues for the Energy Sector and manufacturers.
• B2C: Long-term Relationships with customers, mainly aggregators and energy communities, will be achieved through branding activities in different channels, aiming to build a trustworthy brand name with a publicly recognized logo</td>
<td rowspan="3">Customer Segments
• DSO
• TSO
• Generation Companies
• Energy communities
• Aggregators</td>
</tr>
<tr>
<td>Key Resources
• SDN-Switch: the intermediate component used for the interconnection and communication of the involved assets.
• XL SIEM Sensors: These sensors are responsible for detecting the aforementioned security threats. These sensors include the Advanced Anomaly Detection (L-ADS) as well as SS-IDPS (Nightwatch).
• S-RAF (OLISTIC Enterprise Risk Management, eVUL): S-RAF (OLISTIC Enterprise Risk Management, eVUL) computes the risk level per asset.</td>
<td>Channels
• Customers will be reached mainly through direct contact, dissemination activities and partners' initiatives
• Services will be provided through web/mobile/cloud service channels
• Through European Union, Government Bodies, Customer Soceties (i.e ENTSOe, EDSO, REScoop)</td>
</tr>
</table>

	• AIDB (Gridpilot): AIDB provides the necessary information for the operation of S-RAF and EDAE. • ARIEC: ARIEC stores and publishes the cybersecurity incident.			
Cost Structure The key cost in this use case concern the development and platform design of the SDN-microSENSE platform, as well as variable costs, such as software and database maintenance, ICT equipment and acquisition of components. Furthermore, personnel costs represent a significant portion of total costs		**Revenue Streams** Clients, mainly Transmission Network Operators, Distribution Network Operators, generation companies and energy communities, will be willing to pay for the service Our revenue sources are the following: i) once-off activation and set-up fee, ii) monthly account maintenance fees, iii) subscription service and iv) volume fees		

Table 15 presents the business model canvas of use case 2.

Key partners involved in the use case are the Consortium partners, and especially the technology providers who develop the technologies and the tools of SDN-microSENSE. Furthermore, hardware and equipment providers (i.e HIL and components) are also considered as key partners.

Regarding the **key activities** of use case 2, SDN-microSENSE will provide enhanced controllability and visibility up to the lower level of the grid, resulting in effective stability area monitoring and grid balancing of demand and supply. Furthermore, a risk assessment analysis will be conducted in all domains of the energy value chain, contributing to security of supply of the power grid. Moreover, Secure energy trading and real-time energy data exchange will be demonstrating, resulting in efficient energy grid management and optimization. Finally, an accurate, efficient and effective anomaly detection will be demonstrated, while a defence-in-depth approach will be implemented for the protection of the power grid at all levels.

The core **value proposition** of the use case 2 is that it demonstrates how the SDN-microSENSE solution can address a massive false data injection attack in a whole energy value chain sandboxing environment using a HIL simulation platform, as well as with a field application in dry-run scenarios

The use case builds **customer relationships** with both Business-to-Business (B2B) and Business-to-Consumer (B2C) customers. More specifically, long-term B2B relationships will be achieved mainly through contacts with industrial energy partners, alongside targeted exhibitions and venues for the Energy Sector and manufacturers. Long-term B2C relationships with customers, mainly aggregators and energy communities, will be achieved through branding activities in different channels, aiming to build a trustworthy brand name with a publicly recognized logo.

The main **customer segments** are: DSO, TSO, Generation Companies, Energy communities and Energy Aggregators.

The **key resources** for the use case stem from SDN-microSENSE developed tools:

- SDN-Switch: the intermediate component used for the interconnection and communication of the involved assets.
- XL SIEM Sensors: These sensors are responsible for detecting the aforementioned security threats. These sensors include the Advanced Anomaly Detection (L-ADS) as well as SS-IDPS (Nightwatch).
- S-RAF (OLISTIC Enterprise Risk Management, eVUL): S-RAF (OLISTIC Enterprise Risk Management, eVUL) computes the risk level per asset.
- AIDB (Gridpilot): AIDB provides the necessary information for the operation of S-RAF and EDAE.
- ARIEC: ARIEC stores and publishes the cybersecurity incident.

Channels are critical element for the success of SDN-microSENSE. Customers will be reached mainly through direct contact, dissemination activities and partners' initiatives. The value proposition of SDN-microSENSE and the use case results will also be promoted through European Union Bodies, Government Bodies, Customer Societies (i.e ENTSOe, EDSO, REScoop). Furthermore, services will be provided through web/mobile/cloud service channels.

The **key costs** in this use case concern the development and platform design of the SDN-microSENSE platform, as well as variable costs, such as software and database maintenance, ICT equipment and

acquisition of components. Furthermore, personnel costs represent a significant portion of the total costs.

Our **revenue streams** will come from our customers, mainly Transmission Network Operators, Distribution Network Operators, generation companies and energy communities, who will be willing to pay for: i) a once-off activation and set-up fee, ii) monthly account maintenance fees, iii) subscription service and iv) volume fees

7.2.3 Activity map

In a succinct overview of the business model activity map, as shown in Figure 27, the relations between core activities and value-adding activities are depicted. The activity map consists of four main core activities and three value-adding activities. The main core activities are energy trading, stability area monitoring, security of supply and grid balancing of demand and supply.

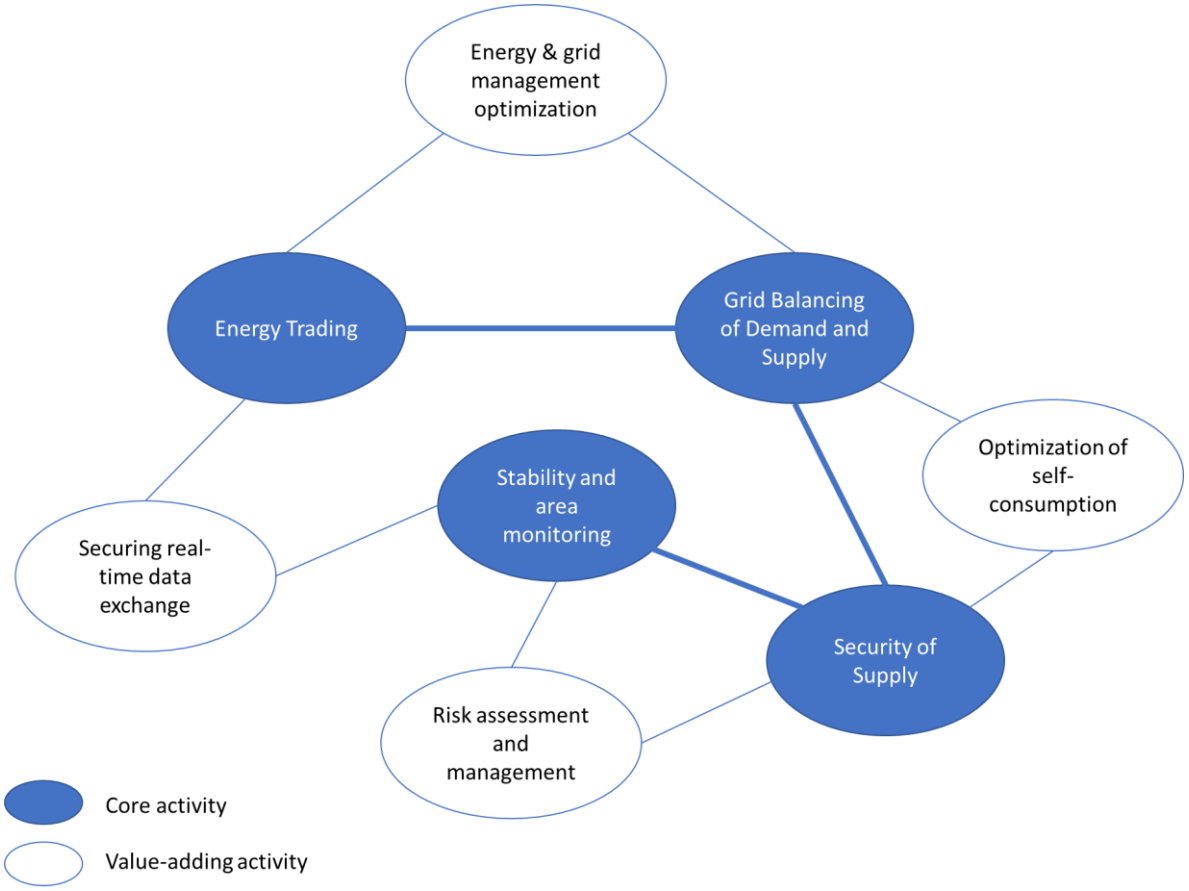


Figure 27: Use Case 2 Activity Map

The value-adding activities of the use case include secure real-time data exchange, optimization of self-consumption, and optimization of energy & grid management. Almost all core and value-adding activities are interrelated, resulting in a holistic solution that intends to protect the grid from cyber-attacks and, at the same time, optimize the grid operation.

7.3 Use Case 3 : Large-scale Islanding Scenario Using Real-life Infrastructure

7.3.1 Use Case Description

The shift from traditional power grids to the smart grid is highlighted by the introduction of DERs in several parts of the grid, which enable the formation of microgrids. Microgrids are parts of the grid that can operate in two modes, connected to the grid or in island mode depending on the local DER. Thus, for the realization of the future of smart grids, real-time calculation of islanding schemes and management of the formed islands are indispensable tools. SDN-microSENSE provides such tools, using them as a last resort in case of a cyberattack, with the intent to isolate parts of the grid to prevent cascading failures and system-wide blackouts. This is a two-fold procedure, as the tools need to be able to alter the topology of the power grid, as well as to manage the local DERs to balance the load and supply in that part of the grid.

This particular use case will demonstrate and validate the islanding mechanisms of SND-microSENSE in large scale, using the newly built Cyclades interconnection. More specifically, the SDN-enabled RTUs will be installed in 150kV substations of IPTO (TSO) that will monitor the pilot infrastructure continuously. After a cyberattack, SDN-SELF will take effect. The islanding schemes in that part of the grid will be calculated by the IIM module, while at the same time, the EMO module will calculate the energy balance instructing the energy sources to provide the necessary power. At the same time, PPC as an energy provider, will operate the Lavrio power plant that acts as the main energy source in the area.

The large scale of the use case and the physical installation of its components will provide a unique testbed to demonstrate the SDN-microSENSE system. At the same time, it will prove the efficiency and usefulness of the SDN-microSENSE platform and particular the SDN-SELF, by providing access to real-time and historical data and real infrastructure. In addition, in the course of the demonstration, significant insights will be obtained regarding the Cyclades interconnection and the future installation of DERs in the Cyclades Islands.

The main actors in the use case are TSO (IPTO) and Energy Provider (PPC). The TSO is the entity that is responsible for the smooth operation of the energy grid and the Energy Provider entity operates the Energy Resources and receives instructions on how much energy he must feed to the system to maintain its balance. In the greater scope, the engaged stakeholders are citizens, businesses and public infrastructures that are dependent on the supply of electricity in the Cyclades Islands as well as the DSO and the Market Operator.

7.3.2 Business Model Canvas

Table 16: Use Case 3 Business Model Canvas

<table>
<tr>
<td rowspan="2">Key Partners
Consortium Partners
Hardware suppliers</td>
<td>Key Activities
Grid Islanding and isolation of problematic grid areas from the main grid
Protection from cyber-threats and incident response
Security of Supply and Grid restoration after unexpected load loss</td>
<td rowspan="2">Value Proposition
Use Case 3 demonstrates how the SDN-microSENSE uses the islanding mechanisms to create a more resilient and secure power system. In the same time, it can be used to enable a more efficient utilization of the DERs.</td>
<td>Customer Relationships
B2B: The Use Case could be used as a marketing asset in this cause to promote the effectiveness of SDN-microSENSE and achieve long-term relationship for TSOs, DSOs and Energy Providers.</td>
<td rowspan="2">Customer Segments
TSOs
DSOs
Energy Providers</td>
</tr>
<tr>
<td>Key Resources
Consortium technical partners to develop the various tools and the various tools themselves.
SDN technology that enables a centralized control of the communication network.
Experienced technicians that will install the various components to the pilot infrastructure</td>
<td>Channels
The existing cooperation with other entities will be used to promote SDN-microSENSE
Participation in exhibitions and venues for the energy sector will be the main channel of dissemination of the project.</td>
</tr>
<tr>
<td colspan="2">Cost Structure
Development of the various software tools
Development and acquisition of the hardware tools (SDN-enabled RTUs, SDN-Switches)
Operational costs</td>
<td colspan="3">Revenue Streams
Clients, mainly the Energy providers connected to the system, the DSO connected to the system and Governmental Institutions, will be willing to pay for the service .
Our revenue sources are the following: i) once-off activation and set-up fee, ii) monthly account maintenance fees, iii) subscription service and iv) volume fees</td>
</tr>
</table>

Table 16 presents the business model canvas of use case 3.

The **key partners** involve the consortium partners that develop the technologies and frameworks of SDN-microSENSE project, and the hardware suppliers (i.e. suppliers of grid components.)

The **key activities** of use case include grid restoration processes that are activated after unexpected load loss and supply balance,and the activation of islanding processes in order to isolate problematic grid areas from the main grid. Last but not least, the SDN-microSENSE solution is used for threat detection, protection from cyber-threats and incident response .

The **core value** of the use case 3 is that it demonstrates how SDN-microSENSE uses the islanding mechanisms to create a more resilient and secure power system. In the same time, the SDN-microSENSE solution will be used to enable a more efficient utilization of the DERs.

The use case builds customer relationships with B2B customers. More specifically, the Use Case can be used as a marketing asset in this cause to promote the effectiveness of SDN-microSENSE and achieve long-term relationships with TSOs, DSOs and Energy Providers.

The main **customer segments** are: TSOs, DSOs and Energy Providers

The **key resources** for the use case stem from SDN-microSENSE development and demonstration phases and are shown below:

- The Consortium technical partners who develop the project's tools
- The various SDN-microSENSE tools
- The SDN technology that enables a centralized control of the communication network
- The experienced technicians that will install the various components to the pilot infrastructure

Customers will be reached mainly through direct contact. The existing cooperation and communication with other entities will be used to promote SDN-microSENSE solution, while the participation in exhibitions and venues for the energy sector will be the main channel of dissemination of the project and the SDN-microSENSE platform.

The **key costs** in this solution concern the development of the SDN-microSENSE tools and platform, the development and acquisition of the hardware tools (SDN-enabled RTUs, SDN-Switches), as well as the operational costs.

Our **revenue streams** will come from our customers, mainly the Energy providers connected to the system, the DSO connected to the system and Governmental Institutions, who will be willing to pay for the service. Our revenue sources are the following: i) once-off activation and set-up fee, ii) monthly account maintenance fees, iii) subscription service and iv) volume fees

7.3.3 Activity map

In a succinct overview of the business model activity map, as shown in Figure 28, the relations between core activities and value-adding activities are depicted. The activity map consists of two main core activities and three value-adding activities. The main core activities are islanding and security of supply.

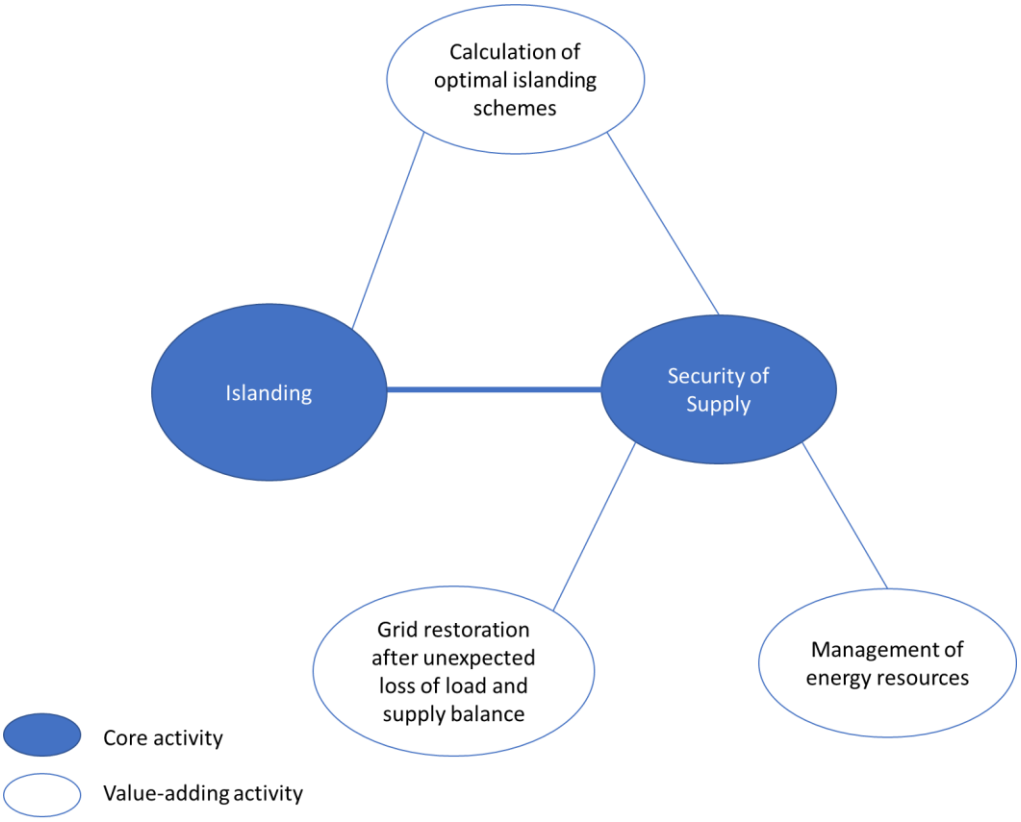


Figure 28: Use Case 3 Activity Map

The value-adding activities of the use case include the calculation of optimal islanding schemes, the management of energy resources, and the grid restoration after an unexpected loss of load and supply balance.

7.4 Use Case 4: EPES Cyber-defence against Coordinated Attacks

7.4.1 Use Case Description

Coordinated cyber-attacks against EPES systems can have an extensive impact on the operation of the power grid and pose a serious threat of disruption to a country's critical infrastructure. SDN-microSENSE develops tools and solutions that address coordinated cyber-attacks from multiple external sources. More specifically, the scenarios of Use case 4 are focused on the evaluation and assessment of the SDN-microSENSE platform against sophisticated, targeted attacks coming from coordinated cyber-attacks that use a variety of attacking tools and methods.

In this use case, a complete EPES infrastructure is deployed, from the power plant to substations and microgrids, including an Operator Control Centre. The systems located at the Operator Control Centre and in the substations are the most critical and attack-attractive assets, due to their monetary value and mainly due to their capital role in the energy value chain, as,by controlling them, the attackers could disrupt the energy services in wide populated areas. Their protection from cyber-attacks is a primary and critical concern for utilities and equipment providers. In particular, this use case will validate how SDN-microSENSE defence systems support the resilience against cyber-attacks of main EPES elements.

This scenario will take place in Spain, involving two substations of the DSO, a PV power plant, a Smart Grid Cybersecurity Lab, which will emulate the control centre and where the cyberattacks will be developed, and a microgrid in a laboratory environment.

The PV Power Plant will cover the generation part of the grid, while a primary substation (boundary substation with TSO) and a secondary substation will be involved, to cover the distribution part of the energy chain, where also the SDN-enabled RTU prototype will be integrated.

The use case will also include a microgrid through an Energy Smart Lab. This laboratory has advanced functionalities, such as microgrid analysis, islanding, network reconfiguration, or cyber-attacks creation and testing. Additionally, the laboratory offers the Power-Hardware in the Loop capability, which is expected to be used for integration with the primary or secondary substations to respond to different grid conditions. To complete this architecture, the Smart Grid Cybersecurity Lab, will simulate a real communication environment between a primary substation and a control room of a DSO. The laboratory contains different devices (IEDs, HMI and protection relays) connected through an EPES infrastructure and a control room that will integrate communication between the elements of the pilot. The Cybersecurity Lab will allow reproducing a set of anomalies and cyber-attacks at different levels of the Smart Grid (e.g. through penetration testing tools - ethical hacking) and validating the effectivity of SDN-microSENSE cyber-security solutions. These different laboratories of the use case will allow to carry out the testing and validation activities in a controlled environment. The validation and demonstration scenarios will include cyber-attacks targeting at the power generation equipment, primary substation, secondary substations and microgrid.

In this use case, the SDN-microSENSE S-RAF framework will be applied in the EPES infrastructure in domains. S-RAF will be used to produce the risk assessment and management results, which will be used for configuring the deployment of the XL-EPDS framework. Furthermore, a honeynet will capture the network traffic and the information of the attack and notify it to other components of the SDN framework. Then, a coordinated attack is planned in all the EPES domains at the same time for validating the SDN-microSENSE platform by giving emphasis to the XL-EPDS framework. In particular, the following attacks will take place:

A first scenario will consist of a MiTM attack to take control of the substation and cause a blackout opening the breakers, while sending fake information to the control centre to hide the attack to the operators, while DoS and DDoS will be sent to the RTUs. Other scenarios will explore the desynchronization of the RTUs, false data injection attack from the RTU to the SCADA to alter electric values which would lead to wrong operational decisions, and again MiTM attack and false data injection to the PV power plant and encryption of the historical data.

Various components will be demonstrated in this use case:

- The XL-SIEM component will monitor the logs of the diverse equipment and capture the traffic traces coming from the systems
- SS-IPPS will perform advanced correlations of the system status parameters and the network traffic traces by applying known attack patterns and signatures
- L-ADS will apply big data analytics in order to do the root-cause analysis of detected anomalies
- DiscØvery will produce analytics for projecting them to HMIs
- the HMI dashboard will be updated when there is an attack, while an alarm will be also triggered
- the AMI honeypots will also be active by recording attack actions and emulating different devices.
- The IIM and EDAE will provide, respectively, the islanding schemes and the network reconfiguration to recover after the attack.
- Finally, the incident database for information sharing with other stakeholders will be updated through the CIS interface of the XL-EPDS

The involved project actors on this use case are Global Manufacturers (SCHNEIDER), Engineering Groups (AYESA), technology Providers (TECNALIA, ATOS, IREC) and DSOs (EPESA). This use case is of great interest to the most important electricity industry actors, such as technology developers and manufacturers, as well as electric utilities. The engaged stakeholders are electrical utility companies, distribution system operators, RES producers, manufacturing firms, technology providers, and in a broader perspective, investors, policymakers, regulators, energy agencies and governments. Some of these groups play an essential role in the implementation of the use case, while others may simply have valuable information, interest, or contacts that help the SDN-microSENSE develop an appropriate solution which is likely to succeed given local conditions.

It should be noted down that, due to some confidentiality issues, the definition of use case 4 has not yet been finalized, and the business analysis of the Use Case is based on all available information from the preparation phase of the project up to the delivery date of the deliverable (M15).

7.4.2 Business Model Canvas

Table 17: Use Case 4 Business Model Canvas

<table>
<tr>
<td rowspan="2">Key Partners
• Consortium Partners
• Hardware Suppliers</td>
<td>Key Activities
• Holistic protection of the power grid from cyber-attacks. Network Security Monitoring, incident detection and response
• Implementation of Risk Assessment Framework that aims to provide security of Supply, including asset assessment and risk management in EPES
• Development and maintenance of a Database of cyber-attack Incidents</td>
<td rowspan="2">Value Proposition
• Use case 4 demonstrates how the SDN-microSENSE solution can address coordinated cyber-attacks from multiple external sources that use a variety of attacking tools and methods.
• Network Security Monitoring (intrusion detection)
• Risk assessment
• Resilient power grid
• Timely detection of cyber-attacks
• Protection from cyber-attacks
• Anonymized Incident Database
• Network reconfiguration to respond to a cyber attack</td>
<td>Customer Relationships
• B2B: These long-term relationships will be achieved mainly through contacts with industrial energy partners, alongside with targeted exhibitions and venues for the Energy Sector. The involved actors of the use case and the consortium partners (global manufacturers, DSOs, RES producers, Technology providers) are directly interested to the solutions, which could potentially result in B2B partnerships
• B2C: Long-term relationships with customers, mainly DSOS, TSOS, governments, energy regulators will be achieved through branding activities in different channels, aiming to build a trustworthy brand name with a publicly recognized logo.
• Focus as well on potential public-private partnerships, since the protection of critical infrastructure is a matter of national concern for the governments</td>
<td rowspan="2">Customer Segments
• DSOs
• TSOs
• Governments
• Energy agencies
• Energy communities
• Energy Regulators
• Defense/Military/ intelligence agencies
• Microgrids in sensitive installations (i.e. Military bases, hospitals)</td>
</tr>
<tr>
<td>Key Resources
• Technologies developed by the consortium technical partners involved in the use case (developers)
• SDN-microSENSE S-RAF Framework,
• SDN-microSENSE Privacy Protection Framework
• SDN-microSENSE XL-EPDS framework
• XL-SIEM
• SS-IPPS
• DiscØvery
• AMI Honeypots
• IIM and EDAE</td>
<td>Channels
• Customers will be reached mainly through direct contact, dissemination activities and partners' initiatives.
• Mult stakeholder Approach towards Cyber-security stakeholders through the</td>
</tr>
</table>

			participation in CIP (Critical Infratsturcture Protection) and Cyber-security workshops • Services will be provided through web/mobile/cloud service channels • Through European Union, Government Bodies	
Cost Structure The key costs in this solution concern the development and platform design of the SDN-microSENSE platform, as well as variable costs, such as software and database maintenance, ICT equipment and acquisition of components. Furthermore, operational and personnel costs represent a significant portion of total costs		**Revenue Streams** Clients, mainly DSOs, TSOs and public bodies, will be willing to pay for the service. Our revenue sources are the following:: i) once-off activation fee, ii) monthly fees for the use of the service, iii) volume fees (i.e. fee based on the level and number of attacks, or/and fees for the detection of the attacks, iv) Continuous Vulnerability Scanning and Risk assessment fees, v) fees for Security Awareness Trainings, vi) Incident Response Triage		

Table 17 presents the business model canvas of use case 4.

The **key partners** involved in the use case are the consortium partners that develop the technologies and frameworks of SDN-microSENSE project, and the hardware suppliers (i.e. suppliers of grid components.).

The **key activities** of the use case include the development of a holistic solution for the protection of the power grid from cyber-attacks, that includes Network Security Monitoring, incident detection and response. Furthermore, another key activity is the development of a Risk Assessment Framework that aims to provide security of Supply, including asset assessment and risk management in EPE. Finally, another key activity is the development and maintenance of a cloud-based repository of cyber-attack Incidents, where information about cyber-attacks will be hosted and exchanged between power grid operators in a secure and anonymized way.

In regard to the **value proposition**, use case 4 demonstrates how the SDN-microSENSE solution can address coordinated cyber-attacks from multiple external sources that use a variety of attacking tools and methods. Moreover, functionalities of the SDN-microSENSE platform, such as Network Security Monitoring (intrusion detection), Risk assessment, Timely detection of cyber-attacks and protection from cyber-attacks are demonstrated.

The use case builds **customer relationships** with B2B and B2C customers. More specifically, long-term B2B relationships will be achieved mainly through contacts with industrial energy partners, alongside with targeted exhibitions and venues for the Energy Sector. The involved actors of the use case and the consortium partners (global manufacturers, DSOs, RES producers, Technology providers) are directly interested to the solutions, which could potentially result in B2B partnerships. Moreover, long-term B2C relationships with DSOS, TSOS, governments and energy regulators will be achieved through branding activities in different channels which will aim to build a trustworthy brand name with a publicly recognized logo. We will focus as well on potential public-private partnerships, since the protection of critical infrastructure is a matter of national concern for the governments.

The main **customer segments** are: DSOs, TSOs, Governments, Energy agencies, Energy communities, Energy Regulators, Defense/Military/intelligence agencies and microgrids in sensitive installations (i.e. Military bases, hospitals)

The main **key resources** for the use case are the technologies developed by the consortium technical partners, which are necessary to set up the novel, scalable, accessible, and desirable solution that will be able to deliver our value proposition. The key resources involve the different SDN-microSENSE tools that are utilized in this use case and are listed below:

- SDN-microSENSE S-RAF Framework;
- SDN-microSENSE Privacy Protection Framework;
- SDN-microSENSE XL-EPDS Framework;
- XL-SIEM;
- SS-IPPS;
- DiscØvery;
- AMI Honeypots
- IIM and EDAE

In regard to the use case's **channels**, our customers will be reached mainly through direct contact, dissemination activities and partners' initiatives. A Multi-stakeholder Approach will be followed towards Cyber-security stakeholders through participation in CIP (Critical Infrastructure Protection) and Cyber-security workshops. Furthermore, dissemination and communication activities will be developed through web/mobile/cloud service channels.

The **key costs** in this solution concern the development and platform design of the SDN-microSENSE platform, as well as variable costs, such as software and database maintenance, ICT equipment and acquisition of components.

Regarding the **revenue streams**, our value proposition will generate revenue through its clients, mainly DSOs, TSOs and public bodies, who will be willing to pay for the provision of the SDN-microSENSE services. Our revenue sources are the following:: i) once-off activation fee, ii) monthly fees for the use of the service, iii) volume fees (i.e. fee based on the level and number of attacks, or/and fees for the detection of the attacks, iv) Continuous Vulnerability Scanning and Risk assessment fees, v) fees for Security Awareness Trainings, vi) Incident Response Triage

7.4.3 Activity map

In a succinct overview of the business model activity map, as shown in Figure 29, the relations between core activities and value-adding activities are depicted. The activity map consists of five main core activities and seven value-adding activities. The main core activities are Protection from cyber-attacks, Risk assessment, Security of Supply, Maintenance of a Database of incidents and Network Security Monitoring. Most of the core activities are interconnected with each other, as show in the figure (linking between the core activities' circles).

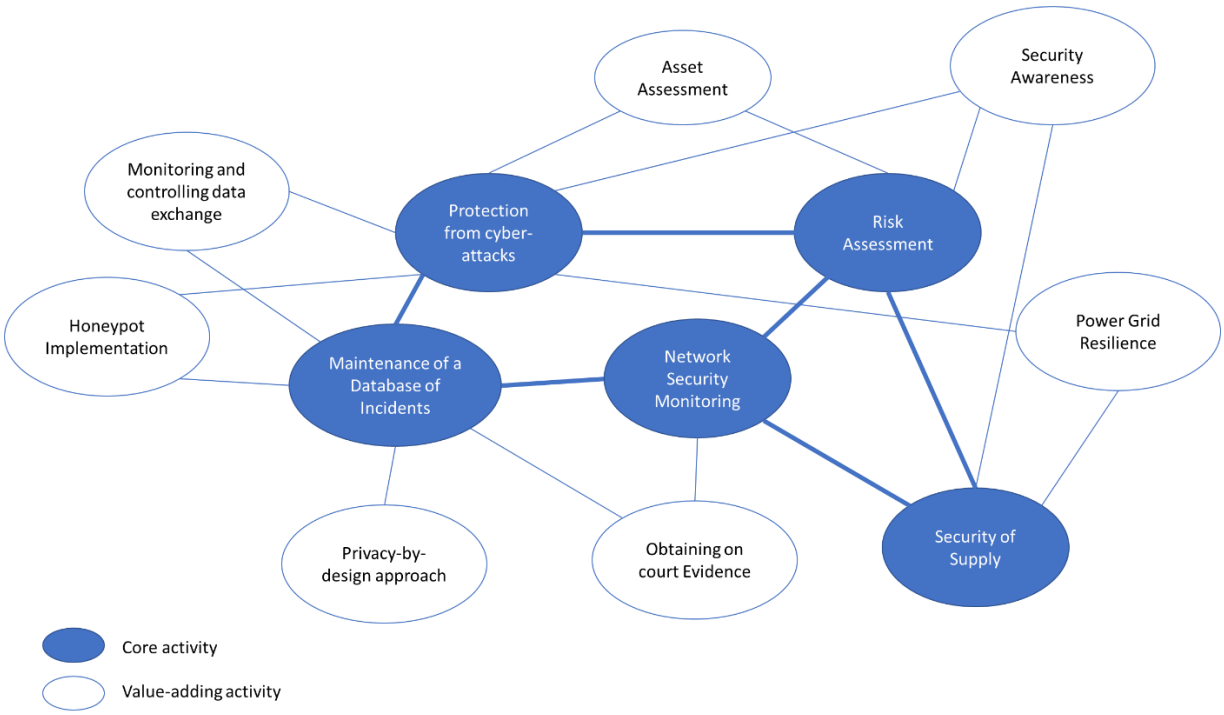


Figure 29: Use Case 4 Activity Map

The value-adding activities of the use case include monitoring and controlling data exchange, privacy-by-design approach, Asset Assessment, Power grid resilience, Security awareness, Honeypot implementation and obtaining on-court evidence.

7.5 Use Case 5: Distribution Grid Restoration in Real-world PM Microgrids

7.5.1 Use Case Description

In the light of the emerging climate change and the strategic initiatives of the European Union towards a carbon-neutral society, DERs are occupying an increasing share in the energy market, whilst their deployment is actively fostered by national and European institutions. Although, the wide adoption of renewables, including photovoltaic power plants and wind parks, introduce new challenges concerning fluctuations and instabilities that are inserted to the system grid that needs to maintain perfect balance of load and supply. Moreover, the advancement in new automation systems that are deployed in DERs, consequently, increase the attack surface by introducing new threats and vulnerabilities that need to be monitored and mitigated to avoid grid failures and possible cascading effects.

SDN-microSENSE offers a variety of tools that shield modern DERs against cyberthreats and provide mechanisms that mitigate and prevent failures and cascading effects. In the fifth use case, the complete set of solutions of SDN-microSENSE is showcased, including anomaly detection, threat sharing, risk analysis and vulnerability assessment, network reconfiguration via SDN as well as isolation and energy management procedures to maintain grid stability. In more detail, the use case concerns a range of cyberattacks against the infrastructure of the photovoltaic park of ALKYONIS, including Man-in-the-Middle, Unauthorized Access and Denial of service attacks, that can cause severe damage to the digital inverters and the SDN-enabled RTU of ALKYONIS. The photovoltaic park supplies the Municipality of Avdera (MoA), which means that anomalies and failures presented in ALKYONIS, due to the aforementioned cyberattacks, can cause cascading effects to MoA, including regional blackouts, that can take off critical infrastructures (e.g. hospitals), and fluctuations that can harm critical or commercial electrical equipment. In this context, SDN-microSENSE components undertake to prevent such events, by employing anomaly detection, through SS-IDPS and XL-SIEM, which notify the S-RAF and SDN-SELF frameworks respectively to evaluate the situation and propose the most appropriate mitigation actions, such as the isolation of the attacker via the SDN layer. Moreover, considering the effects of each attack, IIM and EMO may propose reconfiguration of the grid, for example after a failure of a PV unit, in order to restore energy balance and grid stability.

The main actors of this use case are the energy producer (ALKYONIS) and the energy consumer (MoA). ALKYONIS owns the DER facility that needs to be protected and MoA is supplied by the energy producer, thus being directly affected by any grid anomalies. Energy consumers of MoA may refer to critical facilities, residential and commercial areas as well as public services. Finally, this use case involves the operator (PPC) that monitors the supply of MoA and the overall grid status. External stakeholders that are indirectly involved in this scenario include the DSO that interface ALKYONIS with the national grid and the market operator (LAGIE) which determines the system marginal price.

7.5.2 Business Model Canvas

Table 18: Use Case 5 Business Model Canvas

<table>
<tr>
<td rowspan="2">Key Partners
• Consortium partners
• Grid Component Suppliers</td>
<td>Key Activities
• Protection from cyber-attacks, including both detection and mitigation of threats
• Optimize Grid operation, including protection, islanding/isolation and energy management
• Conduct risk assessment which will lead to vulnerability discoveries, threat detection and mitigation</td>
<td rowspan="2">Value Proposition
• Cyberthreats detection and mitigation in the operational environment of a PV power plant
• Addressing and mitigating cascading effects that can have real-life consequences
• Power grid security</td>
<td>Customer Relationships
• Long-term B2B relationships: Bilateral contacts and direct Interaction with the customers. Establish a speedy customer response strategy</td>
<td rowspan="2">Customer Segments
• Power plant operators, including DERs
• DSOs
• TSOs
• Microgrids in sensitive installations (i.e. Military bases, hospitals)
• Energy Communities</td>
</tr>
<tr>
<td>Key Resources
• The state-of-art technology that SDN-microSENSE is based on, that implements advanced network management, threat detection/mitigation, risk assessment and power grid monitoring.
• The technical partners (technology providers) involved in the development of the SDN-microSENSE platform.
• Technical personnel in the pilot sites to provide real data from the operational environment (e.g. electricity measurements and network traffic).</td>
<td>Channels
• Participation in targeted exhibitions and workshops related to power grid (i.e. Enlit Europe)
• Dissemination activities, including publications, flyers, newsletters and blog posts.
• Pilot demonstrations</td>
</tr>
<tr>
<td colspan="2">Cost Structure
• Development of the SDN-microSENSE software components
• Purchase of hardware equipment that interacts with the software (e.g. SDN switches, SDN-enabled RTUs)
• Infrastructure maintenance that hosts the SDN-microSENSE platform</td>
<td colspan="3">Revenue Streams
The main sources of revenue include the following: i) lump sum platform deployment, configuration and activation fee, ii) subscription service fees for update, maintenance and technical support in a monthly or yearly basis, iii) volume fees</td>
</tr>
</table>

Table 18 presents the business model canvas of use case 5.

The **key partners** involved in the use case are the consortium partners that develop the technologies and frameworks of SDN-microSENSE project, and the suppliers of grid components.

One of the **key activities** of the use case 5 is the effective and efficient protection of the microgrid from cyber-attacks, including both detection and mitigation of threats. Moreover SDN-microSENSE will optimize the grid operation, including protection, islanding/isolation and energy management. Furthermore, in this use case a risk assessment will be conducted, leading to vulnerability discoveries, threat detection and mitigation

The **value Proposition** of the use case includes:

- Cyberthreats detection and mitigation in the operational environment of a PV power plant
- Addressing and mitigating cascading effects that can have real-life consequences
- Power grid security

The main type of **relationships with customers** are long-term B2B relationships, where bilateral contacts will be signed with the clients (i.e. with RES operators, DSOs and energy communities). Direct interaction and a speedy response strategy will be established with customers in order to achieve a better understanding of their needs and provide a high level of service quality.

The main **customer segments** are: Power Plant operators, including DERs, DSOs, TSOs, Microgrids in sensitive installations (i.e. Military bases, hospitals) and Energy Communities

The **key resources** for the use case include:

- the state-of-art technology that SDN-microSENSE is based on, which implements advanced network management, threat detection/mitigation, risk assessment and power grid monitoring
- the technical partners (technology providers) involved in the development of the SDN-microSENSE platform.
- technical personnel in the pilot sites that will provide real data from the operational environment (e.g. electricity measurements and network traffic).

The **main channels** of delivering our value proposition include participation in targeted exhibitions and venues in the Energy Sector, dissemination activities, including publications, flyers, newsletters and blog posts and the Pilot demonstrations. Moreover, the involved project partners have developed close personal ties to national and European power sector companies, power plant and DER operators and can use their communication channels for the promotion of the SDN-microSENSE solution.

The **key costs** in our business model include the development of the SDN-microSENSE software components, the purchase of hardware equipment that interacts with the software (e.g. SDN switches, SDN-enabled RTUs) and the maintenance of the infrastructure that hosts the SDN-microSENSE platform.

Our values proposition's main **revenue streams** stem from clients, mainly power plant and DER operators. The main sources of revenue include the following: i) lump sum platform deployment, configuration and activation fee, ii) subscription service fees for the update, maintenance and technical support in a monthly or yearly basis, iii) volume fees

7.5.3 Activity map

In a succinct overview of the business model activity map, as shown in Figure 30, the relations between core activities and value-adding activities are depicted. The three darker circles represent the foundations of the overall core activities. All of the other activities support or add value to the core activities of the use case. The activity map consists of three main core activities and six value-adding activities. The main core activities are protection from cyberattacks, including both detection and mitigation, risk assessment and Grid protection, including islanding/isolation and energy management.

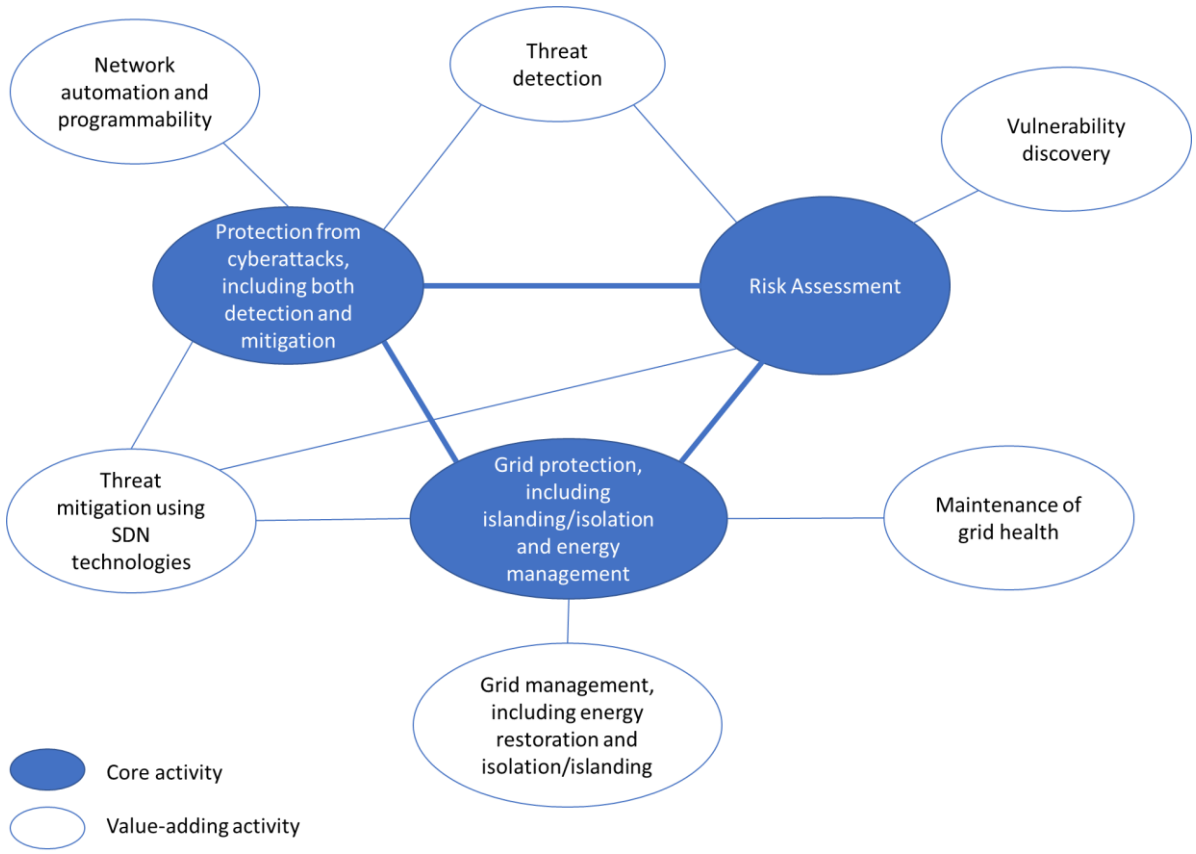


Figure 30: Use Case 5 Activity Map

The value-adding activities of the use case include threat detection, threat mitigation utilising SDN technologies, grid management, including energy restoration and isolation/islanding, vulnerability discovery, network automation and programmability, and, last but not least, maintenance of grid health.

7.6 Use Case 6: Realising Private and Efficient Energy Trading among PV Prosumers

7.6.1 Use Case Description

Electric power networks are headed towards a distributed generation paradigm, where prosumers, self-consumption and renewable energy generation will play a greater role and radically transform the sector. Addressing these transformations, this use case deals with the realization of Private and Efficient Energy Trading among PV Prosumers. The SDN-microSENSE solution addresses one of the most important changes that will promote "self-consumption" in the energy sector, the transformation of the consumer into prosumer, and their participation in energy trading, putting the privacy and security of the individual and sensitive data as of utmost importance when considering sharing prosumers data.

The specific deployment will demonstrate crucial aspects of the SDN-microSENSE solution, specifically the energy exchange capabilities and the provided data breach protection. In more detail, the proposed SDN-SELF techniques will be applied for energy exchange between the participating buildings. According to the adopted concept, the buildings have different peak power generation times; during these times, the corresponding building can transmit power to another requesting building. The energy exchange is agreed between the two parties using smart contracts, which dictate the amount of energy to be transmitted and the receiver's obligation to return the power when it has a surplus and upon request. The energy exchange details are recorded as a transaction in the shared Ethereum-based blockchain. The suggestions regarding the optimal energy exchanges (participants, time, amount of exchanged energy) are provided by the Cloud-based Monitoring Platform, which collects power generation/consumption information from the three buildings to feed the respective optimisation algorithms. Moreover, as part of the XL-EPDS privacy framework, homomorphic encryption is first applied to the links to the Cloud-based Monitoring Platform for advanced confidentiality. Furthermore, to protect against revealing the details of the energy consumption patterns, consumption shaping techniques are tested on the installed residential energy storage systems. Private Information Retrieval techniques are also applied on the platform to allow prosumers/consumers to access their data without jeopardising their own privacy.

This use case validates and demonstrates the efficiency of the SDN-microSENSE platform in implementing a trading environment, based on the SDN-SELF blockchain technologies, that can respond to real-time outages caused by network conditions or cyberthreats and mitigate trading agreements in support of network flexibility, stability, energy balancing and valorisation. It investigates how energy related capacities of the buildings can be traded within the area maximizing resource and economic efficiency, while improving security and privacy aspects.

Furthermore, the SDN-microSENSE solution will protect consumers and prosumers privacy by demonstrating the XL-EPDS privacy protection platform in the consumers and prosumers premises when private data are collected and being transmitted to the operator control centre. Overall, the adjusted SDN-microSENSE solution for this use case will involve testing and implementation of SDN-SELF (Blockchain, IIM, EMO, EDAE), XL-EPDS (ARIEC) applications and Management plane components such as Privacy protection framework and GridPilot.

In this particular use case (Pilot 6), the focus is on testing the SDN-SELF, which will be implemented for the private and efficient energy trading amongst PV Prosumers. Our partner CheckWatt AB will provide dataset required for this work package. Given the specificity of the data, which come from a pool of

over 4,000 PV Swedish real prosumers, Pilot 6 is expected to achieve an output of substantial depth for a potential scale up phase.

In addition Pilot 6 is of particular importance and current pertinence since it explores elements related to unauthorized access to data/network that could be used for identity theft, fudging of data or used as access to the bigger actors in the electricity system for example, energy suppliers network via Advanced Persistent threats. Therefore, protection of these data against a privacy and theft at both the prosumer level, i.e. smart meters and more centrally, i.e. servers, is of high priority.

In particular, three scenarios are applied to Pilot 6. The first scenario focuses on attacks on data privacy and how SDN-microSENSE components would implement data protection by restrictive access and anonymisation. The second scenario deals with the attacks on the energy trading platform and how a blockchain based system could provide a secured and reliable trading platform and thirdly on the self-healing aspect of the SDN energy management tools during restoration in the case of an attack.

The main actors of this use case are residential prosumers, community prosumers, DSOs and energy traders. The prosumer is in the centre of this use case, emerging as a great agent of change and value generation, which can be either connected to a microgrid (grid-connected or islanded) or to the main grid. The engaged stakeholders are citizens, businesses, energy utilities, energy communities, and in a broader perspective investors, policymakers, and regulators. Some of these groups play essential role in the implementation of the use case, while others may simply have valuable information, interest, or contacts that help the SDN-microSENSE develop an appropriate solution which is likely to succeed given local conditions.

7.6.2 Business Model Canvas

Table 19: Use Case 6 Business Model Canvas

<table>
<tr>
<td rowspan="2">Key Partners
• Consortium partners
• Blockchain technology provider</td>
<td>Key Activities
• Use of blockchain technology for accessing and sharing energy data
• Mitigating trading agreements in support of network flexibility and stability
• Implementation of a private and reliable decentralized energy trading environment</td>
<td rowspan="2">Value Proposition
• Use case 6 demonstrates how the SDN-microSENSE solution can address different privacy and security issues in energy trading services, by developing secure, trustworthy and GDPR compliant products for communication among actors and safe exchange of energy trading data
• Self-consumption optimization considering grid and user needs
• Privacy protected energy trading</td>
<td>Customer Relationships
• B2B: These long-termrelationships will be achieved mainly through contacts with industrial energy partners, alongside with targeted exhibitions and venues for the Energy Sector.
• B2C: Long-term relationships with customers, mainly prosumers and energy communities, will be achieved through branding activities in different channels, aiming to build a trustworthy brand name with a publicly recognized logo.</td>
<td rowspan="2">Customer Segments
• Prosumers
• Energy Aggregators
• DSOs
• TSOs
• Energy communities</td>
</tr>
<tr>
<td>Key Resources
• The experienced and highly-qualified personnel that works on the development and validation of the technologies
• SDN-SELF blockchain technology
• SDN-microSENSE Privacy Protection Framework
• Energy-trading Platform</td>
<td>Channels
• Customers will be reached mainly through direct contact, dissemination activities and partners' initiatives.
• Services will be provided through web/mobile/cloud service channels
• Through European Union, Government Bodies</td>
</tr>
<tr>
<td colspan="2">Cost Structure
The key cost in this solution concern the development and platform design of the SDN-microSENSE platform, as well as variable costs, such as software and database maintenance, ICT equipment and acquisition of components.</td>
<td colspan="3">Revenue Streams
Our revenue sources are the following: i) once-off set -up and activation fee, ii) monthly account maintenance and technical support fees, iii) volume fees</td>
</tr>
</table>

Table 19 presents the business model canvas of use case 6.

The **key partners** involved in the use case are the consortium partners who are the technology developers and integrators of the SDN-microSENSE solution. Furthermore, another key partner is the blockchain technology provider, who will allow for the recording of transactions on a distributed ledger.

Regarding the **key activities** of the use case, blockchain technology will be used for accessing and sharing energy data. Furthermore the SDN-microSENSE solution, through the SDN-SELF component, will be able of mitigating trading agreements in support of network flexibility and stability Finally another key activitiy of the use case involves the development of a private and reliable decentralized energy trading environment for the implementation of direct energy trades among prosumers or/and microgirds.

In regard to the **value proposition** of the use case, it is demonstrated how the SDN-microSENSE solution can address different privacy and security issues in energy trading services by developing secure, trustworthy and GDPR compliant products for communication among actors and safe exchange of energy trading data. Furthermore, self-consumption optimization considering grid and user needs and power grid security are enhanced through the utilization of the SDN-microSENSE platform, while privacy protected energy trading is enabled.

The use case builds **customer relationships** with both B2B and B2C customers. More specifically, long-term B2B relationships will be achieved mainly through contacts with industrial energy partners, alongside with targeted exhibitions and venues for the Energy Sector. Long-term B2C relationships with customers, mainly prosumers and energy communities, will be achieved through branding activities in different channels, aiming to build a trustworthy brand name with a publicly recognized logo.

The main **customer segments** are Prosumers, Energy Aggregators, DSOs, TSOs and Energy communities.

The **key resources** for the use case stem from the development of the SDN-microSENSE tools:

- The experienced and highly-qualified personnel that works on the development and validation of the technologies
- SDN-SELF blockchain technology
- SDN-microSENSE Privacy Protection Framework
- Energy-trading Platform

Regarding the **channels** through which the SDN-microSENSE partners will reach their clients, customers will be reached mainly through direct contact, dissemination activities and partners' initiatives. The value proposition of SDN-microSENSE and the use case results will be also promoted through European Union Bodies and Government Bodies. Furthermore, services will be provided through web/mobile/cloud service channels.

The **key cost** in this solution concerns the development and platform design of the SDN-microSENSE platform, as well as variable costs, such as software and database maintenance, ICT equipment and acquisition of components. A low-cost value proposition will be adopted while special focus will be given on social impact creation.

Our value proposition will generate **revenue** through its clients, mainly prosumers and energy communities, who will be willing to pay for: i) activation and set-up, ii) monthly account maintenance and iii) subscription service Our revenue sources are the following: i) once-off activation fee, ii) monthly fees, and iii) volume fees .

7.6.3 Activity map

In a succinct overview of the business model activity map, as shown in Figure 31, the relations between core activities and value-adding activities are depicted. The activity map consists of three main core activities and five value-adding activities. The main core activities are energy trading, privacy protection and data management.

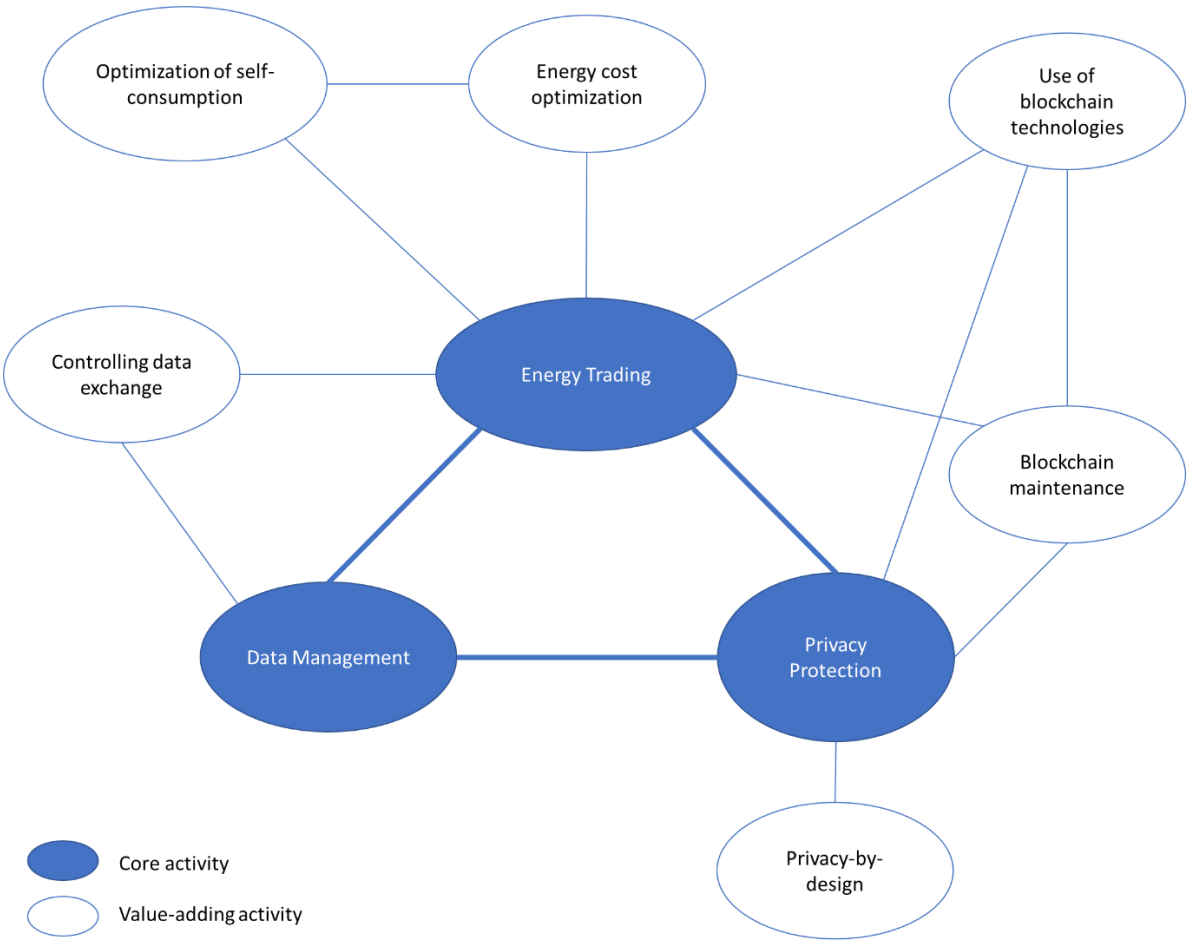


Figure 31: Use Case 6 Activity Map

The value-adding activities of this use case include the use and maintenance of blockchain technologies, the monitoring and control of data exchange, the optimization of self-consumption, the energy cost optimization and the Privacy-by design approach.

8. Conclusions

The Critical Infrastructure Cyber Security Market has been growing rapidly for the past few years. With the emergence of advanced cyber-threats on the power grid, the need for continuous development of cyber security solutions that protect the power grid is imminent. Cyberattacks are becoming more sophisticated and frequent, exposing organizations and nations to new risks that cut across the technology and underlying systems that govern society.

SDN-microSENSE project aims to respond to these challenges by providing a set of secure, privacy-enabled and resilient to cyberattacks tools, thus ensuring the normal operation of the power system, as well as the integrity and the confidentiality of communications. Understanding the market potential of the SDN-microSENSE solution is crucial for the future steps of the project in terms of exploitation and commercialization. This deliverable provides the necessary market concept that is required to be clear for the implementation of the SDN-microSENSE solution, elaborates on the market characteristics and illustrates the business roadmap of the project as well as the business models that are followed on the use cases of the project.

The PESTLE analysis indicated that SDN-microSENSE has the potential to be adopted in the European Market, as well as globally, especially in terms of key partners being utilized to launch the product. The EU market as a whole and the market that SDN-microSENSE will be initially targeting (the EU critical infrastructure sector) can be assessed as favourable for launching an innovative from all aspects; Political, Economic, Social, Technological, Legal and Environmental.

The Five Forces of Porter analysis indicated that the market is quite competitive, but definitely attractive with sustainable growth opportunities. The bargaining power of suppliers is considered as low due to the big number of competitors offering similar services. The bargaining power of buyers is considered to be low-medium. On one hand there is a number of existing Cyber Security solutions that provide a level of service. On the other hand, SDN-microSENSE includes a set of innovative tools that no other cybersecurity solution provides currently in the market.

The threat of new entry is assessed as low-medium. Although the barriers of entry in order to create a product like SDN-microSENSE are high, the market itself is quite lucrative with large IT companies aspiring to enter the market. The threat of substitute products is considered as low-medium, since there are already products offering similar services with some of the SDN-microSENSE services but none of those products is able to provide the bundle of tools that is offered by our solution. Industry Rivalry is considered to be low-medium for the same reason, however this might change once SDN-microSENSE is launched in the Critical Infrastructure Cyber Security Market.

The SWOT analysis assessed the strengths and weaknesses of the internal environment of SDN-microSENSE, along with the external opportunities and threats. Overall, the strategic advantage of SDN-microSENSE has been assessed as quite high. The information derived from the analysis will direct the future strategy of SDN-microSENSE, focusing on its strengths and highlighting its weaknesses.

The Fuzzy AHP Analysis conducted among experts has identified technology and features of the developed SDN-microSENSE solution, as well as security, being the most important factors that affect the adoption of the SDN-microSENSE outcomes.

The SDN-microSENSE use cases have been carefully selected and contribute greatly to the value proposition of the SDN-microSENSE, demonstrating the SDN-microSENSE developed tools and

platform and the solutions that it provides on the critical infrastructure field. The potential clients of the SDN-microSENSE solution have been identified, while the analysis performed has taken into account the particularities of each use case, creating six testable hypotheses for the business approach that SDN-microSENSE could adopt. As a result of the business modelling and stakeholder analysis, the six use cases could be summarised as follows.

Use case 1 investigates a series of versatile cyber-attacks and demonstrates how the SDN-microSENSE platform confronts a variety of attack methodologies in the EPES infrastructure. The particular use case shows that the SDN-microSENSE solution can be utilized for R&D and testing activities at a low cost. Industrial partners, Energy Utilities, TSOs and DSOs and academic institutes are the targeted customers of this use case.

Use case 2 demonstrates a massive false data injection cyberattack against state operation and automatic generation control, while the majority of the SDN-microSENSE developed tools are tested. Through this use case, it is validated that the SDN-microSENSE platform complies with the core functionalities of a Cybersecurity Framework, being able to identify, protect, detect, respond, and recover from cyberattacks. Industrial partners, Energy Utilities, TSOs and DSOs are the targeted customers of this use case.

Use case 3 investigates a large-scale islanding scenario using real-life infrastructure. It is demonstrated in a real-world environment how the SDN-microSENSE platform performs islanding processes in order to isolate a problem area of the grid, which could be exposed to a cyber-attack. This use case is of particular importance to Governmental Institutions, TSOs and DSOs.

Use Case 4 demonstrates how the SDN-microSENSE solution can address coordinated cyber-attacks from multiple external sources that use a variety of attacking tools and methods. Customers that would be interested in the results of this use case include DSOs, TSOs, Governments and Energy agencies.

Use Case 5 demonstrates the SDN-microSENSE capability to perform grid restoration and aims to benefit sensitive regions, like islands or rural areas, that could be significantly affected by a power grid failure. The solution is clearly focused on remote rural communities and RES producers, with high potential to be expanded to islands and critical infrastructures like military or hospital microgrids.

Use Case 6 validates and demonstrate the efficiency of the SDN-microSENSE platform in implementing a trading environment, based on the SDN-SELF blockchain technologies, that can respond to real-time outages caused by network conditions or cyberthreats. The target market of this use case includes prosumers, DR aggregators, energy communities and energy utilities.

Based on the business analysis of the project's six use cases, the BMC assessment has broadened the heterogeneity of possible business approaches that can be adopted by SDN-microSENSE. A wide field of value propositions, customers and channels have been identified. Furthermore, a wide range of key activities and key resources which are needed to deliver the value propositions have been identified.

In spite of the heterogeneity of the use cases, certain key features that are relevant for each business model have been observed. The possible revenue streams are common for all use cases ,while the main customer segments are similar, aiming to target a mass market.

The preliminary observations and the information provided on this deliverable constitute a solid basis for the future work of Work Package 9 and enhance the commercialization potential of the project.

References

[1] Tan, J. , W. L.Chua, C. K.Chow, M. C.Chong, and B. C.Chew . 2012. “PESTLE Analysis on Toyota Hybrid Vehicles .” *IC-TMT* 2012: 1–7

[2] C. Zalengera, R. Blanchard, P. Eames, A. Juma, M. Chitawo and K. Gondwe, "Overview of the Malawi energy situation and A PESTLE analysis for sustainable development of renewable energy", *Renewable and Sustainable Energy Reviews*, vol. 38, pp. 335-347, 2014. Available: 10.1016/j.rser.2014.05.050 [Accessed 27 July 2020].

[3] R. Reinhardt, S. Domingo, B. Garcia and I. Christodoulou, "Macro environmental analysis of the electric vehicle battery second use market", *2017 14th International Conference on the European Energy Market (EEM)*, 2017. Available: 10.1109/eem.2017.7982031 .

[4] D. Issa, A. Chang and D. Issa, "Sustainable Business Strategies and PESTEL Framework", *GSTF INTERNATIONAL JOURNAL ON COMPUTING*, vol. 1, no. 1, 2010. Available: 10.5176/2010-2283_1.1.13.

[5] A. Christodoulou and K. Cullinane, "Identifying the Main Opportunities and Challenges from the Implementation of a Port Energy Management System: A SWOT/PESTLE Analysis", *Sustainability*, vol. 11, no. 21, p. 6046, 2019. Available: 10.3390/su11216046.

[6] J. Song, Y. Sun and L. Jin, "PESTEL analysis of the development of the waste-to-energy incineration industry in China", *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 276-289, 2017. Available: 10.1016/j.rser.2017.05.066.

[7] Porter ME. The five competitive forces that shape strategy. Harvard business review. 2008 Jan 1;86(1):25-40.

[8] G. Karagiannopoulos, N. Georgopoulos and K. Nikolopoulos, "Fathoming Porter's five forces model in the internet era", *info*, vol. 7, no. 6, pp. 66-76, 2005. Available: 10.1108/14636690510628328

[9] K. Uchino, "Piezoelectric Actuators 2008: Key Factors for Commercialization", *Advanced Materials Research*, vol. 55-57, pp. 1-9, 2008. Available: 10.4028/www.scientific.net/amr.55-57.1.

[10] W. Yunna and Y. Yisheng, "The competition situation analysis of shale gas industry in China: Applying Porter’s five forces and scenario model", *Renewable and Sustainable Energy Reviews*, vol. 40, pp. 798-805, 2014. Available: 10.1016/j.rser.2014.08.015 .

[11] T. Grundy, "Rethinking and reinventing Michael Porter's five forces model", *Strategic Change*, vol. 15, no. 5, pp. 213-229, 2006. Available: 10.1002/jsc.764 .

[12] M. Asad, "Porter Five Forces vs Resource Based View - A Comparison", *SSRN Electronic Journal*, 2012. Available: 10.2139/ssrn.1986725 .

[13] H. Fung, "Using Porter Five Forces and Technology Acceptance Model to Predict Cloud Computing Adoption among IT Outsourcing Service Providers", *Internet Technologies and Applications Research*, vol. 1, no. 2, p. 18, 2014. Available: 10.12966/itar.09.02.2013.

[14] M. E. Dobbs, "Guidelines for applying Porter's five forces framework: a set of industry analysis templates", *Competitiveness Review*, vol. 24, no. 1, pp. 32-45, 2014. Available: 10.1108/cr-06-2013-0059 .

[15] R. Dyson, "Strategic development and SWOT analysis at the University of Warwick", *European Journal of Operational Research*, vol. 152, no. 3, pp. 631-640, 2004. Available: 10.1016/s0377-2217(03)00062-6 .

[16] Gürel E, Tat M. SWOT analysis: a theoretical review. Journal of International Social Research. 2017 Aug 1;10(51).

[17] E. Valentin, "Swot Analysis from a Resource-Based View", *Journal of Marketing Theory and Practice*, vol. 9, no. 2, pp. 54-69, 2001. Available: 10.1080/10696679.2001.11501891.

[18] B. Phadermrod, R. Crowder and G. Wills, "Importance-Performance Analysis based SWOT analysis", *International Journal of Information Management*, vol. 44, pp. 194-203, 2019. Available: 10.1016/j.ijinfomgt.2016.03.009.

[19] "SWOT analysis: A 'How To' Example of Best Practice", *Paul Boag - User Experience Advice*, 2020. [Online]. Available: https://boagworld.com/digital-strategy/swot-analysis/.

[20] J. Jaber, F. Elkarmi, E. Alasis and A. Kostas, "Employment of renewable energy in Jordan: Current status, SWOT and problem analysis", *Renewable and Sustainable Energy Reviews*, vol. 49, pp. 490-499, 2015. Available: 10.1016/j.rser.2015.04.050 [Accessed 27 July 2020].

[21] C. Okello, S. Pindozzi, S. Faugno and L. Boccia, "Appraising Bioenergy Alternatives in Uganda Using Strengths, Weaknesses, Opportunities and Threats (SWOT)-Analytical Hierarchy Process (AHP) and a Desirability Functions Approach", *Energies*, vol. 7, no. 3, pp. 1171-1192, 2014. Available: 10.3390/en7031171.

[22] J. Terrados, G. Almonacid and P. Pérez-Higueras, "Proposal for a combined methodology for renewable energy planning. Application to a Spanish region", *Renewable and Sustainable Energy Reviews*, vol. 13, no. 8, pp. 2022-2030, 2009. Available: 10.1016/j.rser.2009.01.025.

[23] B. Cayir Ervural, S. Zaim, O. Demirel, Z. Aydin and D. Delen, "An ANP and fuzzy TOPSIS-based SWOT analysis for Turkey's energy planning", *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 1538-1550, 2018. Available: 10.1016/j.rser.2017.06.095 [Accessed 27 July 2020].

[24] T. L. Saaty, "A scaling method for priorities in hierarchical structures," Journal of Mathematical Psychology, vol. 15, pp. 234-281, 1977.

[25] A. M. A. Bahurmoz, "The analytic hierarchy process at DarAl-Hekma, Saudi Arabia," Interfaces, vol. 33, pp. 70-78, 2003.

[26] A. Kengpol and C. O'Brien, "The development of a decision support tool for the selection of advanced technology to achieve rapid product development," International Journal of Production Economics, vol. 69, pp. 177-191, 2001.

[27] G. Noci and G. Toletti, "Selecting quality-based programmes in small firms: A comparison between the fuzzy linguistic approach and the analytic hierarchy process," International Journal of Production Economics, vol. 67, pp. 113-133, 2000.

[28] M. M. Albayrakoglu, "Justification of New Manufacturing Technology: A Strategic Approach Using the Analytical Hierarchy Process," Production and Inventory Management Journal, First Quarter, vol. 37, pp. 71-76, 1996.

[29] T. L. SAATY, The analytic hierarchy process: planning, priority setting, resource allocation. New York: McGraw-Hill International Book Co., 1980.

[30] G. Dede, et al., "Towards a Roadmap for Future Home Networking Systems: An Analytical Hierarchy Process Approach," IEEE Systems Journal, vol. 5, pp. 374-384, 2011.

[31] G. Dede, et al., "Evaluation of Optical Wireless Technologies in Home Networking: An Analytical Hierarchy Process Approach," IEEE/OSA Journal of Optical Communications and Networking, vol. 3, pp. 850-859, 2011.

[32] S. Nikou, et al., "Analytic Hierarchy Process (AHP) Approach for Selecting Mobile Service Category (Consumers' Preferences)," in 2011 10th International Conference on Mobile Business, 2011, pp. 119-128.

[33] S. Qingyang and A. Jamalipour, "Network selection in an integrated wireless LAN and UMTS environment using mathematical modeling and computing techniques," IEEE Wireless Communications, vol. 12, pp. 42-48, 2005.

[34] D.-Y. Chang, "Applications of the extent analysis method on fuzzy AHP," European Journal of Operational Research, vol. 95, pp. 649-655, 1996.

[35] P. J. M. van Laarhoven and W. Pedrycz, "A fuzzy extension of Saaty's priority theory," Fuzzy Sets and Systems, vol. 11, pp. 229-241, 1983/01/01 1983.

[36] T.-H. Chang and T.-C. Wang, "Using the fuzzy multi-criteria decision making approach for measuring the possibility of successful knowledge management," Information Sciences, vol. 179, pp. 355-370, 2009.
[37] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, pp. 338-353, 1965.
[38] G. Büyüközkan and O. Feyzıoğlu, "A fuzzy-logic-based decision-making approach for new product development," International Journal of Production Economics, vol. 90, pp. 27-45, 2004.
[39] J. J. Buckley, "Ranking alternatives using fuzzy numbers," Fuzzy Sets and Systems, vol. 15, pp. 21-31, 1985/02/01 1985.
[40] J. J. Buckley, "Fuzzy hierarchical analysis," Fuzzy Sets and Systems, vol. 17, pp. 233-247, 1985/12/01 1985.
[41] J. J. Buckley, et al., "Fuzzy hierarchical analysis revisited," European Journal of Operational Research, vol. 129, pp. 48-64, 2001.
[42] A. P. D. Mark, "A Multicriteria Decision Model Application for Managing Group Decisions," The Journal of the Operational Research Society, vol. 45, pp. 47-58, 1994.
[43] T. L. Saaty and M. S. Ozdemir, "Why the magic number seven plus or minus two," Mathematical and Computer Modelling, vol. 38, pp. 233-244, 2003.
[44] M. Enea and T. Piazza, "Project Selection by Constrained Fuzzy AHP," Fuzzy Optimization and Decision Making, vol. 3, pp. 39-62.
[45] Z. Güngör, et al., "A fuzzy AHP approach to personnel selection problem," Applied Soft Computing, vol. 9, pp. 641-646, 2009.
[46] F. Tiryaki and B. Ahlatcioglu, "Fuzzy portfolio selection using fuzzy analytic hierarchy process," Information Sciences, vol. 179, pp. 53-69, 2009.
[47] N.-F. Pan, "Fuzzy AHP approach for selecting the suitable bridge construction method," Automation in Construction, vol. 17, pp. 958-965, 2008.
[48] M. H. Vahidnia, et al., "Hospital site selection using fuzzy AHP and its derivatives," Journal of Environmental Management, vol. 90, pp. 3048-3056, 2009.
[49] S. Tesfamariam and R. Sadiq, "Risk-based environmental decision-making using fuzzy analytic hierarchy process (F-AHP)," Stochastic Environmental Research and Risk Assessment, vol. 21, pp. 35-50, 2006.
[50] N.-F. Pan, "Fuzzy AHP approach for selecting the suitable bridge construction method," Automation in Construction, vol. 17, pp. 958-965, 2008.
[51] M. H. Vahidnia, et al., "Hospital site selection using fuzzy AHP and its derivatives," Journal of Environmental Management, vol. 90, pp. 3048-3056, 2009.
[52] S. Tesfamariam and R. Sadiq, "Risk-based environmental decision-making using fuzzy analytic hierarchy process (F-AHP)," Stochastic Environmental Research and Risk Assessment, vol. 21, pp. 35-50, 2006.
[53] G. Zheng, et al., "Application of a trapezoidal fuzzy AHP method for work safety evaluation and early warning rating of hot and humid environments," Safety Science, vol. 50, pp. 228-239, 2012
[54] A. Osterwalder and Y. Pigneur, *Business model generation*. Hoboken, N.J.: Wiley, 2009.
[55] M. Toro-Jarrín, I. Ponce-Jaramillo and D. Güemes-Castorena, "Methodology for the of building process integration of Business Model Canvas and Technological Roadmap", *Technological Forecasting and Social Change*, vol. 110, pp. 213-225, 2016. Available: 10.1016/j.techfore.2016.01.009 [Accessed 27 July 2020].
[56] "Social Entrepreneurship - Base of the Pyramid Business model Innovation", *PennState College of Engineering*. [Online]. Available: https://sites.psu.edu/edsgn453/9-social-entrepreneurship/. [Accessed: 27- Jul- 2020].
[57] "Business Model Canvas Template - A Guide to Business Planning", *Corporate Finance Institute*. [Online]. Available:

https://corporatefinanceinstitute.com/resources/knowledge/strategy/business-model-canvas-template/. [Accessed: 27- Jul- 2020].
[58] R. Li, H. Song and S. Su, "Study on Business Model of Virtual Power Plant based on Osterwalder Business Model Canvas", *2019 IEEE 3rd International Electrical and Energy Conference (CIEEC)*, 2019. Available: 10.1109/cieec47146.2019.cieec-2019632 [Accessed 27 July 2020].
[59] M. Urban, M. Klemm, K. Ploetner and M. Hornung, "Airline categorisation by applying the business model canvas and clustering algorithms", *Journal of Air Transport Management*, vol. 71, pp. 175-192, 2018. Available: 10.1016/j.jairtraman.2018.04.005 [Accessed 27 July 2020].
[60] "Activity Map", *Strategic Toolkits*. [Online]. Available: http://strategictoolkits.com/strategic-concepts/activity-map/. [Accessed: 27- Jul- 2020].
[61] A. Smith, W. Rupp and D. Motley, "Corporate reputation as strategic competitive advantage of manufacturing and service-based firms: multi-industry case study", *International Journal of Services and Operations Management*, vol. 14, no. 2, p. 131, 2013. Available: 10.1504/ijsom.2013.051826 [Accessed 27 July 2020].
[62] Seddon, Peter B. and Geoffrey P. Lewis. "Strategy and Business Models: What's the Difference?" *PACIS*, 2003.
[63] Bulmer S., "The member states of the European Union," Oxford University Press, USA, 2020.
[64] Treaty on the Functioning of the European Union, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010 / C83 / 01) Available at: http://www.minjust.gov.ua/file/23491.PDF.
[65] The Energy Community Treaty. Official Journal, 20.7.2006, L 198. Available at: http://www.energycommunity.org
[66] "Employment rate of people aged 20 to 64 in the EU reached a new peak at 73.2% in 2018", *Eurostat newsletter*, 2020. [Online]. Available: https://ec.europa.eu/eurostat/documents/2995521/9747515/3-25042019-AP-EN.pdf/b226fab2-566d-4dad-a830-a22b9fa5c251. [Accessed: 27- Jul- 2020].
[67] M. Lindström and S. Olsson, "The European Programme for Critical Infrastructure Protection", *Crisis Management in the European Union*, pp. 37-59, 2009. Available: 10.1007/978-3-642-00697-5_3 [Accessed 14 July 2020].
[68] "Policy on Critical Information Infrastructure Protection (CIIP) - Shaping Europe's digital future - European Commission", *Shaping Europe's digital future - European Commission*, 2013. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip. [Accessed: 14- Jul- 2020].
[69] "Challenges to effective EU cybersecurity policy", 2019. [Online]. Available: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf. [Accessed: 14- Jul- 2020].
[70] "Proposal for a Regulation on Privacy and Electronic Communications - Shaping Europe's digital future - European Commission", *European Commission*, 2020. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications. [Accessed: 14- Jul- 2020].
[71] "Winter 2020 Economic Forecast - European Commission", *European Commission - European Commission*, 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_232. [Accessed: 14- Jul- 2020].
[72] "Summer 2020 Economic Forecast: An even deeper recession with wider divergences - European Commission", *European Commission*, 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1269. [Accessed: 14- Jul- 2020].
[73] "Summer 2019 Economic Forecast: Growth clouded by external factors - European Commission", *European Commission*, 2019. [Online]. Available:

https://ec.europa.eu/commission/presscorner/detail/en/IP_19_3850. [Accessed: 14- Jul- 2020].

[74] M. Pollitt, "The European Single Market in Electricity: An Economic Assessment", *Review of Industrial Organization*, vol. 55, no. 1, pp. 63-87, 2019. Available: 10.1007/s11151-019-09682-w [Accessed 14 July 2020].

[75] Population by Country (2020) - Worldometer." [Online]. Available: https://www.worldometers.info/world-population/population-by-country/.

[76] "The EU's population projected up to 2100 - Product - Eurostat." [Online]. Available: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20190710-1.

[77] "Sustainable development Goals - European Commission", *European Commission*. [Online]. Available: https://ec.europa.eu/sustainable-development/about_en. [Accessed: 14- Jul- 2020].

[78] "Europe faces shortage of 800,000 IT workers by 2020", *CloudWATCH*, 2020. [Online]. Available: https://www.cloudwatchhub.eu/europe-faces-shortage-800000-it-workers-2020. [Accessed: 14- Jul- 2020].

[79] "Global Smart Grid Cyber Security Market – Industry Analysis and Forecast (2018-2026)", *Maximizemarketresearch.com*. [Online]. Available: https://www.maximizemarketresearch.com/market-report/global-smart-grid-cyber-security-market/24516/. [Accessed: 14- Jul- 2020].

[80] "Cyber Security Market Size and Share | Industry Analysis, 2025", *Allied Market Research*,. [Online]. Available: https://www.alliedmarketresearch.com/cyber-security-market#:~:text=The%20cyber%20security%20market%20size,11.9%25%20from%202018%20to%202025. [Accessed: 14- Jul- 2020].

[81] S. Weerakkody and B. Sinopoli, "Challenges and Opportunities: Cyber-Physical Security in the Smart Grid", *Smart Grid Control*, pp. 257-273, 2018. Available: 10.1007/978-3-319-98310-3_16 [Accessed 14 July 2020].

[82] C. Greer et al., "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0", 2014. Available: 10.6028/nist.sp.1108r3 [Accessed 29 July 2020]."ISO/IEC 27002:2005", *ISO*, 2020. [Online]. Available: https://www.iso.org/standard/50297.html.

[83] G. Ridley, J. Young and P. Carroll, "COBIT and its utilization: a framework from the literature", *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, 2004. Available: 10.1109/hicss.2004.1265566 [Accessed 29 July 2020].

[84] "ISO/IEC 27002:2005", *ISO*. [Online]. Available: https://www.iso.org/standard/50297.html. [Accessed: 29- Jul- 2020].

[85] P. Voigt and A. von dem Bussche, "The EU General Data Protection Regulation (GDPR)", 2017. Available: 10.1007/978-3-319-57959-7 [Accessed 14 July 2020].

[86] S. Greengard, "Weighing the impact of GDPR", *Communications of the ACM*, vol. 61, no. 11, pp. 16-18, 2018. Available: 10.1145/3276744 [Accessed 14 July 2020].

[87] K. Begg, "The Kyoto Protocol — International Climate Policy for the 21st Century Sebastian Oberthür and E. Ott, Springer-Verlag, Berlin, Heidelberg, 1999, 359 pp., UK£ 37.50, ISBN 354066470X", *Climate Policy*, vol. 1, no. 1, pp. 145-146, 2001. Available: 10.1016/s1469-3062(00)00014-0.

[88] C. Böhringer, T. Rutherford and R. Tol, "THE EU 20/20/2020 targets: An overview of the EMF22 assessment", *Energy Economics*, vol. 31, pp. S268-S273, 2009. Available: 10.1016/j.eneco.2009.10.010 [Accessed 14 July 2020].

[89] "European Commission Cloud Strategy", *European Commission*, 2019. [Online]. Available: https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en#:~:text=The%20European%20Commission's%20cloud%20strategy,hybrid%20multi%2Dcloud%20service%20offering. [Accessed: 14- Jul- 2020].

[90] ""IBM QRadar SIEM", Ibm.com, 2019. [Online]. Available: https://www.ibm.com/uk-en/marketplace/ibm-qradar-siem." [Online].
[91] "McAfee Enterprise Security Manager", Mcafee.com, 2019. [Online]. Available: https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html .," [Online]. "
[92] "ArcSight Security Information and Event Management: SIEM Software," Micro Focus. [Online]. Available: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview. [Accessed: 29-Nov-2019]," [Online].
[93] "AlienVault OSSIM The world's most widely used open source SIEM," AT&T Cybersecurity. [Online]. Available: https://www.alienvault.com/products/ossim. [Accessed: 29-Nov-2019]," [Online].
[94] ""Trustwave SIEM Enterprise Overview," Trustwave, 03-Feb-2014. [Online]. Available: https://trustwave.azureedge.net/media/13581/tw-siem-enterprise.pdf. [Accessed: 29-Nov-2019]," [Online].
[95] "Kaspersky Endpoint Security" [Online]. Available: https://usa.kaspersky.com/small-to-medium-business-security.
[96] IBM Security Guardium - Smarter Data Protection", Ibm.com, 2019. [Online]. Available: https://www.ibm.com/security/data-security/guardium.
[97] "Risk Management Software Solution | LogicGate", LogicGate, 2019. [Online]. Available: https://www.logicgate.com/solutions/it-security-risk/.
[98] "Logicmanager ERM Software | Enterprise Risk Management & GRC Solutions", ERM Software, 2019. [Online]. Available: https://www.logicmanager.com/.
[99] CURA Risk Management Software Solutions, ERM Software", Cura Software, 2019. [Online]. Available: https://www.curasoftware.com/enterprise-risk-management/.
[100] "BitSight: Security Ratings Leader - Cyber Risk Management Solutions", BitSight, 2019. [Online]. Available: https://www.bitsight.com/.
[101] IBM Spectrum Protect Plus. Link: https://www.ibm.com/us-en/marketplace/ibm-spectrum-protect-plus.
[102] Rubrik polaris radar. Link: https://www.rubrik.com/product/polaris-radar/. Last visited: 04.09.2019.
[103] SolarWinds N-central. Link: https://www.solarwindsmsp.com/products/n-central.
[104] "Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures", *Cordis.europa.eu*, 2020. [Online]. Available: https://cordis.europa.eu/project/id/832907. [Accessed: 15- Jul- 2020].
[105] "SPEAR Project", *Spear2020.eu*, 2020. [Online]. Available: https://www.spear2020.eu/. [Accessed: 15- Jul- 2020].
[106] "PHOENIX - H2020", 2020. [Online]. Available: https://phoenix-h2020.eu/. [Accessed: 15- Jul- 2020].
[107] "Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID", *Sgrid.eu*. [Online]. Available: https://www.sgrid.eu/. [Accessed: 16- Jul- 2020].
[108] "Solutions for intelligent distribution grids - UNITED-GRID", *UNITED-GRID*. [Online]. Available: https://united-grid.eu/. [Accessed: 16- Jul- 2020].
[109] "Home – FORESIGHT project", *FORESIGHT*, 2020. [Online]. Available: https://foresight-h2020.eu/. [Accessed: 16- Jul- 2020].
[110] Introduction to the IEC 60870-5-104 standard - ENSOTEST - 2019", *ENSOTEST*. [Online]. Available: https://www.ensotest.com/iec-60870-5-104/introduction-to-the-iec-60870-5-104-standard/. [Accessed: 27- Jul- 2020].
[111] R. Mackiewicz, "Overview of IEC 61850 and benefits", *2006 IEEE Power Engineering Society General Meeting*, 2006. Available: 10.1109/pes.2006.1709546.