VPP4ISLANDS

Virtual Power Plant for Interoperable and Smart isLANDS

VPP4Islands

LC-SC3-ES-4-2020

GA 957852

Deliverable Report

Deliverable ID	D5.1	**Version**	1.0
Deliverable name	VPP Risk assessment		
Lead beneficiary	BC2050		
Contributors	All		
Reviewer	BUL, INAVITAS		
Due date	30/9/2021		
Date of final version	30/9/2021		
Dissemination level	Public		
Document approval	Seifeddine BEN ELGHALI	**Date**	30/9/21

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Acknowledgement: VPP4ISLANDS is a Horizon 2020 project funded by the European Commission under Grant Agreement no. 957852.

REVISION AND HISTORY CHART

Version	Date	Main Author(s)	Summary of changes
v0.1	24/3/2021	BC2050	Document creation
v0.2	22/7/2021	BC2050	Added Methodology information
v0.3	1/9/2021	BC2050	Consolidation of questionnaires
v0.4	27/9/2021	BC2050	Review version
v0.5	29/9/2021	BUL	Peer reviewed version
v1.0	30/9/2021	BC2050	Release version

Authors: Konstantinos Tsiomos
Entrit Metai
Dr. Ioannis Dontas
Peter Tjia
Dr. Nikos Bogonikolos

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

TABLE OF CONTENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

LIST OF FIGURES

LIST OF TABLES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ALPHABETICAL LISTS OF ABBREVIATIONS AND ACRONYMS

PARTNERS

Abbreviation	Meaning
ALWA	AlgoWatt
AMU	Aix-Marseille Université
BC2050	Blockchain2050
BornholmsVarme	Bornholms Varme A/S
BoZI	Bozcaada Belediye Baskanligi
BUL	Brunel University London
CIVI	CIVIESCO srl
CSIC	Consejo Superior de Investigaciones Científicas
CU	Cardiff University
DAFNI	Network of Sustainable Greek Islands
FORM	Consell Insular de Formentera
FTK	FTK Forschungsinstitut fur Telekommunikation und Kooperation EV
GRADO	Comune di Grado
IDEA	Ingenieria Y Diseno Estructural Avanzado
INAVITAS	INAVITAS Enerji AS
LIS	Laboratoire Informatique des Systèmes
PVM	Protisvalor Méditerranée
RDIUP	RDI'UP
REGENERA	REGENERA LEVANTE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

SCHN	Schneider Electric
TROYA	TROYA CEVRE DERNEGI
UEDAS	Uludag Electric Dagitim

TERMS

Abbreviation	Meaning
AAI	Authentication and Authorization Infrastructure
BSP	Balancing Service Provision
Dapp	Decentralized Application
DeFi	Decentralized Finance
DER	Distributed Energy Resources
DT	Digital Twin
DLT	Digital Ledger Technologies
DSO	Distribution System Operator
EMS	Energy Management Systems
GHG	Greenhouse gases
ISMS	Information Security Management System
LCOE	Levelised Cost of Energy
MSD	Market Systems Development
PoS	Proof of Stake
PoW	Proof of Work

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

PV	Photovoltaic
RES	Renewable Energy Sources
RTU	Remote Terminal Unit
SoA	Statement of Applicability
TSO	Transmission System Operator
VESS	Virtual Energy Storage Systems
VPP	Virtual Power Plant
VU	Virtual Units

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

1. Executive Summary

Risk Management is of great importance for Information Security. This document's intention is to facilitate the assessment and management of incidents that could endanger the project's informational infrastructure as well as incidents that could potentially cause harm to the data stored within, especially those of sensitive nature. Moreover, it aims to provide effective measures that will counteract any anticipated damage before it occurs, or at least reduce to a minimum any harmful effects.

Overall, the methodology that will be followed herein consists of a feedback algorithmic process that identifies potential threats, then analyses, evaluates and prioritizes them based on criticality. Subsequently it proposes measures to all relevant stakeholders in order to proceed with the proper actions to address them. An asset-based approach will be followed to better safeguard each informational asset of the project. The expected outcomes are accurate and effective controls against risks that may arise at any time during the system's operation.

An in-depth risk assessment with the individual VPP stakeholders will be performed twice, measures will be proposed on both occasions and until the risk owners accept the remaining risks.

These risks and measures will be fed into the requirements engineering of WP2, WP3, WP4, WP5, and WP6. The assessment activities will be aligned with the validation activities defined in WP7.

The current document is a live document, and this is its first iteration (M12). Subsequent iterations (M24, M36 and M42) will provide additional data, more identified risks, and re-evaluation of threats.

The final outputs of this documents (M42) will be based and in accordance with ISO 31000/2018. [1]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

1. INTRODUCTION

1.1. ABOUT VPP4ISLANDS PROJECT

Under the Horizon2020 framework, the submitted proposal "**VPP4Islands**" was evaluated positively by the EU Commission and on October 1st, 2020 the 42 months project commenced. VPP4Islands goal is to accelerate the transition towards smart and green energy by facilitating the integration of Renewable Energy Systems (RES) in island areas. It also aims to help islands exploit energy efficiency potential and innovative storage approaches, foster the active participation of citizens and become self-sufficient in energy. All these, while reducing costs, greenhouse gas (GHG) emissions and reliance on fossil fuels to generate power. Another goal is to also create new intelligent business, growth and local skilled jobs.

For the realization of the above, VPP4Islands project proposes disruptive solutions based on Digital Twin (DT) concept, Virtual Energy Storage Systems (VESS) and Distributed Ledger Technology (DLT) to revolutionize the existing VPP and build smart energy communities.

Based on aggregation and smart management of Distributed Energy Resources (DERs), VPP4Islands will increase the flexibility and profitability of energy systems while providing novel services. VPP4Island will also enhance the Demand Response Capability of consumers by understating their behaviors and promoting self-consumption.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

1.2. About Risk

Although the term "**risk**" is rendered in various ways, all of them seem to revolve around a common meaning. In general, "risk" refers to the possibility of an unfortunate occurrence that will eventually lead to an unwanted result. Risk involves uncertainty about the effects and/or implications of an activity with respect to something of value (such as health, well-being, environment, wealth, property, or other assets), often focusing on negative, undesirable consequences.

"**Project Risk**" is defined as "an uncertain event or condition that, if it occurs, it may bring a negative effect on a project's objectives, if not addressed effectively". [2]

"**Risk Assessment**" is a procedure that determines potential mishaps, their likelihood and consequences, as well as the tolerances for such events. The results of this process may be expressed in a quantitative or qualitative fashion. Risk Assessment is an inherent part of a broader risk management strategy to help reduce any potential risk-related consequences. [3]

"**Risk Management**" is the identification, evaluation, and prioritization of risks (as the effect of uncertainty on the objectives) followed by coordinated application of appropriate measures, that may include the investment of resources, to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities. [4]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

2. METHODOLOGY SUMMARY

All projects assume some degree of uncertainty. Risk management helps minimizing the potential adverse impact that such uncertainty may have on the project outcomes by avoiding crisis and by improving problem-solving during the course of the project. Risks are inherent to project development, and they can lead to problems and delays if not properly managed.

Following the completion of a project, and once the outcomes become operational, risks are still lurking, ready to jeopardize the seamless operation. To that end, another risk assessment study should be completed that will direct all necessary actions for risk management during operation. Systems that include and handle information, especially in digital form, are prone to human mistakes, and malicious acts, either deliberate or not.

The goal of each risk assessment methodology is to identify all possible risks and establish a course of action for each potential threat, seeking either its complete avoidance, its mitigation, or a close monitoring, depending on the risk priority, during any time of system's operation.

This Risk Assessment and Management Plan will take on an asset-based approach, meaning that risk identification and evaluation will be performed per each unique information element of the project. Information elements consist of hard copies, electronic information, stationery devices, portable devices, removeable media and other intangible information. The reasons for choosing an asset-based approach is because it is more precise compared to other approaches since it focuses on each specific element that contains potentially endangered information, and more shift actions may be taken in order to counter any threats that arise and restore the system to its seamless operation as soon as possible.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Ultimately, at the final version of this document (M42) a formal risk management methodology will be introduced, that will identify all potential risks and to guarantee the successful operation, with minimal impacts in cases of threat occurrences.

The process includes five stages, that constantly monitor the arisen risk, analyse it, evaluate it, prioritize it versus other that may occur at the same time, handling it and start anew as many times as required, based of measures' outcomes, and until the threat is effectively dealt with.

For the first version of this document (M12) a questionnaire was distributed among partners, to be filled with preliminary identified risks that may show up during the operation of the system. The questionnaire is available in Annex A of this document while the filled ones, as received by the partners who responded are included in Annex B.

Figure 2.1: Risk monitoring iterative process

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

2.1. Risk Identification

At this stage of the Risk Management process, team members identify and document potential risks together with their possible consequences. Risk identification is an iterative process which is performed along the entire project life cycle.

2.2. Risk Analysis

Each risk will be documented in terms of likelihood of occurrence and potential impact on system's operation. According to ISO 31000/2018 [1], risk avoidance measures or mitigation plans are proposed by VPP4Islands consortium and agreed by the PO.

- Probability/Likelihood: how likely is this risk to happen?
- Impact: what would be the effects on the system should the risk materialize?
- Asset importance: how valuable is the asset for the seamless operation of the system

2.3. Risk Evaluation and Prioritisation

Once the probability and impact of each risk have been assessed, VPP4Islands stakeholders will follow the standard procedure described below:

1. Risk evaluation to identify and decide which actions ought to be taken.
2. Risk prioritisation to know where to focus. These decisions are made based on a probability and impact matrix.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

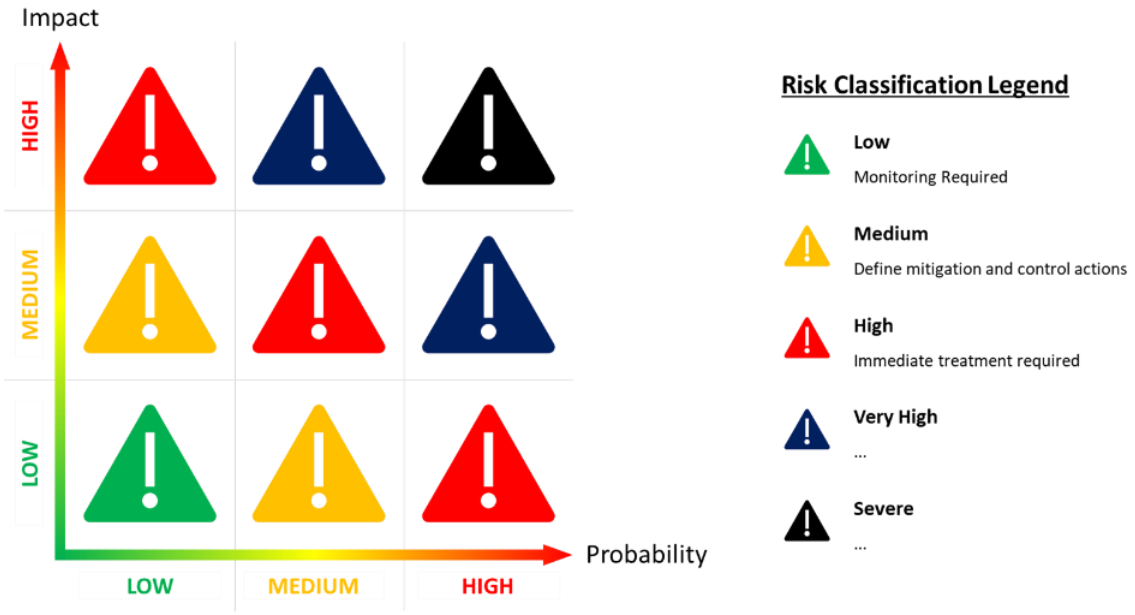

Figure 2.2: 5-level risk classification

2.4. RISK HANDLING

Once the stakeholders know which risks are to be dealt with and which need only to be monitored, mitigation plans are established for each one, knowing that one risk may have more than one action associated to mitigate its impact and/or reduce its likelihood. Such plans include, but are not limited to:

- Actions to be implemented
- Identification and assignment of responsibility
- Risk status
- Planning
- Effort

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

2.5. FEEDBACK AND REVISION

Risks are dynamic and rarely remain stable along the project life cycle, therefore permanent monitoring is needed to:

- Detect, analyse, and treat new risks.
- Check effectiveness of actions already taken to mitigate existing risks to make sure these actions have a positive effect, otherwise they are reviewed, and complementary measures are taken.
- Identify and assess secondary and residual risks.

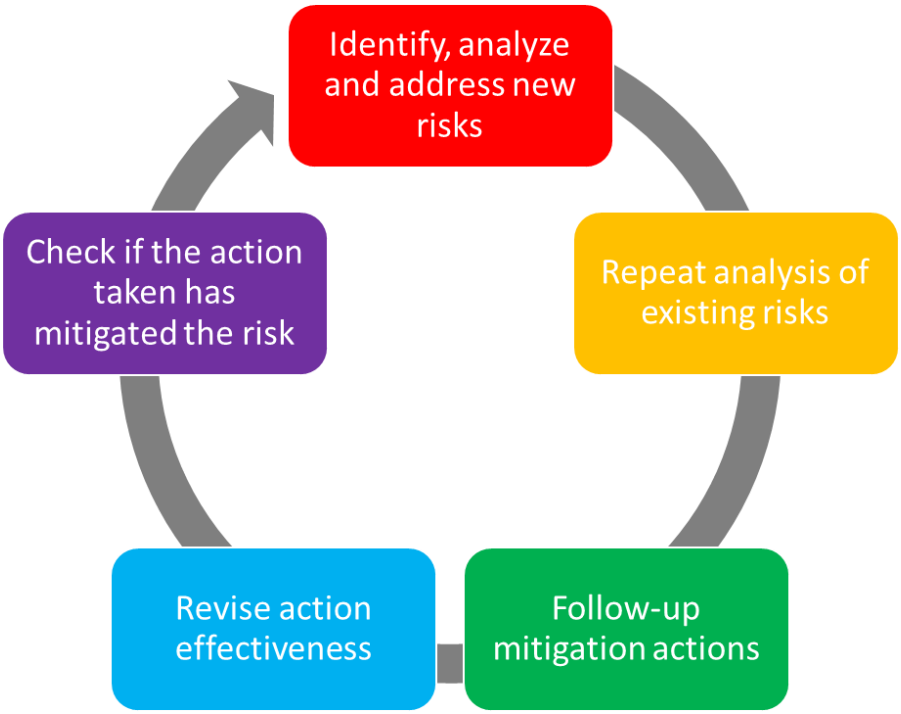

Figure 2.3: Iterative process for controls' optimization

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. RISK IDENTIFICATION PER INFORMATION ASSET TYPE

Risk identification is an iterative process which is performed along the entire project life cycle. This paragraph lists all identified threats per information asset type, as those where pinpointed by the VPP4Islands partners, at this stage of the project's development (M12). Each sub-section is dedicated to a specific information asset type (hard copies, electronic information, stationery devices, portable devices, removeable media and other intangible information) and consists of a consolidating table with the asset type's name, the name and a short description of a potential risk, potential consequences of that risk and the partner associated with the corresponding identification.

More specifically:

- hard copies refer to documents in physical form, both original or copies of them, on a variety of materials such as paper, carton, plastic, etc.;
- electronic information refers to any information in digital form;
- stationery devices refer to desktop computers, smart meters, VPPBoxes/Nodes, photovoltaic panels and any other equipment of the project that is assigned to one specific place and requires relative effort to move it away from it;
- portable devices refer to laptops, tablets, mobile phone and any other equipment of the project that requires no effort to move it away from it;
- removeable media refer to portable devices that can store digital information such as external hard disks, USB flash drives, etc.;
- intangible information refers to information such as intellectual property, historical information, etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3.1. ELECTRONIC INFORMATION

Table 3.1: Risk Identification for Electronic Information Assets

Electronic Information name	Risk name / description	Potential consequences	Associated partner or stakeholder
Forecasting data	Failure to receive correct data (from a human/algorithm to software platform): The correct information about some input parameters for prediction are not received by the prediction module.	The optimization engine uses wrong and invalid predictions. Hence, the produced set points will be erroneous.	AMU
Data on VPP members and physical assets	Unauthorized third-party access: An unauthorised third party gains access to information on the system.	Failure of the system due to erroneous control signals produced by VPP.	AMU
		Unauthorised circulation of personal data on members or technical data on installations	ALWA
Baseline	Failure to receive baseline (from human/algorithm to software platform): Software platform does not receive the baseline of some or all aggregate components.	Abnormal operation or non-functioning in the flexibility dispatching process.	ALWA
Measurements' data	Failure to receive measures: Software platform does not receive real-time field measurements. Abnormal operation or non-functioning in the flexibility dispatching process.	Errors in the whole VPP system.	AMU
		Corrupt or unavailable measurements do not allow to: Observ and control physical assets.	ALWA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

		Quantify the flexibility (for SP-BSP) or self-consumed energy (for SP-CE).	
Price Data	Failure to receive price data (from a human/algorithm to software platform): The selling price of the flexibility of one or more physical assets are not received by the software platform.	The physical assets that do not make available data on sales prices will not be able to take part in the flexibility dispatching process.	ALWA
Control signals	Failure to send control signals (from software platform to power plants, ESS, etc.): The software platform loses the ability to remotely control production and/or consumption of power units, flexible loads and ESS in the field.	Production and/or consumption units will not be able to participate in the balancing market.	AMU
			ALWA
Reports on remunerations	Unauthorized third-party access: An unauthorised third party gains access to information on the system.	Unauthorised circulation of personal data on members or technical data on installations.	ALWA
Computational models	Leakage/theft of data/information: Intentional human intervention, resulting in break into system and/or premises and access confidential/critical information.	Threaten exploitation success of VPP energy solution. Loss of intellectual property.	BUL
	Loss of system design data/information: - Introduction of weaknesses into the systems during routine maintenance. - Premises will suffer an electrical outage, which could knock servers offline and stop employees from working, unable to access sensitive information for hours or even days	Compromised operation of the VPP4ISLANDS energy solution	BUL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

	- Digital files are corrupted and/or are rendered unavailable		
Design information	Leakage/theft of data/information: Intentional human intervention, resulting in break into system and/or premises and access confidential/critical information.	Threaten exploitation success of VPP energy solution. Loss of intellectual property.	BUL
	Loss of system design data/information: - Introduction of weaknesses into the systems during routine maintenance. - Premises will suffer an electrical outage, which could knock servers offline and stop employees from working, unable to access sensitive information for hours or even days - Digital files are corrupted and/or are rendered unavailable	Compromised operation of the VPP4ISLANDS energy solution	BUL
Operational information	Leakage/theft of data/information: Intentional human intervention, resulting in break into system and/or premises and access confidential/critical information.	Threaten exploitation success of VPP energy solution. Loss of intellectual property.	BUL
	Loss of system design data/information: - Introduction of weaknesses into the systems during routine maintenance. - Premises will suffer an electrical outage, which could knock servers offline and stop employees from working,	Compromised operation of the VPP4ISLANDS energy solution	BUL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

	unable to access sensitive information for hours or even days - Digital files are corrupted and/or are rendered unavailable		
Technology characteristics (for components of VESS)	Unauthorized access: An unauthorized person may gain access to essential information on the VPP4IBox	Information integrity compromised, potential impact on the performance of the VESS.	CU
Measurements (for VESS)	Damaged or manipulated measurements: Control schemes of the VESS receive compromised measurements.	Incorrect or misleading control actions are given to the VESS components, which leads to revenues cut and system reliability degradation.	CU
Control signals (for VESS)	Damaged or manipulated Control signals: Components of the VESS receive a modified or damaged control signals.	Inaccurate services provision by the VESS components, which leads to revenues cut and system reliability degradation.	CU
Smart Planning Tool (SPT))	Lack of meaningful data: Difficulty to collect enough data from the demos and the generation of poor information. Thus, will affect the robustness of the MLs and the decision making.	Difficulties to generate replication plans.	RDIUP
Remote Terminal Unit (RTU)	RTU misuse/data tampering: A malicious user is able to tamper with the RTU or to supplant another device connecting to the RTU, and is able to successfully sending erroneous data to the RTU.	Decisions resulting on the analysis of misleading information could lead to issues on the grid or to an underperformance of the provided services.	SCHN

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Gökçeada WPP1 and WPP2 Data	Intentional or unintentional human intervention: Energy production data can be used for pricing policy and commercial benefits. It is also important for reactive energy control service. The data in this context is not made available to third parties.	No major problems expected	UEDAS
Gökçeada SPP1 Data	Intentional or unintentional human intervention: Energy production data can be used for pricing policy and commercial benefits. It is also important for reactive energy control service. The data in this context is not made available to third parties.	No major problems expected	UEDAS
Gökçeada ESS1 Data	Intentional or unintentional human intervention: The load values of the energy storage system may be important if it can be used for a commercial purpose. As there are emerging technologies, it is possible for manufacturers for development purposes to need energy charge-discharge data.	No major problems expected	UEDAS
Gökçeada Feeder	Intentional or unintentional human intervention.	No major problems expected	UEDAS
Gökçeada GIS Island1 Map	Malicious acts		UEDAS
Gökçeada Customer list	May pose a target by companies seeking commercial benefits.		UEDAS
Gökçeada Consumer data	May pose a target by companies seeking commercial benefits		UEDAS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3.2. STATIONERY DEVICES

Table 3.2: Risk Identification for Stationery Device Assets

Stationary Device name	Risk name / description	Potential consequences	Associated partner or stakeholder
Rooftop PV	Loss of data by system failure or hacking.	Blindness to function and operation.	Bornholms Varme
Electric boilers	Loss of data by system failure or hacking.	Electric boilers are not operable.	Bornholms Varme
Smart Meters at consumers	Loss of data by system failure or hacking.	Data are not available.	Bornholms Varme
Danfoss computers at selected consumers.	Loss of data	Computers at consumers are not available for flexibility experiments.	Bornholms Varme

3.3. INTANGIBLE INFORMATION

Table 3.3: Risk Identification for Intangible Information Assets

Intangible Information name	Risk name / description	Potential consequences	Associated partner or stakeholder
Historical consumption data	Problems in obtaining data: Historical consumption data may be protected, and permissions may have to be requested or more smart meters may have to be installed to get them than defined in the proposal.	Longer implementation time and increased budget.	REGE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

4. Risk Analysis per information asset type

Via the distributed questionnaires, partners were kindly asked to evaluate a potentially affected asset 's importance, the likelihood of a threatening risk to happen for that asset and the impact severeness of said risk. Each of these three, are valued on a scale from 0 to 10.

The following tables are based on those partners feedback, and include the provided score, along with the stakeholder that is responsible to deal with the risk and prevent its consequences.

Each risk will be documented in terms of likelihood of occurrence and potential impact on system's operation. Risk avoidance measures or mitigation plans will be proposed by VPP4Islands consortium and agreed by the PO.

4.1. Electronic Files

Table 4.1: Risk Analysis for Electronic Information Assets

Information asset name	Risk name / description	Asset's importance	Likelihood	Impact severeness	Mitigating stakeholder
Forecasting data	Failure to receive correct data (from a human/algorithm to software platform): The correct information about some input parameters for prediction are not received by the prediction module.	6	6	10	-
Data on VPP members and physical assets	Unauthorized third-party access: An unauthorised third party gains access to information on the system.	6	6	5	All members who hold system passwords

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Baseline	Failure to receive baseline (from human/algorithm to software platform): Software platform does not receive the baseline of some or all aggregate components.	8	6	10	-
Measurements' data	Failure to receive measures: Software platform does not receive real-time field measurements. Abnormal operation or non-functioning in the flexibility dispatching process.	9	6	10	RTU's developer Telecommunications system
Price Data	Failure to receive price data (from a human/algorithm to software platform): The selling price of the flexibility of one or more physical assets are not received by the software platform.	6	6	10	-
Control signals	Failure to send control signals (from software platform to power plants, ESS, etc.): The software platform loses the ability to remotely control production and/or consumption of power units, flexible loads and ESS in the field.	9	6	10	-
Reports on remunerations	Unauthorized third-party access: An unauthorised third party gains access to information on the system.	8	6	5	All members who hold system passwords

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Computational models	Leakage/theft of data/information: Intentional human intervention, resulting in break into system and/or premises and access confidential/critical information.	10	2-3	6-7	BUL DPO and/or Cyber & Information Security Manager
	Loss of system design data/information: - Introduction of weaknesses into the systems during routine maintenance. - Premises will suffer an electrical outage, which could knock servers offline and stop employees from working, unable to access sensitive information for hours or even days Digital files are corrupted and/or are rendered unavailable	10	2-3	6-7	BUL DPO and/or Cyber & Information Security Manager
Design information	Leakage/theft of data/information: Intentional human intervention, resulting in break into system and/or premises and access confidential/critical information.	10	2-3	6-7	BUL DPO and/or Cyber & Information Security Manager
	Loss of system design data/information:	10	2-3	6-7	BUL DPO and/or Cyber & Information Security Manager

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

	- Introduction of weaknesses into the systems during routine maintenance. - Premises will suffer an electrical outage, which could knock servers offline and stop employees from working, unable to access sensitive information for hours or even days Digital files are corrupted and/or are rendered unavailable				
Operational information	Leakage/theft of data/information: Intentional human intervention, resulting in break into system and/or premises and access confidential/critical information.	10	2-3	6-7	BUL DPO and/or Cyber & Information Security Manager
	Loss of system design data/information: - Introduction of weaknesses into the systems during routine maintenance. - Premises will suffer an electrical outage, which could knock servers offline and stop employees from	10	2-3	6-7	BUL DPO and/or Cyber & Information Security Manager

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

	working, unable to access sensitive information for hours or even days Digital files are corrupted and/or are rendered unavailable				
Technology characteristics (for components of VESS)	Unauthorized access: An unauthorized person may gain access to essential information on the VPP4IBox	6	5	5	VESS aggregator
Measurements (for VESS)	Damaged or manipulated measurements: Control schemes of the VESS receive compromised measurements.	7	6	8	Sending devices and communications system operators
Control signals (for VESS)	Damaged or manipulated Control signals: Components of the VESS receive a modified or damaged control signals.	8	6	9	VESS aggregator or communication system operator
Smart Planning Tool (SPT))	Lack of meaningful data: Difficulty to collect enough data from the demos and the generation of poor information. Thus, will affect the robustness of the MLs and the decision making.	8	5	8	RDIUP, Leading & follower islands
Remote Terminal Unit (RTU)	RTU misuse/data tampering: A malicious user is able to tamper with the RTU or to supplant another device connecting to the RTU,and is	7	6	9	Operator / IT Security department

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

	able to successfully sending erroneous data to the RTU.				
Gökçeada WPP1 and WPP2 Data	Intentional or unintentional human intervention: Energy production data can be used for pricing policy and commercial benefits. It is also important for reactive energy control service. The data in this context is not made available to third parties.	8	5	6	Security policies stakeholder
Gökçeada SPP1 Data	Intentional or unintentional human intervention: Energy production data can be used for pricing policy and commercial benefits. It is also important for reactive energy control service. The data in this context is not made available to third parties.	8	7	6	Security policies stakeholder
Gökçeada ESS1 Data	Intentional or unintentional human intervention: The load values of the energy storage system may be important if it can be used for a commercial purpose. As there are emerging technologies, it is possible for manufacturers for development purposes to need energy charge-discharge data.	4	8	3	Security policies stakeholder
Gökçeada Feeder	Intentional or unintentional human intervention.	2	4	2	Security policies stakeholder

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Gökçeada GIS Island1 Map	Malicious acts	8	6	8	Security policies stakeholder
Gökçeada Customer list	May pose a target by companies seeking commercial benefits.	8	4	4	Security policies stakeholder
Gökçeada Consumer data	May pose a target by companies seeking commercial benefits	8	4	4	Security policies stakeholder

4.2. STATIONERY DEVICES

Table 4.2: Risk Analysis for Stationery Device Assets

Stationery Device type / name	**Risk name / description**	**Asset's importance**	**Likelihood**	**Impact severeness**	**Mitigating stakeholder**
Rooftop PV	Loss of data by system failure or hacking.	1	1	0	Asset's owner
Electric boilers	Loss of data by system failure or hacking.	3	1	2	Asset's owner
Smart Meters at consumers	Loss of data by system failure or hacking.	9	1	1	Asset's owner
Danfoss computers at selected consumers.	Loss of data	1	1	1	Bornholms Varme A/S

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

4.3. INTANGIBLE INFORMATION

Table 4.3: Risk Analysis for Intangible Information Assets

Intangible Information type	Risk name / description	Asset's importance	Likelihood	Impact severeness	Mitigating stakeholder
Historical consumption data	Problems in obtaining data: Historical consumption data may be protected, and permissions may have to be requested or more smart meters may have to be installed to get them than defined in the proposal.	9	6	8	Leading / following island

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

5. Risk Evaluation and Prioritization

5.1. Risk Evaluation

Once all risks have been identified and catalogued, they will be evaluated on how each one will be dealt with. Mitigating stakeholders responsible for dealing with the risks will be defined, as well as their roles in cases where more than one is assigned for a risk. Countermeasures and courses of action will be also defined for each one involved mitigating stakeholder.

Once all risks have been identified and catalogued, they will be evaluated on how each one will be dealt with. Mitigating stakeholders responsible for dealing with the risks will be defined, as well as their roles in cases where more than one is assigned for a risk. Countermeasures and courses of action will be also defined for each one involved mitigating stakeholder.

Risk evaluation may also hold additional information. Such information may add more insights about the identity of a risk in question. For example:

- **Residual Risk:** Risk treatments do not necessarily reduce risks to zero. Remaining risk after treatment is known as residual risk.
- **Secondary Risk:** It is common for one's efforts to reduce risk to have risks of their own. These are called secondary risks.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

5.2. RISK PRIORITIZATION

Once all risks have been identified, catalogued, and evaluated, they will be prioritized based on five quantified levels of criticality: low, medium, high, very high and severe. These levels could act as flags of importance in cases where a multi-hazard incident occurs.

Prioritization on same level risks will be decided based on criticality score, that will derive from the final values of asset importance, risk likelihood, and impact severeness. Risk prioritization will facilitate mitigating stakeholders on where to focus. These decisions will be based on a probability and impact matrix.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

6. Risk Reporting

Risk reporting will be a process that will be defined during the last revision of the document (M42). It consists of different actions that apply to system safety and security monitoring both while a threatening incident occurs or not. The first refers to the ongoing procedure of status reporting on the developments of dealing with a risk while the latter refers to procedures of active monitoring and scouting for potential incoming threats (such as hailstorms that can damage the solar panels).

For each case, different risk reporting plans might be introduced, as for example interval-reporting for risks with prolonged duration.

6.1. Risk Treatment Plan

The risk treatment plan will include a summary of each of the identified risks, as well as the treatments that have been produced for each individual risk, the stakeholders in charge of mitigating those risks, and the deadlines for applying the corresponding treatments.

A risk treatment is an action that is taken to manage a risk. Identifying, assessing, and treating risks are all steps in the risk management process. There are five methods of risk treatment in general.

1. **Avoidance:** Deciding not to take on the risk by avoiding the actions that cause the risk.
2. **Reduction:** Deciding to take mitigation actions that reduce the risk.
3. **Transfer:** Deciding to transfer all or part of the risk to a third party. The two main types of transfer are insurance and outsourcing.
4. **Acceptance:** Deciding to accept the risk. Also known as risk retention, is choosing to face a risk.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

5. **Sharing:** Deciding to share the risk. This refers to the distribution of risk to multiple entities. This is done for a variety of reasons including insurance products and self-insurance strategies.

6.2. STATEMENTS OF APPLICABILITY

Within the VPP4Islands framework, the Statement of Applicability (SoA) will serve as the primary link between risk assessment and risk treatment for all stakeholders. SoA is a regularly updated and managed document that offers an overview of information security implementation and is a crucial prerequisite for Information Security Management System (ISMS) implementations. A concise chart of controls will be prepared as the SoA for the purposes of this document

Written policies, procedures, and work instructions are required to implement the ISMS. Most information security gaps can be filled by adhering to these policies and methods. To do so, one must first determine why and how the ISMS is being implemented. The goal of information security is to preserve the confidentiality, integrity, and availability of information (CIA).

An ISMS is a risk-based strategy to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security. As a result of risk analysis, an ISMS can be deployed to eradicate or decrease risk to an acceptable level. The preservation of CIA information is the foundation of information security:

- **Confidentiality:** Ensures information accessibility only to authorized staff
- **Integrity:** Ensures information accuracy, verifying that it is complete and not modified without authorization
- **Availability:** Ensures information accessibility to authorized users when required

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

The SoA will serve as a checklist for implementing ISMS in VPP4Islands, ensuring that no controls are overlooked.

The SoA controls will identify all applicable regulatory and technical requirements, as well as obligations and controls connected to the system's requirements. The SoA will be one-of-a-kind and pertinent to the system.

An information security risk assessment with mapped risk acceptance criteria is the first stage in creating a SoA. The loss of Confidentiality, Integrity, and Availability of information is linked to the risk assessment process, which must include

- People
- Software
- Hardware
- Data and databases
- Information
- History of attacks
- Previous audits
- Current and planned controls to decrease risk
- External vulnerability, assessment and penetration test (VA/PT) exercises
- Subject matter experts
- Procedures or work instructions to which staff must adhere

Each risk must be recognized and analysed in order to identify risk levels, appraised for relevance, recorded, and reviewed. After the SoA document is finalized, real-world risk treatment processes will begin. The risk treatment will determine whether the mitigating stakeholder accepts, avoids, decreases,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

shares the source of, changes the likelihood of, or alters the consequence of each risk found in the risk assessment.

Information security auditors will walk through the ISMS process controls using the SoA as the core document. All management and staff must be aware of every control contained in the SoA. Any participating stakeholder will be able to understand the information security controls in the SoA.

6.3. REPORT DOCUMENT TEMPLATE

To be defined during the last stages of this report (M36 or M42).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

7. CONCLUSIONS

The first version of this live document was compiled to primarily reflect its purpose, in a way that is understandable and comprehensible to the other partners.

At the same time, with the contribution of the partners, an initial material was collected related to possible risks that are likely to occur in the system when it is put into operation. The aim for this material was to serve as a basis for setting up this first version of the document, as well as all subsequent ones. In addition, it constitutes a guide for future additions regarding risks that will be recognized in the future during the development of the project.

The incoming material can be characterized as relatively sufficient in quantity but currently does not have the expected variety. As lesson learned, future requests for material concerning this document will further detailed.

As expected, a significant percentage of the volume was focused on electronic information. Potential risks to other information assets, such as hard copies, portable devices, and removable media, did not appear to be identified at this point. However, this was relatively expected as the project runs its 12th month its implementation, out of a total of 42, and many relevant parameters have not yet been determined.

Last, but not least it is important to clarify that in the final version of this report, which will be delivered on M42 of the project, more concrete information and further conclusions will be provided across the entirety of the document, concerning the risk assessment and management of the final product once it is set into operation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ANNEX A: DISTRIBUTED QUESTIONNAIRE

Questionnaire for information security Risk Assessment and Management plan

VPP4ISLANDS project aims to facilitate and revolutionize the integration of RES in existing power distribution networks through the implementation of innovative technologies and procedures, offering disruptive solutions based on the Digital Twin concept, Virtual Energy Storage Systems and Distributed Ledger Technologies, such as Blockchain per se.

For this purpose, many different partners and stakeholders will cooperate to realize and put in motion the VPP. Through this multidisciplinary collaboration, large volumes of information will be created, shared, and managed, several of which are characterized as sensitive.

Thus, it becomes of imperative nature to setup and deploy a robust Risk Assessment and Management plan for information security that will address effectively and in a timely manner all potential threats that may arise and could jeopardize any of the system's information, regardless of nature or criticality.

To that end, an asset-based approach questionnaire was formed in order to document as many of the expected of likely risks that can been foreseen at this point of the **VPP4ISLANDS** project progress stage and it is distributed herein, for all partners and involved stakeholders to fill.

- The first part of the Questionnaire requires a few basic information from your part.
- The second part consists of 10 questions which give space for elaborating as much as deemed necessary. Please refrain from answering in a tersely manner and feel encouraged to provide all critical information you can share.
- In the third and last part, we provide a table in which we kindly ask you to fill with relevant

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

information for each foreseen risk you identify regarding information security. Although you will find two copies of the relevant table, you can replicate it as many times as you see fit and as circumstances dictate, in order to list all the risks in question.

The questions that follow, aim to create the maximum possible knowledgebase of potential risks which will be used to enrich the ***Deliverable 5.1: Risk Assessment and Management Plan***.

Please make sure to read through the whole document before filling it with information and try to keep information in context throughout all tables.

Thank you in advance for providing your feedback and for the time you spent in filling this questionnaire.

If required, we will contact personally and individually with whomever necessary in order to obtain clarification on the contents of the filled questionnaire.

Please respect the deadline for the completion of the questionnaire (Friday, 20 August 2021).

We are always at your disposal for any additional information and clarification you might need.

The Blockchain2050 team

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ID information

1. **Full name:** _
2. **E-mail address:** _
3. **Organization:** _
4. **Role in the project:** *(please click here to choose one from the list)*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. **Please describe in detail your involvement and function in the project?**

   _

2. **What information assets fall within your area of involvement?**

   _

3. **Where are these assets located?**

   _

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

–

5. **Which of these assets deal with critical information?**

–

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

–

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

–

8. **What cascading effects may take place if an information asset of yours is affected?**

–

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

–

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

–

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

How to fill the table

For each of the fields below, replace the indicative number with the information requested in the numbered list below.

Each number of the list corresponds to the relevant field that should be filled. All fields are required to be filled.

Although two tables are provided herein, feel free to replicate them as many times as you deem necessary, in order to provide information for all possible/expected risks that you have identified towards one or more information assets which fall within your involvement with the project.

1. In the "***Information asset name***" field, please provide a name for the asset in question. If possible, please try to maintain uniqueness between assets.
2. In the "***Asset importance***" field, please fill in a number between **0 to 10**, with 10 describing the highest importance. Please grade objectively.
3. In the "***Information asset type***" field, please state between *Hard copies, Electronic Files, Stationary Device(s), Portable Device(s), Intangible Information*. Intellectual property is an example of the latter. In case you identify another information asset type, that does not fall under the aforementioned categories, please write "***Other:***" and the type of said asset.
4. In the "***GDPR sensitive***" field, please write **YES** in case the information involved are GDPR sensitive. Otherwise, fill **NO**.
5. In the "**Owning *Stakeholder***" field, please fill in the name of the stakeholder that owns/handles the asset in question.
6. In the "***Stakeholder Type***" field, please state between *Conventional Power Plant, Solar-power Power Plant, Win-power Power Plant, ESS, VESS, Utility Grid, DSO, TSO, Meteorological Data Provider, Consumers, or Prosumers*. In case you identify another stakeholder type, that does not fall under the aforementioned categories, please write "***Other:***" and the type of said stakeholder.
7. In the "***Identified risk***" field, please write a name for the potential information security related risk you have identified.
8. In the "***Likelihood***" field, please fill in a number between **0 to 10**, with 10 describing the highest probability of occurrence. Please grade objectively.
9. In the "***Risk's origin***" field, please state the potential point(s) of origin of the risk in question. Such cases may be *natural disasters, intentional or unintentional human intervention, malicious acts*, etc.
10. In the "***Impact severeness***" field, please fill in a number between **0 to 10**, with 10 referring to a scenario with the most negative consequences. Please grade objectively.
11. In the "***Risk description***" field, please write a short description of the potential information security related risk

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

you have identified.

12. In the "***Expected consequences***" field, please describe the expected repercussions in case the threat successfully affects the system.
13. In the "***Mitigating stakeholder***" field, please note the partner or stakeholder which will be responsible to deal with the threatening incident, by taking proper actions.
14. In the "***Solution / mitigation actions***" field, please describe, even in the form of suggestion, the suitable actions that need to be taken in order for the mitigating stakeholder to deal effectively with the risk in question. In case you advise to let the incident unfold or ignore it completely, please provide the reasoning behind such action.

Information asset name	1	**Asset importance**	2
Information asset type	3	**GDPR sensitive**	4
Owning Stakeholder	5	**Stakeholder type**	6
Identified risk	7	**Likelihood**	8
Risk's origin	9	**Impact severeness**	10
Risk description	11		
Expected consequences	12		
Mitigating stakeholder	13		
Solution / mitigation actions	14		

Information asset name	1	**Asset importance**	2
Information asset type	3	**GDPR sensitive**	4
Owning Stakeholder	5	**Stakeholder type**	6
Identified risk	7	**Likelihood**	8
Risk's origin	9	**Impact severeness**	10
Risk description	11		
Expected consequences	12		
Mitigating stakeholder	13		
Solution / mitigation actions	14		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ANNEX B: PARTNER-FILLED QUESTIONNAIRES FOR M12 ASSESSMENT

1. AIX-MARSEILLE UNIVERSITY [AMU]

ID information

1. **Full name:** Seifeddine BenElghali
2. **E-mail address:** seifeddine.benelghali@lis-lab.fr
3. **Organization:** Aix-Marseille University
4. **Role in the project:** *Other*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. Please describe in detail your involvement and function in the project?

AMU team is responsible for developing the distributed optimization engine and weather forecasting engine.

The optimization engine has two main responsibilities; First, the technical data coming from each VPP4IBox in a configurable scheduled manner is stored in this database with proper time stamps. The data collected from installations is first unified and anonymized to meet the requirements of general data protection rules (GDPR). Then, the anonymized parameters of grid structure corresponding to a specific slot of time is treated as a whole data frame and stored in the database as a Json document with a time stamp. The stored data is managed based on a Rolling Window scheme: When Jason documents aged beyond the configured time limit (e.g., 5 days), the contents of them is transferred to the data warehouse database at the cloud and the node-level document is deleted. This enables deployment of the VPP software on machines with limited disk size. An API gets the data frames from the anonymization module

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

and converts them to corresponding Json files. Note that, in this step the setpoints or technically equivalent control variables of installations over the grid is unknown. Hence, their value in the corresponding Json documents is unknow. These values will be specified by Distributed Optimization Engine.

2. What information assets fall within your area of involvement?

The data collected from installations (including the owners' personal data and technical data) is first unified and anonymized to meet the requirements of general data protection rules (GDPR). Hence, after unification the following information fall in our scope.

1. Data on physical assets which includes:
    a. Technical data on power plants (PPs)
    b. Flexible loads
    c. Fixed Loads
    d. Virtualized Energy Storage Systems (VESS)
    e. Renewable Energy Sources (RES) including wind and photovoltaic farms.
2. Measurements
   Signals and measurements corresponding each asset under the VPP control.
3. Control signals (set pints generated by optimization engine)
4. Forecasted parameters
   These parameters come from weather, market and consumption forecasting modules and are used in optimization engine to produce correct set points.

3. Where are these assets located?

In the Data Base (DB) at VPP4INode level.

4. Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?

The assets are indirectly accessible through provided web APIs. Also, any communication between modules is done through a set of standard communication services which are provided by APIs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

5. **Which of these assets deal with critical information?**
   a. Measurements:
      Corrupted or unavailable measurements do not allow to remotely observe the behavior of psychic assets in the field and to quantify the flexibility
   b. Control signals
      Corrupted or manipulated set point values would not allow the system to work properly.

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**
   To be done.

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**
   The data on the node-level database will be backed up in a tunable period and the backup will be stored in the storage system at the VPP platform. The backup ensures system in saving a safe copy of more recent information.

8. **What cascading effects may take place if an information asset of yours is affected?**
   Any disruption or unauthorized access to the information my cause considerable error in the produced outputs of the distributed optimization engine. Consequently, the operation of whole VPP system my encounter fatal errors.

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**
   1. Measurements/Electronic device failure.
   2. Cyber-attack.
   3. Telecommunications system failure
   As explained in point 8, any failure or error may cause failure of whole control system, so that the recovery of system in such cases may require high operational costs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**
    No additional information at the moment.

Risk information tables

The following tables refer to the SP-BSP, but they can easily be brought back for the SP-CE platform. It is observed that the SP-CE unlike the SP-BSP does not receive price signals from the components in the field. This is because the EC elements are operated to maximize self-consumption of energy and not to profit in the markets.

1 - Data on physical assets

Information asset name	Data on physical assets	Asset importance	6
Information asset type	Electronic files	GDPR sensitive	YES
Owning Stakeholder	VPP asset owners	Stakeholder type	Conventional Power Plant, Solar-power Power Plant, Wind-power Power Plant, VESS, Flexible Loads

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Identified risk	Unauthorized third-party access	Likelihood	6
Risk's origin	Web app access passwords come into the possession of unauthorized third parties.	Impact severeness	5
Risk description	An unauthorized third-party gains access to information on the system.		
Expected consequences	Failure of the system due to erroneous control signals produced by VPP.		
Mitigating stakeholder	Access according to predefined privilege levels.		
Solution / mitigation actions	Setting high security passwords and authority mechanisms.		

2 – Measurements

Information asset name	Measurement's data	Asset importance	9
Information asset type	Electronic files	GDPR sensitive	YES
Owning Stakeholder	power plant manager or consumer	Stakeholder type	Conventional Power Plant, Solar-power Power Plant, Win-power Power Plant, ESS, Flexible

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

			Loads, consumer
Identified risk	Failure to receive measures	Likelihood	6
Risk's origin	Failure of individual measuring device or failure of data telecommunication system.	Impact severeness	10
Risk description	Software platform does not receive real-time field measurements. Abnormal operation or non-functioning in the flexibility dispatching process.		
Expected consequences	Errors in the whole VPP system.		
Mitigating stakeholder	RTU developer Telecommunications system		
Solution / mitigation actions	Adopt highly reliable electronic devices		

3 – Control signals (set points)

Information asset name	Control signals	Asset importance	9
Information asset type	Electronic File	GDPR sensitive	YES
Owning Stakeholder	VPP optimization engine	Stakeholder type	Conventional Power Plant, ESS, Flexible Loads,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Identified risk	Failure to send control signals (from software platform to power plants, ESS, etc.)	Likelihood	6
Risk's origin	Malicious acts such as Cyber-attack or failure of telecommunication system. Intentional or unintentional human intervention.	Impact severeness	10
Risk description	The software platform loses the ability to remotely control production and/or consumption of power units, flexible loads and ESS in the field.		
Expected consequences	Production and/or consumption units will not be able to participate in the balancing market.		
Mitigating stakeholder			
Solution / mitigation actions	Exploiting inter-module security mechanisms, providing a systematic approach for periodical reliability and safety assessment of optimization engine		

4 – Forecasting data

Information asset name	Forecasting data	Asset importance	6
Information asset type	Database files	GDPR sensitive	
Owning Stakeholder	VPP node	Stakeholder type	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Identified risk	Failure to receive correct data (from a human/algorithm to software platform).	Likelihood	6
Risk's origin	Malicious acts such as Cyber-attack or failure of telecommunication system. Intentional or unintentional human intervention	Impact severeness	10
Risk description	The correct information about some input parameters for prediction are not received by the prediction module.		
Expected consequences	The optimization engine uses wrong and invalid predictions. Hence, the produced set points will be erroneous.		
Mitigating stakeholder			
Solution / mitigation actions	Ensuring safety and reliability of the output of the forecasting modules and their communication links.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

2. algoWatt [ALWA]

ID information

1. **Full name:** Diego Piserà
2. **E-mail address:** **diego.pisera@algowatt.com**
3. **Organization:** ALWA - algoWatt
4. **Role in the project:** *Technical Partner: Software*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. Please describe in detail your involvement and function in the project?

Software provider. AlgoWatt will provide a Software Platform for Balancing Services Provider (SP-BSP) and a Software Platform for the management of Energy Communities (SP-CE).

SP-BSP: It is a Commercial Virtual Power Plant (CVPP) which allows Distributed Energy Resources (DER) and flexible loads to be aggregate and participate in the balancing market. Only DERs that can be controlled can participate in balancing markets. The BSP is the coordinator of the DERs and has the task of selling the flexibility made available by these on the balancing market. The technical specifications of this software are described in the document VPP4INode Technical Specifications, Section 3.3

SP-CE: It is a Commercial Virtual Power Plant (CVPP) which allows active customers to be aggregate and forming an Energy Community (EC). The EC manager is the coordinator of the EC and has the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

role of managing assets shared among community members (e.g., energy storage units or photovoltaic panels on the roofs of residential buildings). The EC manager also has the role of informing the members of the energy community about their performance in terms of self-consumed energy, and of managing state incentives and sharing them among the CE members, if any. The technical specifications of this software are described in the document VPP4INode Technical Specifications, Section 3.4

2. What information assets fall within your area of involvement?

The information assets managed by the software platforms for BSP and CE are listed below:

SP-BSP:

1. Data on VPP members and physical assets:
    a. Data on the BSP, and managers of real power plants or flexible loads.
    b. Technical data on power plants and flexible loads in BSP portfolio.
2. Baseline (i.e., Scheduled active power injection/absorbent):
    a. Generator power injection schedules.
    b. Energy storage unit charging and discharging schedules.
    c. Flexible load power absorption schedule of flexible loads
3. Measurements:
    a. Active and reactive power measurement at the point of delivery (POD) to which the physical assets (generators, flexible loads, energy storage systems, etc.) are connected.
4. Price signals:
    a. Price-energy pairs at which a power plant manager offer the flexibility of their components to BSP (note: a real power plant can be composed of several components, a virtual power plant is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

composed of several real power plant)

b. Price-energy pairs at which the BSP offer the flexibility of the VPP to balancing market.

5. Control signals:

a. Set point of active power injection/absorption for each component involved in the CVPP when the flexibility is activated.

6. Remuneration of individual real plants:

a. Data on revenues from balancing market

SP-CE:

1. Data on EC members and physical assets:

a. Data on the members and managers of EC.

b. Technical data on renewable energy source such as Photovoltaic plants, wind turbines and energy storage system owned by the EC members.

2. Scheduling of controllable assets:

a. Generator power injection schedules.

b. Energy storage unit charging and discharging schedules.

c. Flexible load power absorption schedule of flexible loads

3. Measurements:

a. Active power measurement at the point of delivery (POD) of any EC member.

4. Control signals:

a. Set point of active power injection/absorption for ESS involved in the CE.

5. Remuneration of individual real plants:

a. Data on revenues from Self-consumption incentives.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. **Where are these assets located?**

   In the Data Base (DB) at VPP4INode level.

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   Both the software platform, SP-BSP and SP-CE, are provided with a web app.

   Through the web app, VPP members can get information about their components and real power plants.

5. **Which of these assets deal with critical information?**

   Control signal:

   1. Corrupted or manipulated set point values would not allow the system to work properly. They would not allow flexibility to be activated when required (for SP-BSP). They would not allow to control ESS to maximize the self-consumed energy (for SP-CE).

   Measurements:

   2. Corrupted or unavailable measurements do not allow to remotely observe the behavior of psychic assets in the field and to quantify the flexibility (for SP-BSP) or self-consumed energy (for SP-CE).

   Baselines:

   3. Corrupted or manipulated set point values would not allow the system to work properly. If a component's baseline is not provided to the SP-BSP then the component will not be able to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

participate in the balancing market (for SP-BSP).

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**
   TBD

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   TBD

8. **What cascading effects may take place if an information asset of yours is affected?**
   See point 5

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   Three types of incidents were identified:

   1. Measurements/Electronic device failure.

   2. Cyber-attack.

   3. Telecommunications system failure

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

    No additional information at the moment.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Risk information tables

The following tables refer to the SP-BSP, but they can easily be brought back for the SP-CE platform. It is observed that the SP-CE unlike the SP-BSP does not receive price signals from the components in the field. This is because the EC elements are operated to maximize self-consumption of energy and not to profit in the markets.

1 - Data on VPP members and physical assets

Information asset name	Data on VPP members and physical assets	**Asset importance**	6
Information asset type	Electronic files	**GDPR sensitive**	YES
Owning Stakeholder	VPP members and BSP	**Stakeholder type**	Conventional Power Plant, Solar-power Power Plant, Win-power Power Plant, ESS, Flexible Loads
Identified risk	Unauthorized third-party access	**Likelihood**	6
Risk's origin	Web app access passwords come into the possession of unauthorized third parties.	**Impact severeness**	5
Risk description	An unauthorised third party gains access to information on the system.		
Expected consequences	Unauthorised circulation of personal data on members or technical data on installations.		
Mitigating stakeholder	All members who hold system passwords such as managers of real plant and BSPs.		
Solution / mitigation actions	Setting high security passwords.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

2 - Baseline

Information asset name	Baseline	**Asset importance**	6
Information asset type	Electronic files	**GDPR sensitive**	YES
Owning Stakeholder	VPP members and BSP	**Stakeholder type**	Conventional Power Plant, Solar-power Power Plant, Win-power Power Plant, ESS, Flexible Loads
Identified risk	Failure to receive baseline (from human/algorithm to software platform)	**Likelihood**	6
Risk's origin	Malicious acts such as Cyber-attack or failure of telecommunication system. Intentional or unintentional human intervention.	**Impact severeness**	5
Risk description	Software platform does not receive the baseline of some or all aggregate components.		
Expected consequences	Abnormal operation or non-functioning in the flexibility dispatching process.		
Mitigating stakeholder			
Solution / mitigation actions			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3 – Measurements

Information asset name	Measurement's data	**Asset importance**	9
Information asset type	Electronic files	**GDPR sensitive**	YES
Owning Stakeholder	power plant manager or consumer	**Stakeholder type**	Conventional Power Plant, Solar-power Power Plant, Win-power Power Plant, ESS, Flexible Loads, consumer
Identified risk	Failure to receive measures	**Likelihood**	6
Risk's origin	Failure of individual measuring device or failure of data telecommunication system.	**Impact severeness**	10
Risk description	Software platform does not receive real-time field measurements. Abnormal operation or non-functioning in the flexibility dispatching process.		
Expected consequences	Corrupt or unavailable measurements do not allow to: Observ and control physical assets. Quantify the flexibility (for SP-BSP) or self-consumed energy (for SP-CE).		
Mitigating stakeholder	RTU developer Telecommunications system		
Solution / mitigation actions	Adopt highly reliable electronic devices		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

4 – Price data

Information asset name	Price data	**Asset importance**	6
Information asset type	Electronic files	**GDPR sensitive**	
Owning Stakeholder	VPP members and BSP	**Stakeholder type**	
Identified risk	Failure to receive price data (from a human/algorithm to software platform).	**Likelihood**	6
Risk's origin	Malicious acts such as Cyber-attack or failure of telecommunication system. Intentional or unintentional human intervention	**Impact severeness**	10
Risk description	The selling price of the flexibility of one or more physical assets are not received by the software platform.		
Expected consequences	The physical assets that do not make available data on sales prices will not be able to take part in the flexibility dispatching process.		
Mitigating stakeholder			
Solution / mitigation actions			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

5 – Control signals

Information asset name	Control signals	**Asset importance**	9
Information asset type	Electronic File	**GDPR sensitive**	YES
Owning Stakeholder	Power plant manager, BSP or CE manager.	**Stakeholder type**	Conventional Power Plant, ESS, Flexible Loads,
Identified risk	Failure to send control signals (from software platform to power plants, ESS, etc.)	**Likelihood**	6
Risk's origin	Malicious acts such as Cyber-attack or failure of telecommunication system. Intentional or unintentional human intervention.	**Impact severeness**	10
Risk description	The software platform loses the ability to remotely control production and/or consumption of power units, flexible loads and ESS in the field.		
Expected consequences	Production and/or consumption units will not be able to participate in the balancing market.		
Mitigating stakeholder			
Solution / mitigation actions			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

6 - Reports on remunerations

Information asset name	Reports on remunerations	**Asset importance**	8
Information asset type	Electronic files	**GDPR sensitive**	YES
Owning Stakeholder	VPP members and BSP or CE manager	**Stakeholder type**	Conventional Power Plant, Solar-power Power Plant, Win-power Power Plant, ESS, Flexible Loads
Identified risk	Unauthorized third-party access	**Likelihood**	6
Risk's origin	System access passwords come into the possession of unauthorized third parties.	**Impact severeness**	5
Risk description	An unauthorised third party gains access to information on the system.		
Expected consequences	Unauthorised circulation of personal data on members or technical data on installations.		
Mitigating stakeholder	All members who hold system passwords such as managers of real plant and BSPs.		
Solution / mitigation actions	Setting high security passwords.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

2. BORNHOLMS VARME A/S [BEOF]

ID information

1. **Full name:** Torben Jørgensen
2. **E-mail address:** **toj@beof.dk**
3. **Organization:** Bornholms Varme A/S
4. **Role in the project:** *End User: Follower Island*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. **Please describe in detail your involvement and function in the project?**

   Project Manager from Bornholm

2. **What information assets fall within your area of involvement?**

   data from PV-production, data from electric boilers at heat plant, data from smart meters at costumers, data from Danfoss computers in selected costumer installations.

3. **Where are these assets located?**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

at the Demo site: Heatplant at Østerlars and the District Heating Network of Østerlars, Østermarie and Gudhjem

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   all I guess can be indirectly accessed by humans

5. **Which of these assets deal with critical information?**

   none I guess

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**
   The electric boilers are today redundant capacity to the main biomass-boiler (straw-fuled)

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   My company has an IT security plan and procedures

8. **What cascading effects may take place if an information asset of yours is affected?**
   It is not clear to me

9. **What would be the highest expected cost for recovery after an incident? Please provide**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

a short justification of the cost.

I think that recovery in our case will be about data, if it is possible to recover

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

–

Risk information tables

Information asset name	Rooftop PV	**Asset importance**	1
Information asset type	solar panels + inverters etc.	**GDPR sensitive**	No
Owning Stakeholder	Bornholms Varme A/S	**Stakeholder type**	*Other (heat plant)*
Identified risk	Loss of data	**Likelihood**	1
Risk's origin	system brake down	**Impact severeness**	0
Risk description	system failure or hacking		
Expected consequences	blindness to function and operation		
Mitigating stakeholder	= owning stakeholder		
Solution / mitigation actions	repair		

Information asset name	Electric boilers	**Asset importance**	3
Information asset type	4 x 0,6 MW boilers	**GDPR sensitive**	No
Owning Stakeholder	Bornholms Varme A/S	**Stakeholder type**	*Other (heat plant*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Identified risk	Loss of data	**Likelihood**	1
Risk's origin	system brake down	**Impact severeness**	2
Risk description	system failure or hacking		
Expected consequences	Electric boilers are not operable		
Mitigating stakeholder	= owning stakeholder		
Solution / mitigation actions	repair		

Information asset name	smartmeters at consumers	**Asset importance**	9
Information asset type	650 Kamstrup smart meters	**GDPR sensitive**	No
Owning Stakeholder	Bornholms Varme A/S	**Stakeholder type**	*Other (heat plant*
Identified risk	Loss of data	**Likelihood**	1
Risk's origin	system brake down	**Impact severeness**	1
Risk description	system failure or hacking		
Expected consequences	12 Data are not available		
Mitigating stakeholder	= owning stakeholder		
Solution / mitigation actions	repair		

Information asset name	Danfoss computers at selected consumers	**Asset importance**	1
Information asset type	Danfoss ICL 310	**GDPR sensitive**	Yes
Owning Stakeholder	Consumers	**Stakeholder type**	*Consumers*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Identified risk	Loss of data	**Likelihood**	1
Risk's origin	Data unavailable	**Impact severeness**	1
Risk description	Danfoss will allow access to their portal		
Expected consequences	computers at consumers are not available for flexibility experiments		
Mitigating stakeholder	Bornholms Varme A/S		
Solution / mitigation actions	Negotiations with Danfoss		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. BRUNEL UNIVERSITY LONDON [BUL]

ID information

1. **Full name:** Geert Jansen
2. **E-mail address:** geert.jansen@brunel.ac.uk
3. **Organization:** BUL
4. **Role in the project:** *Other*

Questions

The questionnaire focuses to the risks of information handling during the envisioned operation of the VPP4ISLANDS system.
So, it does not have to do with the operation of the physical assets like fuel cells etc., as it is about the digital information handling risks: transactions info, technical data info, personal data info, all shared info in the system.

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. **Please describe in detail your involvement and function in the project?**

   BUL will develop experimentally validated energy models of various types of islands' renewable power plants with energy storage systems that enable the optimisation of the design solutions and the simulation of a full-scale integrated power streams to determine the system behaviour under different configurations and control strategies, the provision of flexibility services and potential revenue streams as well as input for the life-cycle assessment. All the mathematical models and optimization algorithms developed and tested will be built on field data provided by the island partners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

2. What information assets fall within your area of involvement?

Computational models

- Modelling and technical/operational design of a hybrid Regenerative Hydrogen Fuel Cell (RHFC) and Battery Energy Storage System.
- Integrated renewable energy generation and storage system mathematical models (energy profiles, round-trip efficiency, LCOE, carbon-electricity impact) with optimization algorithms for effective Virtual Power Plant (VPP) design and deployment.
- Modelling data informs energy system commissioning and site preparation, and overall optimised operation and maintenance aspects of the VPP4ISLANDS energy solution.

Design information

- Concentration of collected data on island's energy generation structures and power consumption profiles.
- Energy consumption data from council owned buildings and anonymous commercial and residential buildings and privately owned power generators (this may require ethical approval process).
- System's technical, environmental, and economical performance and load-factor characteristics of the RHFC.
- Literature support documentation on VPP system design, components, modelling, policies, etc.
- Knowledge on social, regulatory, and technical barriers for implementation of VPP.
- Operation & maintenance characteristics of the RHFC system.

Operational information

- Operation & maintenance data of the RHFC system.
- Weather data (historic, real-time, and forecasted climate, weather, etc).

3. Where are these assets located?

Brunel SharePoint, local hard disk (off-line), expertise/specialised knowledge, Shared Knowledge Base (To be confirmed with consortium, protection methods to be determined by consortium)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   All

5. **Which of these assets deal with critical information?**

   All (critical for operation of optimised VPP solutions)

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

   All information at BUL is classified according to the BUL-POL-8.2 into University Confidential, Protect and Unclassified. This policy, along with the BUL-PROC-8.02 Information Classification guidelines, assists all members of the University to ensure that correct classification and handling methods are applied and information is managed accordingly. Thereby, the BUL-ADV-FILE (File Handling Guideline) is set up. The purpose of this Advisory is to outline the acceptable ways of handling information assets and file storage at Brunel University London (BUL).
   The BUL Network Access Policy (BUL-POL-09.02) establishes the area within BUL covering who or what has authorised permission to access the University network and information. The Password Management Policy (BUL-POL-9.3.3) establishes the area within BUL covering Password Management and reflects the current good practice recommended by NCSC1 and Microsoft. This document is valid for all University information systems and all applications that are password protected. This excludes Third party systems that require University access (e.g., password protected APIs for modelling input data).

   - Brunel SharePoint: Two-Factor Authentication login helps to stop hackers from getting into accounts, even if they have the password.
   - Local hard disk: Off-line backup stored in room accessible only by authorized personnel with physical key.
   - Expertise/specialised knowledge: Non-Disclosure Agreement signed by students and staff that have access to the critical information.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Thereby, a data protection policy is laid out which describes the standards and obligations to be met with respect to the processing of personal data by members of the University: (https://www.brunel.ac.uk/about/documents/pdf/DP-policy.pdf)

7. With information security in mind, what kind of mitigation actions have you planned in case of emergency?

The Information Security Incident Management Data Breach Procedure (BUL-PROC-16.03) relates to all personal and special categories (sensitive) data held by the University regardless of format. This procedure sets out the action to be followed to ensure a consistent and effective approach is in place for managing data breaches and is aligned to the BUL ISMS information security incident management policy and procedure across the University. The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

When a breach is ongoing, every effort must be made to contain the breach. Containment is most likely to be necessary in cases where a breach is caused by a cybersecurity incident, such as phishing. Recovery takes place after the breach event has ended. This phase includes learning lessons from the breach and putting measures in place to try to avoid any similar breaches occurring in the future.
In the case of simple email breaches (where an email containing personal data has been sent to the wrong individual), recovery will most often consist of requesting that the person or people who received the email in error, delete the email.
Containment and recovery measures should be organised by the Data Protection Office (DPO) / Cyber and Information Security Manager (CISM).
Notify the DPO of the breach before trying to recover from it.
(For more information, please see: https://www.brunel.ac.uk/about/documents/pdf/breach.pdf)

8. What cascading effects may take place if an information asset of yours is affected?

Cascading effect 1	Cascading effect 2
1. Leakage/theft of critical design/operational information of the VPP4ISLANDS energy solution.	1. Loss of access to critical design/operational information of the VPP4ISLANDS energy solution.
2. Plagiarise/replicate designs and	2. Malfunctioning computational models

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

computational models of the VPP4ISLANDS energy solution.	of the VPP4ISLANDS energy solution.
3. Threaten exploitation success of VPP4ISLANDS energy solution / Loss of intellectual property on VPP4ISLANDS energy solution.	3. Compromised optimal operation of the VPP4ISLANDS energy solution, not meeting the demonstrated performance objectives.

Mitigation methods in place to prevent these cascading effects from occurring are given in the Table 4 and Table 5 on page 75 of this document.

9. What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.

Loss of access to technical design information and/or computational models may result in (severe) delays to recreate the files and ensure accurate operation of the VPP4ISLANDS energy solution.
Cost of recovery after such incident can mainly be attributed to the cost of time to recreate the affected files. This is mitigated by extensive notetaking and documentation of the followed design procedure and restoring of models form previous versions stored and backed up.
Drives at BUL are backed up each night with a full backup at the weekend and incremental backup each night. These backups are kept on-site for 35 days. An additional full backup is run every 4 weeks and kept off-site for 175 days. Thereby, the '3-2-1-rule for Backup' is followed wherever possible as best practice:

3. Keep 3 copies of important files
2. on 2 different media (if possible)
1. with 1 copy being stored offsite (or offline)

These mitigations ensure it is possible to restore the capacity to keep supporting the VPP4ISLAND energy solution in operation as quickly as possible. An estimate for the maximum recovery time (worst-case scenario) is about 2 person-months, with cost associated to hourly wages, computational licenses, and additional overhead costs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

10. Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.

The purpose of the Brunel Email Use Policy (BUL-POL-EMAIL) is to outline the acceptable use of electronic mail within BUL, and while using email and allied facilities using an account provided by BUL or managed on behalf of BUL by a third party.

Brunel IS Acceptable Use Policy (BUL-POL-AUP) and the Brunel Acceptable Computer Use Policy (BACUP) outline the acceptable use of IT equipment at BUL and to lay forth the rules for computer use by BUL duly authorised users (whether or not such use is conducted on the premises of BUL),

The Information Security Risk Management Policy (BUL-POL-IRM01) is essential to ensure that information, in whatever format, is provided the correct level of protection commensurate with its sensitivity and criticality to BUL business and operations.

All staff undergo annual roll dependent compliance training for:

- Data protection.
- Environmental sustainability.
- Health and safety.
- Information security.

Risk information tables

Table 4: Information on information leak/theft risk for information assets during operation of the VPP4ISLANDS energy solution

Information asset name	All information assets mentioned under question 2 on page 71	**Asset importance**	10
Information asset type	Electronic Files	**GDPR sensitive**	NO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Owning Stakeholder	BUL	**Stakeholder type**	Other: VPP4ISLANDS energy solutions
Identified risk	Leakage/theft of data/information mentioned under question 2 on page 71	**Likelihood**	2-3
Risk's origin	- Disclosure of passwords - Unauthorized access to the network/premises - Theft/hacking	**Impact severeness**	6-7
Risk description	Intentional human intervention, resulting in break into system and/or premises and access confidential/critical information		
Expected consequences	- Threaten exploitation success of VPP energy solution. - Loss of intellectual property.		
Mitigating stakeholder	BUL Data Protection Officer and/or Cyber and Information Security Manager		
Solution / mitigation actions	Internal policies and advisories for: - Data classification - Data storage and backups - File handling (including via email within the consortium) - Password and two-factor authentication protection These policies and advisories are regularly reviewed by the Data Protection team and Cyber and Information Security. Thereby, antivirus and firewall software are parts of the overall information security.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Table 5: Information on information loss/compromised data risk for information assets during operation of the VPP4ISLANDS solution

Information asset name	All information assets mentioned under question 2 on page 71	**Asset importance**	10
Information asset type	Electronic Files	**GDPR sensitive**	NO
Owning Stakeholder	BUL	**Stakeholder type**	Other: VPP4ISLANDS energy solution
Identified risk	Loss of system design data/information	**Likelihood**	2-3
Risk's origin	- Maintenance error - Electrical outage - Destruction of records	**Impact severeness**	6-7
Risk description	- Introduction of weaknesses into the systems during routine maintenance. - Premises will suffer an electrical outage, which could knock servers offline and stop employees from working, unable to access sensitive information for hours or even days - Digital files are corrupted and/or are rendered unavailable		
Expected consequences	Compromised operation of the VPP4ISLANDS energy solution		
Mitigating stakeholder	BUL Data Protection Officer and/or Cyber and Information Security Manager		
Solution / mitigation actions	Internal policies and advisories for: - Data classification - Data storage and backups - File handling (including via email within the consortium) - Password and two-factor authentication protection These policies and advisories are regularly reviewed by the Data Protection team and Cyber and Information Security. - Thereby, antivirus and firewall software are parts of the overall information security.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

4. CARDIFF UNIVERSITY [CU]

ID information

1. **Full name:** Saif S Sami
2. **E-mail address:** **Samis1@cardiff.ac.uk**
3. **Organization:** Cardiff University
4. **Role in the project:** *Technical Partner: Software*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. Please describe in detail your involvement and function in the project?

Cardiff University (CU) is responsible for promoting the concept of the Virtual Energy Storage System (VESS). The VESS aggregates different components of energy systems, that include conventional Energy Storage Systems (ESS), flexible loads, distributed generation (DG) and multi-vector energy systems.

Cardiff University will develop models of components of the VESS (i.e. Task 3.2 of the project). These models include flexible loads such as heat pumps, domestic refrigerators and small behind-the-meter energy storage systems. CU will also collaborate with other partners to develop control schemes of the VESS to provide flexibility services (i.e. Task 4.3, Task 4.4 and Task 4.6 of the project). Through these control schemes, the VESS will be able to provide various services to transmission and distribution systems operators. The developed models and Application Programming Interface (API) will be validated by simulations and tested through Hardware-In-Loop (HIL) approach by CU, AMU

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

and BUL (i.e. Task 3.4 in the project). CU will define a use case study for the VESS demonstration area (i.e. Task 7.2.1 in the project). In addition, CU will support defining the smart contracts (i.e. Task 2.5 in the project) to be implemented.

2. What information assets fall within your area of involvement?

During mathematical modelling of some of the VESS components, some detailed information regarding the modelled buildings is required. For example, representative data of thermal properties of buildings (or historical time-series data for outdoor and indoor temperatures, as well as the heat supplied to buildings), specifications of selected appliances to be included in the VESS portfolio and minimum and maximum limits for indoor temperature. Control schemes of the VESS will continuously receive information from the local controllers of the VESS components, including but not limited to, temperatures of buildings and information related to appliances, distribution network, behind-the-meter ESS and DG. Some of these control schemes will also receive weather and load forecasting data and energy market prices. The VESS demonstration area related information may include, the VESS components information, distribution network parameters, data on DG and non-flexible loads. The aforementioned information assets can fall under these two categories:

1- Technology characteristics: these are essential assets information, such as ESS and DG capacities, rated power of flexible loads.

2- Operational data: these data can be classified into measurements and control set-points.

Measurement signals include, but are not limited to, the system frequency and voltages at selected busbars, in addition to measurements from ESS, flexible loads and DG. Control signals can be the instructions issued by the VESS controllers to its components, or they can be signals related to the forecasting or the energy market sent by VPP4INode(s) and systems operators to the VESS controllers.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. **Where are these assets located?**

   Technology characteristics are mainly stored at VPP4IBox level. Measurement signals are received by the VPP4Ibox mainly from Remote Terminal Units (RTU) at flexible loads, ESS and DG premises, in addition to signals sent by VPP4INode(s) and system operators. Control signals are generated by different control schemes of the VESS at VPP4Ibox level and sent to RTUs and VPP4INode(s) and system operators.

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   Both information assets can be accessed by authorised personnel.

5. **Which of these assets deal with critical information?**

   Both technologies characteristics and operational data retain vital information, compromised or damaged information results in improperly functioning controllers of the VESS.

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

   Technology characteristics are static and do not change during the operation, and if damaged it can be restored from backup facilities. However, operational data are continuously changing variables, replacing any missing signal with a recorded value may result in inaccurate VESS actions. A secure communications configuration can protect the confidentiality, integrity and availability of the different signals.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   An emergency plan can involve restoring technology characteristics by an authorised person with backup files. However, an interruption to the VESS routine is inevitable in case of damaged or manipulated operational data.

8. **What cascading effects may take place if an information asset of yours is affected?**

   Both Information assets are driving the control schemes of the VESS, and thus issues with the assets may lead to losing the VESS ability to provide the contracted services. Depending on the type of service provided, the system operator may have to activate contingency plans to compensate for the VESS under or over delivery. Consequently, there will be economic aspects and an impact on the VESS reliability.

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   As a failure to provide a contracted service, the VESS aggregator may face at least a reduction in revenues. The VESS aggregator may also finance the costs incurred to procure the service from other providers.

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**
    Further observations or notes may rise as the project progress.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Risk information tables

Information asset name	Technology characteristics (for components of VESS)	**Asset importance**	6
Information asset type	Electronic files	**GDPR sensitive**	Yes
Owning Stakeholder	VESS aggregator VPP aggregator	**Stakeholder type**	Solar-power Power Plant, Wind-power Power Plant, VESS
Identified risk	Unauthorized access	**Likelihood**	5
Risk's origin	Intentional or unintentional human intervention	**Impact severeness**	5
Risk description	An unauthorized person may gain access to essential information on the VPP4IBox		
Expected consequences	Information integrity compromised, potential impact on the performance of the VESS		
Mitigating stakeholder	VESS aggregator		
Solution / mitigation actions	Tighten security measurements, create backup copies		

Information asset name	Measurements (for VESS)	**Asset importance**	7
Information asset type	Electronic files	**GDPR sensitive**	Yes
Owning Stakeholder	VESS aggregator VPP aggregator	**Stakeholder type**	Solar-power Power Plant, Win-power Power Plant, VESS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Identified risk	Damaged or manipulated measurements	**Likelihood**	6
Risk's origin	Failure in the sending devices (e.g. RTU) or communication system, exposed and altered measurements	**Impact severeness**	8
Risk description	Control schemes of the VESS receive compromised measurements.		
Expected consequences	Incorrect or misleading control actions are given to the VESS components, which leads to revenues cut and system reliability degradation.		
Mitigating stakeholder	Sending devices and communications system operators.		
Solution / mitigation actions	Highly reliable and secure sending and communication systems adaptation		

Information asset name	Control signals (for VESS)	**Asset importance**	8
Information asset type	Electronic files	**GDPR sensitive**	Yes
Owning Stakeholder	VESS aggregator	**Stakeholder type**	VESS
Identified risk	Damaged or manipulated Control signals	**Likelihood**	6
Risk's origin	Failure in control schemes of the VESS or communication system, exposed and altered Control signals	**Impact severeness**	9
Risk description	Components of the VESS receive a modified or damaged control signals		
Expected consequences	Inaccurate services provision by the VESS components, which leads to revenues cut and system reliability degradation		
Mitigating stakeholder	VESS aggregator or communication system operator		
Solution / mitigation actions	Highly reliable and secure control and communication systems adaptation		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

5. GRADO MUNICIPALITY [GRADO]

ID information

1. **Full name:** Maria Antonietta Genovese
2. **E-mail address:** maria.genovese@comunegrado.it
3. **Organization:** Municipality of Grado
4. **Role in the project:** End User: Follower Island

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. **Please describe in detail your involvement and function in the project?**

   Main contact for the Municipality of Grado (Follower Island).

   Administrative and techincal management of the project within the Municipality, coordination of activities, assigning and evaluation of internal and external contributions.

2. **What information assets fall within your area of involvement?**

   As the head officer of the technical division, Dr. Genovese has access to all information assets, but is mainly involved in technical, geographical, and environmental data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. **Where are these assets located?**

   All digital assets are hosted on the Municipality's servers, physically located in the Municipality's headquarters. Backup servers are located on a separated building, also property of the Municipality.

   There are some assets provided by the Public Body Friuli Venezia Giulia Region, and hosted on their premises.

   Some applications are hosted on servers/VMs of external providers, who are subject to specific SLAs.

4. **Regardless of frequency, which of these assets are accessible directly or indirectly by humans while in operation?**

   Most assets are accessed directly by the end-users, either directly as files on network shares or indirectly through domain-specific applications.

   API / automated accesses are instead in use mainly for maintenance purposes (backups, monitoring).

5. **Which of these assets deal with critical information?**
   - GDPR
   - financial and banking information
   - public tender information

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

- password based
- IP restriction (VLAN)
- perimetric firewall
- VPN
- registry of GDPR processing operations, including assessment of the risks and mitigation tied to the GDPR.

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   Automated differential backups, with a retention period exceeding 6 months, are in place on dedicated local NAS, in a different building than the server.

   Bare-metal recovery procedures are also available by means of VM backups.

8. **What cascading effects may take place if an information asset of yours is affected?**

   Very little, as all important data are not only backed up, but also printed in hard copy.

   Furthermore, there is also an insurance in place.

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   Buying and configuring a complete new set of servers would cost about 50.000 €, in case of total failure (i.e. burn/flooding)

   A ransomware attack could try to request an amount of 100.000 € or higher (evaluation is based on the yearly budget of the Municipality).

   NAS data are however not shared on nor accessible from the network.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

As most Municipalities, the main concern about data security is focused on GDPR, while other aspects are usually not considered so critical.

Risk information tables

n/a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

6. INGENIERIA Y DISEÑO ESTRUCTURAL AVANZADO [IDEA]

ID information

1. **Full name:** Francisco Méndez Flores
2. **E-mail address:** **fmendez@ideaingenieria.es**
3. **Organization:** IDEA Ingeniería
4. **Role in the project:** *Technical Partner: Software*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. **Please describe in detail your involvement and function in the project?**

   IDEA Ingeniería develops the digital twin engine as the leader of work package 3 and participate in other work packages as well.

2. **What information assets fall within your area of involvement?**

   The digital twin engine, the electrical grid model and the environment model.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. **Where are these assets located?**

   Within the digital twin system, and therefore, the VPP4I Platform.

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   The assets may be indirectly accessed by humans if they request a simulation.

5. **Which of these assets deal with critical information?**

   We find the assets not dealing with critical information, just historical data of different data sources and the electrical grid description of the island.

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**
   Not applicable.

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   We find the digital twin engine to be a subsystem of the core, which is de VPP4I Cloud Platform.

8. **What cascading effects may take place if an information asset of yours is affected?**
   Not applicable.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   Not applicable.

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

    No comments.

Risk information tables

Information asset name	Digital twin engine	**Asset importance**	5
Information asset type	Software	**GDPR sensitive**	No
Owning Stakeholder	Consortium	**Stakeholder type**	TBD
Identified risk	NA	**Likelihood**	NA
Risk's origin	NA	**Impact severeness**	10
Risk description	NA		
Expected consequences	NA		
Mitigating stakeholder	NA		
Solution / mitigation actions	NA		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

7. RDIUP [RDIUP]

ID information

1. **Full name:** Habib NASSER
2. **E-mail address:** **habib.nasser@rdiup.com**
3. **Organization:** RDIUP
4. **Role in the project:** *R&D director*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. **Please describe in detail your involvement and function in the project?**

   RDIUP is responsible for the development of data analytics modules in the node level and DSS/SPT module for replication in the platform VPP4I. Also RDIUP is the WP leader for communication, dissemination and exploitation.

2. **What information assets fall within your area of involvement?**

   Regarding the technical activities RDIUP will provide tailored plans for replication in three islands

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. **Where are these assets located?**

   the question is not clear, but our plans will be replicated in Grado, Bozcaada and Bornholm islands

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   Our off-line modules will not in contact with humans while in operation

5. **Which of these assets deal with critical information?**

   The replication plans allow to enhance the behaviors of the existing energy systems. Critical information have to be defined by the concerned stakeholders such as DSOs.

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

   prevention/protection safeguards are not concerned in our modules.

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   Our solutions provide high level services and off-line replication plans. The provided recommendations will support key stakeholders to make decisions. Therefore, the mitigation actions will be planned by these stakeholders.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

8. **What cascading effects may take place if an information asset of yours is affected?**
   The decisions will be made by end-users and VPP owners and not by our modules

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   We just support owners to optimize their portfolio so no costs are engendered by our solutions.

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

    –

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Risk information tables

Information asset name	SPT (smart planning tool)	**Asset importance**	8
Information asset type	Cloud-based application	**GDPR sensitive**	yes
Owning Stakeholder	Aggregator or DSO	**Stakeholder type**	DSO
Identified risk	Lack of meaningful data	**Likelihood**	5
Risk's origin	Confidentiality, absence of monitoring systems and ethical aspects	**Impact severeness**	8
Risk description	The difficulty to collect enough data from the demos and the generation of poor information. Thus, will affect the robustness of the MLs and the decision making.		
Expected consequences	Difficulties to generate replication plans		
Mitigating stakeholder	RDIUP, leading and follower islands		
Solution / mitigation actions	it is possible to look for historical data, open datasets, gather data from existing projects and complete with simulated data from the digital twin.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

8. REGENERA [REGE]

ID information

1. **Full name:** Beatriz Castro Granados
2. **E-mail address:** bcastro@regeneralevante.com
3. **Organization:** Regenera Levante S.L.
4. **Role in the project:** *Other*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. Please describe in detail your involvement and function in the project?

REGENERA will develop a forecasting engine of market price (T4.1.2) and the energy and CO2 savings tool (T4.1.4).

2. What information assets fall within your area of involvement?

Following data is required:

- Historical consumption data for more than 1 year

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

- Marks for special days
- Weather forecasts for past and future with below tags
    - Temperature
    - Humidity
    - Precipitation
    - Wind Speed
    - Cloud Cover
- Both weather and consumption data with same frequency

3. **Where are these assets located?**

   All this information assets are provided by WP2.

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   Forecasting engine of market price and the energy and CO2 savings tool will be controlled by humans.

5. **Which of these assets deal with critical information?**

   None of them.

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

To be determined.

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   To be determined.

8. **What cascading effects may take place if an information asset of yours is affected?**

   Results of WP4 will be affected.

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   –

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

    No additional information.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Risk information tables

Information asset name	Historical consumption data	**Asset importance**	9
Information asset type	Intangible Information	**GDPR sensitive**	YES
Owning Stakeholder	Leading/following island	**Stakeholder type**	DSO, TSO, Consumers, or Prosumers
Identified risk	Problems in obtaining this data	**Likelihood**	6
Risk's origin	Data protection	**Impact severeness**	8
Risk description	Historical consumption data may be protected, and permissions may have to be requested or more smart meters may have to be installed to get them than defined in the proposal.		
Expected consequences	Longer implementation time and increased budget.		
Mitigating stakeholder	Leading/following island		
Solution / mitigation actions	To be assisted by DSO's who have access to the information.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

9. SCHNEIDER ELECTRIC [SCHN]

ID information

1. **Full name:** David Pampliega
2. **E-mail address:** **david.pampliega@se.com**
3. **Organization:** Schneider Electric
4. **Role in the project:** *Other*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. **Please describe in detail your involvement and function in the project?**

   Schneider Electric is contributing to VPP4Islands project by providing Remote Terminal Units (RTU), which are devices in charge of monitoring and control of the electric infrastructure. These RTU are part of the VPP4IBox concept that is going to be implemented in the project.

2. **What information assets fall within your area of involvement?**

   The RTU will process electric magnitudes, to be shared with other elements of the VPP4Islands architecture. These magnitudes would be obtained normally by some monitoring devices or energy analyzers available in each of the monitored sites at the islands.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. **Where are these assets located?**

   In the VPP4IBoxes, in several location in the two main islands of the project.

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   The RTU are designed to work in an autonomous way, without an intervention from the operators. Nevertheless, the RTU could be accessed either locally or remotely by the operators in order to have their configuration updated or to have access to real-time data that is being exchanged through the RTU.

5. **Which of these assets deal with critical information?**

   The RTU deals with electric magnitudes (for instance, voltage, frequency, power), that could be used by other elements of the VPP4Islands architecture to come up with different strategies as per the defined use cases in the project.

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

   The RTU implements cybersecurity mechanisms in order to safeguard its behaviour against cyber attacks. Also, as an extra security measure, it is common that IP communications are within a VPN.

   Redundancy capabilities would be also available at the RTU, contributing to a high availability of the system in place.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   The RTU includes cyber security mechanisms. However, the mitigation actions to be implemented in case of emergencies are dependent of the internal policies at electric utilities making use of the RTU.

   An example of mitigation actions could be for instance the utilization of honeypots, the utilization of VPN to avoid the exchange of information of the RTU with the outside of the VPN, or the utilization of physical security measures in the VPP4IBox.

8. **What cascading effects may take place if an information asset of yours is affected?**

   If the RTU were compromised, a cyber attacker could send erroneous information to the higher levels of the VPP4Islands architecture, and thus, the decisions resulting on the analysis of such information could lead to issues on the grid or to an underperformance of the provided services.

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   This cost should be obtained jointly between the providers of the use cases and the operators, so they could jointly evaluate the different incidences that could appear, and the recovery cost associated to them.

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

It's important to highlight that the RTU is not the only component available at the VPP4IBox. VPP4IBox will also have a Raspberri Pi performing some functions (Smart Contracts, VESS), so in order to have a complete evaluation of the VPP4IBox, the Raspberri Pi component should also be considered.

Risk information tables

Information asset name	RTU	**Asset importance**	7
Information asset type	Other – hardware/software controller	**GDPR sensitive**	TBD – It depends if customer data is collected from the islands or not (it is not clear yet)
Owning Stakeholder	UEDAS / Formentera	**Stakeholder type**	DSO / Formentera government
Identified risk	RTU misuse / data tampering	**Likelihood**	6
Risk's origin	Malicious acts	**Impact severeness**	9
Risk description	A malicious user is able to tamper with the RTU or to supplant another device connecting to the RTU, and is able to successfully sending erroneous data to the RTU.		
Expected consequences	Decisions resulting on the analysis of misleading information could lead to issues on the grid or to an underperformance of the provided services.		
Mitigating stakeholder	Operator / IT Security department		
Solution / mitigation actions	Physical protection of the VPP4IBox through secure locks, and establishment of secure communications between the RTU and other elements.		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

10. TROYA ENVIRONMENTAL ASSOCIATION [TROYA]

ID information

1. **Full name:** Oral Kaya
2. **E-mail address:** info@troyacevre.org , oralkaya@gmail.com
3. **Organization:** TROYA Environmental Association
4. **Role in the project:** *Other*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. Please describe in detail your involvement and function in the project?

TROYA is **non-technical partner** of the project. Our main task is gathering and distributing information regarding policies and legislations with regard to energy transition in islands.

In addition, Troya performs activities for networking purposes and creating community based energy cooperation. Furthermore, our tasks includes following conferences about renewable energy, energy efficiency and establish links with other energy cooperatives and islands that advocate for energy independence.

TROYA will also participate in the activities of environment and social assessment. We will

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

assist the island representatives to build living labs in the islands.

2. **What information assets fall within your area of involvement?**

   During networking, social assessment and living lab activities, Troya will contact the residents, representatives of NGO's, companies, academicians and conduct interviews and gather some private information. Troya has *Personal Data Protection And Privacy Policy* and *Informed Consent Form* to be used during these activities. Troya will take all necessary measures and show the necessary care to keep confidential information strictly private and confidential, and to prevent all or any part of confidential information from entering the public domain or unauthorized use or disclosure to a third party.

3. **Where are these assets located?**

   N/A

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   N/A

5. **Which of these assets deal with critical information?**

   N/A

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

N/A

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**

   N/A

8. **What cascading effects may take place if an information asset of yours is affected?**

   N/A

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**

   N/A

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**

    TROYA is non-technical partner of the project and therefore, do not possess any technical or innovative system information.

Risk information tables

n/a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

11. ULUDAĞ ELEKTRIK DAĞITIM A.Ş: GÖKÇEADA ISLAND [UEDAS]

ID information

1. **Full name:** Mehmet KOÇ
2. **E-mail address:** **mkoc@uedas.com.tr**
3. **Organization:** ULUDAĞ ELEKTRİK DAĞITIM AŞ
4. **Role in the project:** *End User: Lead Island*

Questions

Based on your experience and/or your role in the VPP4Islands project, please answer the following questions:

1. Please describe in detail your involvement and function in the project?

- We are the implementer of project, data source and data generator of the project. The project will apply in our distribution area with Electricity distribution system. From TSO to customers include local renewable energy plants will be include in project.

2. What information assets fall within your area of involvement?

- In this project, electricity grid and AMR (Automatic Meter Reading) system of UEDAS will be used . The electricity grid includes TSO, customers' datas, distribution centers, Wind

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

power plants and solar power plants. AMR system includes monitoring, active protection subsystems, analyzed data, whole control of grid (switches, relay, interrupt etc.).

3. **Where are these assets located?**

   - UEDAS has 4 cities land to distributed electricity that includes Bursa Province, Yalova Province, Balıkesir Province and Çanakkale Province with more than 3.5M customer. The project area located in whole Gökçeada Island in Çanakkale Province.

4. **Regardless of frequency, which of these assets are access directly or indirectly by humans while in operation?**

   - The grid feeds every customer in hospital, police station, military areas, city lights, government offices in Gökçeada Island. Moreover, local wind turbine and solar energy plants connected to the grid. The datas are not publicly available. It can be used by only Authorized users and It is enclosured on servers of UEDAS.

5. **Which of these assets deal with critical information?**

   - Energy production and consumption information, data read from customer meters and network structure are considered as critical information.

6. **What kind of prevention/protection safeguards are implemented in each one? Please refer to any redundancy capability and its capacity prior to anything else.**

   - Data is obtained remotely automatically or closely manually and stored on system servers. Our IT system processes stored data in accordance with ISO 27001 Information Security Management System protocols.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

7. **With information security in mind, what kind of mitigation actions have you planned in case of emergency?**
   - All kinds of data processed in our information security system, in accordance with the quality assurance system, "Emergency Plan" has been created within the scope of ISO 27001. In this context, the inspection and control mechanism is operated by reviewing the annual Exercises and possible scenarios.

8. **What cascading effects may take place if an information asset of yours is affected?**
   - Risk Management Procedure was created within the scope of ISO 27001. This procedure is controlled by the IT department.

9. **What would be the highest expected cost for recovery after an incident? Please provide a short justification of the cost.**
   - Compensation cases related to third parties are important.
   - There may be "major commercial losses" between information loss and energy trading.

10. **Please add any comments, remarks or additional information that you deem important to mention and was not covered by the questions above.**
    - Within the scope of the project, it may be important that there may be evaluation of legal regulations and site plans that may violate the security policy, especially in the information transfer that will occur between EU countries and non-EU countries.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Risk information tables

Information asset name	Gökçeada WPP 1	**Asset importance**	8
Information asset type	*Electronic Files*	**GDPR sensitive**	NO
Owning Stakeholder	UEDAS	**Stakeholder type**	Win-power Power Plant
Identified risk	WPP1 DATA	**Likelihood**	5
Risk's origin	*intentional or unintentional human intervention,*	**Impact severeness**	6
Risk description	Energy production data can be used for pricing policy and commercial benefits. It is also important for reactive energy control service. The data in this context is not made available to third parties.		
Expected consequences	No major problems expected		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

Information asset name	Gökçeada WPP 2	**Asset importance**	8
Information asset type	*Electronic Files*	**GDPR sensitive**	NO
Owning Stakeholder	UEDAS	**Stakeholder type**	Win-power Power Plant
Identified risk	WPP2 DATA	**Likelihood**	5

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Risk's origin	*intentional or unintentional human intervention,*	**Impact severeness**	6
Risk description	Energy production data can be used for pricing policy and commercial benefits. It is also important for reactive energy control service. The data in this context is not made available to third parties.		
Expected consequences	No major problems expected		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

Information asset name	Gökçeada SPP 1	**Asset importance**	8
Information asset type	*Electronic Files*	**GDPR sensitive**	NO
Owning Stakeholder	UEDAS	**Stakeholder type**	Solar-power Power Plant
Identified risk	SPP1 DATA	**Likelihood**	7
Risk's origin	*intentional or unintentional human intervention,*	**Impact severeness**	6
Risk description	Energy production data can be used for pricing policy and commercial benefits. It is also important for reactive energy control service. The data in this context is not made available to third parties.		
Expected consequences	No major problems expected		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Information asset name	Gökçeada ESS1	**Asset importance**	4
Information asset type	*Electronic Files*	**GDPR sensitive**	NO
Owning Stakeholder	UEDAS	**Stakeholder type**	Energ Storage System
Identified risk	EES1 DATA	**Likelihood**	8
Risk's origin	*intentional or unintentional human intervention,*	**Impact severeness**	3
Risk description	The load values of the energy storage system may be important if it can be used for a commercial purpose. As there are emerging technologies, it is possible for manufacturers for development purposes to need energy charge-discharge data.		
Expected consequences	No major problems expected		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

Information asset name	Gökçeada Feeder	**Asset importance**	2
Information asset type	*Electronic Files*	**GDPR sensitive**	NO
Owning Stakeholder	UEDAS	**Stakeholder type**	TSO
Identified risk	Feeder 1	**Likelihood**	4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Risk's origin	*intentional or unintentional human intervention,*	**Impact severeness**	2
Risk description	Network structure is important in terms of security measures.		
Expected consequences	No major problems expected		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

Information asset name	Gökçeada GIS	**Asset importance**	8
Information asset type	*Electronic Files*	**GDPR sensitive**	NO
Owning Stakeholder	UEDAS	**Stakeholder type**	Utility Grid
Identified risk	ISLAND 1 Map	**Likelihood**	6
Risk's origin	*malicious acts*	**Impact severeness**	8
Risk description	Network structure is important in terms of security measures.		
Expected consequences	This is important issue. Should not be shared with third parties		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

Information asset name	Gökçeada Customer	**Asset importance**	8
Information asset type	*Electronic Files*	**GDPR sensitive**	NO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Owning Stakeholder	UEDAS	**Stakeholder type**	Consumer
Identified risk	Customer list	**Likelihood**	4
Risk's origin	*commercial benefit, customer services*	**Impact severeness**	4
Risk description	It is vulnerable to abuse by companies seeking commercial benefits.		
Expected consequences	This is important issue. Should not be shared with third parties		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

Information asset name	Gökçeada Consumer	**Asset importance**	8
Information asset type	*Electronic Files*	**GDPR sensitive**	NO
Owning Stakeholder	UEDAS	**Stakeholder type**	Consumer
Identified risk	Consumer data	**Likelihood**	4
Risk's origin	*commercial benefit, customer services*	**Impact severeness**	4
Risk description	It is vulnerable to abuse by companies seeking commercial benefits.		
Expected consequences	This is important issue. Should not be shared with third parties		
Mitigating stakeholder	The stakeholder responsible for the security policies in the project should take the necessary measures.		
Solution / mitigation actions	We can stop to share or VPN connection if any problem		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ANNEX C: PARTNER-FILLED QUESTIONNAIRES FOR M24 ASSESSMENT

Not applicable at this stage of VPP4Islands project development stage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ANNEX D: PARTNER-FILLED QUESTIONNAIRES FOR M36 ASSESSMENT

Not applicable at this stage of VPP4Islands project development stage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ANNEX E: PARTNER-FILLED QUESTIONNAIRES FOR M42 ASSESSMENT

Not applicable at this stage of VPP4Islands project development stage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

ANNEX F: MATERIAL FOR FUTURE REVISIONS

1. POTENTIAL RISKS THAT MAY ARISE, PER STAKEHOLDER TYPE

The following table is aimed to be incorporated in a subsequent revision of this report (M36 or M42), paragraph #2.2

Stakeholder Type	Risk name / description	Information asset type	Probability	Impact
Conventional Power Plant				
Solar-power Power Plant				
Wind-power Power Plant				
ESS / VESS				
Utility Grid				
Distribution System Operators (DSO)				

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

Transmission System Operators (TSO)				
Meteorological Data Providers				
Consumers				
// other //				

2. Other Information Asset Tables for Risk Identification

This section contains information assets tables for the Risk Identification paragraph, that were not filled until this iteration of the document.

Hard Copies

Hard Copy name	Risk name / description	Potential consequences	Associated partner or stakeholder
n/a	-	-	-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

PORTABLE DEVICES

Portable Device name	Risk name / description	Potential consequences	Associated partner or stakeholder
n/a	-	-	-

REMOVABLE MEDIA

Removable Media name	Risk name / description	Potential consequences	Associated partner or stakeholder
n/a	-	-	-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

3. Other Information Asset Tables for Risk Analysis

This section contains information assets tables for the Risk Analysis paragraph, that were not filled until this iteration of the document.

Hard Copies

Hard Copy type / name	Risk name / description	Asset's importance	Likelihood	Impact severeness	Mitigating stakeholder
n/a	-		-	-	-

Portable Devices

Portable Device type / role	Risk name / description	Asset's importance	Likelihood	Impact severeness	Mitigating stakeholder
n/a	-	-	-	-	-

Removable Media

Removable Media type / role	Risk name / description	Asset's importance	Likelihood	Impact severeness	Mitigating stakeholder
n/a	-	-	-	-	-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852

8. REFERENCES

[1] International Standards Organization (ISO), "Risk Managment: ISO 31000 [ebook]," International Standards Organization, 2018.

[2] Wikipedia contributors, "Project risk management," Wikipedia, The Free Encyclopedia.

[3] M. Rausand and S. Haugen, Risk Assessment: Theory, Methods, and Applications (ISBN: 978-1-119-37723-8), John Wiley & Sons, 2020.

[4] D. Hubbard, The Failure of Risk Management: Why It's Broken and How to Fix It, John Wiley & Sons, 2009.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement n°957852