PLUG-N-HARVEST

Plug-n-play passive and active multi-modal energy Harvesting systems, circular economy by design, with high replicability for Self-sufficient Districts & Near-Zero Buildings

768735, H2020-EEB-2017

Deliverable D7.2.2:

Risk Assessment

Deliverable Version:	D7.2.2, v.1.0
Document Identifier:	d7.2.2_risk_assesment_v1.0
Preparation Date:	March 20, 2018
Document Status:	Final
Author(s):	Kyriaki Alexandridou, Christos Ravanis, Iakovos Michailidis, Elias Kosmatopoulos
Dissemination Level:	PU - Public

Project funded by the European Union in the H2020 Framework Programme

H2020-EEB-07-2017 - Integration of energy harvesting at building and district level

Deliverable SUMMARY SHEET

Deliverable Details	
Type of Document:	Deliverable
Document Reference #:	D7.2.2
Title:	Risk Assessment
Version Number:	1.0
Preparation Date:	March 20, 2018
Delivery Date:	February 28, 2018
Author(s):	Kyriaki Alexandridou, Christos Ravanis, Iakovos Michailidis, Elias Kosmatopoulos
Document Identifier:	d7.2.2_risk_assesment_v1.0
Document Status:	Final
Dissemination Level:	PU - Public

Project Details	
Project Acronym:	PLUG-N-HARVEST
Project Title:	Plug-n-play passive and active multi-modal energy Harvesting systems, circular economy by design, with high replicability for Self-sufficient Districts & Near-Zero Buildings
Project Number:	768735
Call Identifier:	H2020-EEB-2017
Call Theme:	**Integration of energy harvesting at building and district level**
Project Coordinator:	Centre for Research and Technology Hellas (CERTH)
Participating Partners:	CERTH – Centre for Research and Technology Hellas – Greece RWTH – RWTH Aachen University – Germany CU - Cardiff University – United Kingdom ALUMIL – Alumil Aluminium Industry S.A. – Greece AIGUASOL – Sistems Avancats d' Energia Solar Termica SCCL – Spain ODINS – Odin Solutions S.L – Spain SIE – Siemens SLR – Romania ETRA – Etra Investigacion y Desarrollo S.A. – Spain ET – Energy Transitions Limited – United Kingdom EIG – Eco Intelligent Growth – Spain AHC – Agencia de l'Habitatge de Catalunya – Spain RWM – Region of Western Macedonia – Greece

	CCC – County Council of the City and County of Cardiff – United Kingdom
Instrument:	
Contract Start Date:	September 1, 2017
Duration:	51 Months

Deliverable D7.2.2: Short Description
Risk Assessment along with detailed Contingency Planning are provided for the technical and scientific results and other objectives of the project. The Expanded Failure Modes and Effects Analysis (EFMEA) technique is chosen to meet the needs of PLUG-N-HARVEST after having taken into account the evaluation in the literature among Risk Analysis Methods in research environments and considering PLUG-N-HARVEST needs. The technique is thoroughly described introducing variables such as Severity (S), Occurrence (O), Detectability (D) and Recoverability (R) for each risk.
Keywords: Risk Assessment, Project Management, PLUG-N-HARVEST, EFMEA

Deliverable D7.2.2: Revision History			
Version:	**Date:**	**Status:**	**Comments**
0.1	02/03/2018	Draft	Structure by Kyriaki Alexandridou, Christos Ravanis, Iakovos Michailidis, Elias Kosmatopoulos
0.5	09/03/2018	Draft	1st complete version available according to DoA
0.6	15/03/2018	Draft	Inputs by AIGUASOL
0.7	16/03/2018	Draft	Inputs by ETRA and CCC
0.8	19/03/2018	Draft	Inputs by EIG, CU and AHC
0.9	20/03/2018	Draft	Inputs by RWTH and CERTH
1.0	20/03/2018	Final	Final version by Kyriaki Alexandridou, Christos Ravanis, Iakovos Michailidis, Elias Kosmatopoulos

Table of Contents

List of Figures

List of Tables

List of definitions & abbreviations

Abbreviation	Definition
ADO	Administration Office
DoA	Description of Action
EAB	Ethical Advisory Board
ERA	European Research Area
FTP	File Transfer Protocol
ICT	Information and Communication Technologies
IPR	Intellectual Property Rights
PB	Plenary Board
QAM	Quality Assurance Manager
QCB	Quality Control Board
QMR	Quarterly Management Report
QP	Quality Plan
PO	Project Office
PC	Project Coordinator
S&T	Scientific and Technical
SAB	Scientific Advisory Board
SC	Steering Committee
STREP	Specific Targeted Research Project
SVN	Subversion

Executive Summary

This document is the deliverable "D7.5 – Risk Assessment Plan" of the PLUG-N-HARVEST project that is funded by the European Commission under its Horizon 2020 Research and Innovation Programme (H2020). The deliverable gives an overview and documentation of the risk assessment in the project. The document constitutes the prime reference point for Risk Assessment procedures of the PLUG-N-HARVEST project. It is strongly emphasized that this is an ongoing document that is being evolved along with the project progress and will be regularly updated to reflect up-to-date information.

Risk Assessment along with detailed Contingency Planning are provided for the technical and scientific results and other objectives of the project. The Expanded Failure Modes and Effects Analysis (EFMEA) technique is chosen to meet the needs of PLUG-N-HARVEST after having taken into account the evaluation in the literature among Risk Analysis Methods in research environments and considering PLUG-N-HARVEST needs. The technique is thoroughly described introducing variables such as Severity (S), Occurrence (O), Detectability (D) and Recoverability (R) for each risk.

Detailed tables are presented containing all identified risks, classified into categories highlighting the most critical of them, i.e. the ones which could have a clear impact on the project and its completion. Mitigation plans are defined for all risks and a total risk estimate is calculated for the whole project both before and after taking them into account. The final results of risk analysis indicate that PLUG-N-HARVEST is not a risky project.

Finally, the identification of risks explained at the Risk Register document will be examined thoroughly throughout the project lifetime. All partners are responsible to report risks they perceive, comment on existing ones and suggest appropriate mitigation actions through the Project Board.

1 Introduction

The main scope and objective of this document is the project's Risk Assessment plan, which describes:

- unknown weaknesses and vulnerabilities of a project, prioritizing their impact and implementing proper security controls and countermeasures to mitigate them
- the tools and the techniques that are applied to monitor and track those events that have the potential to impact the outcome of a project.
- the quality control of the whole project, including the peer-reviewing evaluation of project's deliverables

Risk management is an ongoing process that continues through the life of a project. It includes processes for risk management planning, identification, analysis, monitoring and control. Many of these processes are updated throughout the project lifecycle as new risks can be identified at any time. It is an objective of risk management to decrease the probability and impact of events adverse to the project. On the other hand, any event that could have a positive impact should be exploited.

2 Risk assessment & Contingency Plan

2.1 Introduction

Risk Assessment is a core element in the research domain. Various opportunities and risks exist in every project providing a complex and often inter-related mix that researches have to address. A Risk Assessment is a process[1] that commences with hazard identification and analysis, through which the probable severity of harm or damage is established, followed by an estimate of the probability of the incident or exposure occurring, and concluding with a statement of risk. The Assessment should include the controls required to eliminate, reduce or minimise the risks.

This section presents the proposed contingency plans and actions to deal with the potential risks during the implementation of the PLUG-N-HARVEST framework. An overview of the method chosen to identify and estimate the severity of the risks is presented (EFMEA). Following, a list of risks is exhibited, resulting after a thorough investigation and contribution from all partners.

To conclude, it is necessary to underline the fact that Risk Assessment is an ongoing process throughout the PLUG-N-HARVEST project. As such, it will be in progress until the end of the project and the Risk Register that is described below will be continuously updated. Finally, it should be mentioned that it is not possible to eliminate the probability of a risk to occur. However, it is possible to be properly prepared in order to cope with it according to the respective contingency plan and minimize its impact on the project.

2.2 Risk Management Plan

A five stage Risk Management Plan has been adopted for the needs of PLUG-N-HARVEST including: Risk Identification, Risk Quantification, Risk Response Development, Risk Monitoring and Control, and Risk Documentation:

- **Risk Identification** examines the risks that can affect the project documenting the characteristics of each one.
- **Risk Quantification** involves the evaluation of risks by determining the interactions, relationships and implications to the project, identifying probabilities of occurrence and assessing the possible effects.
- **Risk Response Development** involves the management of risks by determining prevention and response strategies plan, project reserves and mitigation strategies.
- **Risk Monitoring and Control** involves controlling risks, making decisions on how to handle each situation, and take corrective actions. The main products are a risk registry, corrective actions and updates to the risk management plan.
- **Risk Documentation** contains the project database development for collecting historical information on the risks encountered.

For the first three stages a formal Risk Analysis and Assessment method is needed. Currently, over 100 Risk Analysis techniques are available in the literature. The most common traits of them are the identification of initiating events (causes), consequences, safeguards, and recommendations. The alternative techniques have been reviewed and an analysis is included in Section 3 explaining that "Expanded Failure Modes and Effects Analysis" (EFMEA) will be used.

2.3 Choice of the FMEA Technique to Be Used

There are several well established FMEA techniques that differ in the way they identify causes or consequences. The five most popular techniques[2] are "Hazard and Operability studies" (HAZOP), "Failure Modes and Effects Analysis" (FMEA) or "Failure Mode, Effects and Critically Analysis" (FMECA), "Expanded Failure Modes and Effects Analysis" (EFMEA), "What if" and "Risk Assessment Decision Matrix Analysis" (RADM). These methods are briefly described below:

2.3.1 Hazard and Operability Studies (HAZOP)

HAZOP[3] is a systematic way to identify possible hazards in a work process. In this approach, the process is broken down into steps, and every variation in work parameters is considered for each

step, to see what could go wrong. HAZOP's meticulous approach is commonly used with chemical production and piping systems, where miles of pipes and numerous containers can cause logistical headaches. According to HAZOP, normal and standard operations are safe and hazards occur only when there is a deviation from the normal operation. The intention of performing a HAZOP is to review the design to pick up design and engineering issues that may otherwise not have been found. The technique is based on breaking the overall complex design of the process into a number of simpler sections called 'nodes' which are then individually reviewed.

2.3.2 Failure Modes and Effects Analysis (FMEA / FMECA)

FMEA[4,5,6] is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, a product or a service. It evaluates the effects of potential failure modes of subsystems, assemblies, components and functions using design and failure knowledge as inputs.

"Failure modes" means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential or actual.

"Effects analysis" refers to studying the consequences of those failures. Its concept is based on the following questions: What can fail? How does it fail? How frequently will it fail? What are the effects of the failure? What is the reliability/ safety consequence of the failure?

2.3.3 Expanded Failure Modes and Effects Analysis (EFMEA)

EFMEA[7] has been designed in order to overcome some of the FMEA limitations[8]. This method provides information to identify critical elements of the overall system, evaluate suitable actions and mitigation strategies, with the overarching goal of contributing to the contingency plans of the project. In EFMEA risk analysis is conducted in two stages: Risk Identification and Risk Mitigation. Also, EFMEA classifies Risks into four categories:

- Technical (physical features of hardware; coding elements of software)
- Legal (based upon existing policies and laws in each nation)
- Behavioural (resulting from user's behaviour)
- Organisational (in relation to disaster mitigation plans and actor's roles).

2.3.4 What-if Analysis

What-if is an inductive method[9] similar to *HAZOP* (although much less systematic and more intuitive). It is actually a brainstorming approach in which a group of experienced people familiar with the subject process raise the question "what-if" instead of using keywords when examining the P&ID (Piping and Instrumentation Diagram) of the system and voice concerns about possible undesired events.

2.3.5 Risk Assessment Decision Matrix Analysis (RADM)

The *RADM* is a technique[10] which uses a graphic representation of the severity or damage of an accident and its occurrence probability. It provides a quick view of risk ranking in different process hazard analysis (e.g. *HAZOP*).

2.3.6 Conclusion

EFMEA has been selected as the best and most suitable approach to meet the needs of PLUG-N-HARVEST after having taken into account the inputs and outputs of each method, the advantages and disadvantages, as well as the evaluation in the literature among Risk Analysis Methods in research environments[10]. EFMEA is a detailed, rigorous method, relatively inexpensive, which accepts a high degree of complexity and is commonly used in a variety of industries for Risk Management, where simple quantification of risk is insufficient, and where identification of root causes of risks and means of mitigation are paramount.

In EFMEA[11], results can be correlated directly with actual risks and the effect of various methods of mitigation/detection on risk can be easily modelled. Moreover, it provides a well-documented record of improvements from the corrective actions implemented as well as useful information in developing test programs and in-line monitoring criteria. It also provides historical information, which is useful in analysing potential failures during the project lifecycle.

2.4 Identification of Risks – Risk Register

The Risk Register is a key document for the management of the PLUG-N-HARVEST project. It can be viewed by project managers as a management tool for monitoring the risk management processes within the project and is used to identify, assess and manage risks down to acceptable levels through a review and updating process. The purpose of a Risk Register is to record the details of all risks that have been identified along with their analysis and plans for how those risks will be treated.

The Risk Register should be maintained to allow the project to identify and manage risk, tracking its mitigation as work proceeds. All risks that are identified from the beginning of the project, their grading in terms of area of expertise, their level of risk, impact on WPs and respective mitigating plans are contained in the Risk Register as well as it ensures the communication of risk management issues to key stakeholders. The Risk Register of PLUG-N-HARVEST project will be stored and maintained on the consortium cloud repository (hosted by the coordinator using SCIEBO) and can be found in the following directory:

\Sciebo\Plug-N-Harvest\WP7\Auxiliary Documents\

The process for identifying and reporting risks is as follows:

In case a risk becomes harmful for the project's work, the members of the consortium are obligated to underline this issue and **immediately** report it to the WP leader(s) and then to the PC and management board via the Project Office (PO). Then, the Risk Register will be updated by the PO to record this new risk.

1. At the half-yearly General Assembly meetings, the risks and mitigation plans are discussed with all partners. Additional risk may be identified during these discussions and should be captured.
2. The WP leaders and the management board will discuss, together with the persons involved, a contingency plan that mitigates the risk. The level of detail of the contingency plan depends on the likelihood and significance of the risk.
    a. If a risk is unlikely, the management board will just add some possible options: the more likely a risk becomes, the more detailed the contingency plans will be made.
    b. In case a risk seems to be very likely, a detailed contingency plan will be established as required.

The updates will be communicated in the half-yearly periodic reporting deliverables.

2.5 The Risk Register Format

The Risk Register contains a number of columns under which each risk is analysed individually. The Risk Register has been created in Excel, which allows the order and grouping of the risks according to the information in any of the columns. These columns are:

- **Risk identification number:** This is a simple serial number. The order of the risks is simply the order in which the risk was added to the list.
- **The type of risk:** The following types have been identified:
    - General
    - Technological
    - Organizational
    - Behavioural

    - Ethical
- **Work-packages** affected by the risk
- **Risk Event:** the definition of what might go wrong, and how this might be caused.
- **Origin:** this records how the risk was identified: this may be the name of an individual or a partner, or it may be an output from a project meeting. The initial items in the Risk Register are those that were included in the project proposal, where the Origin is shown as Prop.
- **S, O, D, R:** S = Severity, O = Occurrence, D = Detectability, R = Recoverability as analysed in Section 2.7
- **RPN:** Risk Priority Number described in Section 2.7.
- **Mitigation Action Plan:** specific steps that will be taken to ensure that the probability and impact of occurrence will be minimised.
- **Mitigation Action Feasibility:** Describes to what extend the Mitigation action is able to reduce the impact of a risk event. *Low=5, High=1*
- **Status:** whether the proposed mitigation has been put in place, and indeed recording if a risk event does occur.

2.6 Use of the Risk Register

Risks should be added to the Risk Register, by the PO, as and when members of the consortium identify and report a new risk, based on (Expanded) FMEA described in Section 2.7.

The Risk Register will be reviewed at each plenary project meeting in order to check:

- That each risk and its impact has been understood.
- That everyone is aware of the potential impact on their work.
- That an appropriate mitigation plan has been developed and is being acted upon.
- That everyone is aware of what they need to do to mitigate the risks.

2.7 Expanded Failure Modes and Effects Analysis

This section presents the methodology of the Expanded Failure Modes and Effects Analysis method. Initially, a brief description of the classic FMEA will be provided.

FMEA is a qualitative and systematic tool, to help practitioners anticipate what might go wrong with a product or process. In addition to identify how a product or process might fail and the effects of that failure, FMEA also helps to find the possible causes of failures and the likelihood of failures being detected before occurrence through recommended actions or compensation provisions.

Used across many industries, FMEA is one of the best ways to analyze potential reliability problems early in the development cycle, making it easier for manufacturers to take quick action and mitigate failure. The ability to anticipate issues early, allows practitioners to design out failures and design in reliable, safe and customer-pleasing features.

The FMEA determines, by failure mode analysis, the effect of each failure and identifies single failure points that are critical. It may also rank failure according to the criticality of a failure effect and its probability of occurring. This course of action, if succeeded, helps to identify potential failure modes based on past experience with similar products or processes, enabling those failures to be designed out of the system, with the minimum of effort and resource expenditure, thereby reducing development time and costs. Some definitions are given below:

Failure Modes are the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential or actual.

Effect Analysis refers to studying the consequences of those failures and can help potential mitigation processes.

Failure Modes Effects Analysis is used:

- When a process, product or service is being designed or redesigned, after quality function development.
- When an existing process, product or service is being applied in a new way.
- Before developing control plans for a new or modified process.
- When improvement goals are planned for an existing process, product or service.
- When analyzing failures of an existing process, product or service.
- Periodically throughout the life of the process, product or service

According to the seriousness of the consequences, the frequency of occurrence and their detectability, failures are prioritized. The combination of these three factors gives the Risk Priority Number (RPN)[12] for each failure mode identified in the system. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones. This procedure is depicted in Figure 1.

Figure 1. FMEA Process Cycle

FMEA is a popular and broadly accepted methodology for Risk Analysis, which has been adopted by various projects. However, it has been criticized for having a number of limitations throughout the various calculations steps, such as tediousness, missing key failures and inability to affect key process decisions if performed too late. Expanded FMEA (EFMEA) designed to overcome some of the FMEA limitations, is being used within the scope of PLUG-N-HARVEST. In Section 3 is described how the EFMEA matches the needs of PLUG-N-HARVEST.

2.7.1 Calculation of Risk Priority Numbers

Risk Priority Number (RPN) is a measure used when assessing risk to help identify critical failure modes associated with the design or process. The **RPN** values range from 1 (absolute best) to 1,000 (absolute worst).

Such an analysis involves various factors of each safety-security issue: severity, occurrence probability, detectability and recoverability, not only for technical risks, but also for behavioural, legal and organizational risks. Severity, rates the severity of the potential effect of the failure, occurrence rates the likelihood that the failure will occur and detection which rates the likelihood that the problem will be detected before it reaches the end-user/customer.

Behavioural risks are related to the users' behaviour, regarding their interaction with the system, concentrating on the possible wrong moves or reactions they might perform. Legal risks include the risks that will arise if the system is not compliant with the legislation of the country. Finally, organizational risks refer to the organizational structure of the service chain, while technical risks are related to project-level technical concerns.

The Risk Priority Number (for each risk) is calculated by Equation 1:

$$RPN = S \times O \times \frac{D + R}{2} \quad (Eq.\ 1)$$

where S = Severity, O = Occurrence, D = Detectability, R = Recoverability

Whilst many (E)FMEA are carried out by a team of experts, it is important to understand that the PLUG-N-HARVEST consortium consists of partners from different countries working independently and so ways of achieving consistent results from all partners are required. The following checklist of 10 key points based upon the question "*What can go wrong?*" has been developed by *Bluvband and Grabov*[8] to assist individuals in identifying possible Failure Modes:

1. The intended function is not performed
2. The intended function is performed, but there are some safety problems, or a problem in meeting a regulation associated with the intended function performance
3. The intended function is performed, but at a wrong time (availability problems)
4. The intended function is performed, but in the wrong place (position in the system)
5. The intended function is performed, but in the wrong way (efficiency problems)
6. The intended function is performed, but the performance level is lower than expected
7. The intended function is performed, but its cost is higher than planned (additional maintenance, repair, power consumption etc.)
8. An unintended/unplanned and/or undesirable function is performed
9. The period of intended function performance (lifetime) is lower than planned (reliability issues)
10. Support for the intended function performance is impossible or problematic (maintenance, repair, service issues etc.)

Based on the overall approach, the following tables have been developed to assist in identifying the level of each risk and the value that should be assigned in the RPN calculation.

Table 1. Severity (S) level analysis

Level of severity	Technical issue	Behavioural issue	Legal issues	Organisational issues
9-10 (extremely severe)	The failure could put user safety at risk, potentially causing injury or fatality	The user error in operating the system could lead to an incident	Are there laws in each country that do not allow the system to be implemented?	Wide and different organizational framework is needed, that is

		worseness (i.e. safety effects)		completely missing (i.e. new services)
7-8 **(severe)**	The failure implies the total loss of the system functions, resulting in user's dissatisfaction	User behavioural error may abort the system benefits (i.e. safety effects due to changes in ways of acquiring info)	New laws are required for system implementation and no relevant work has been performed yet	Organisational framework adaptation is needed (some initial actions have been taken on this domain)
5-6 **(slightly severe)**	The failure implies the partial loss of the system function, resulting in user's dissatisfaction	User's behavioural changes may significantly reduce the positive effects of the system	New laws are required for system implementation and work required has already been performed	Organizational framework adaptation is needed which has already started being realised
3-4 (significant)	The failure implies slight dissatisfaction to the user	User's behavioural changes may somehow influence the positive effects of the system	New laws are required for system implementation but consensus on them exist	There is a need for limited and easily realized organizational changes
1-2 (insignificant)	The failure does not imply perceptible effects to the system function and to the user's satisfaction	User's behaviour is not expected to reduce the system benefits significantly, or may even further enhance them	No new laws are required for implementation	There is no need at all for organizational changes

Table 2. Occurrence (O) level analysis

Occurrence level	Technical issue	Behavioural issue	Legal issues	Organisational issue
9-10 **(high)**	It is certain that some failures will sometimes occur	It is certain that some behavioural effects will occur (by the system users)	It is certain that some legal problems will occur	It is certain that there will be a need for organizational restructuring
6-8 **(medium)**	A failure could occasionally occur	Some behavioural effects could occasionally occur	Some legal problems could occasionally occur	A need for organizational restructuring could occasionally occur (depending on the needs of the service, that will arise after the operation of the system)
3-5 **(low)**	There is only a slight probability that an	There is only a slight probability that some	There is only a slight probability that some	There is only a slight probability that a need for organizational

	error/failure will occur	behavioural effects will occur	legal problems will occur	restructuring will occur
1-2 (improbable)	It is unlikely that a fault will occur	It is unlikely that some behavioural effects will occur	It is unlikely that some legal problems will occur	It is unlikely that a need for organizational restructuring will occur

Table 3. Detectability (D) level analysis

Detectability level	Technical issue	Behavioural issue	Legal issue	Organisational issue
9-10 (improbable)	It is impossible or improbable that a problematic area will be detected	It is impossible or improbable that a user's behavioural effect will be detected	It is impossible or improbable that a legal problem will be detected	It is impossible or improbable that an organizational problem will be detected
7-8 (slight)	The problematic area is detected only in particular cases	The user's behavioural effect is detected only in particular cases	The legal problem is detected only in particular cases	The organizational problem is detected only in particular cases
5-6 (moderate)	It is probable that the problem will be detected (depending on the situation)	It is probable that the user's behavioural effect will be detected	It is probable that the legal problem will be detected	It is probable that the organizational problem will be detected
3-4 (high)	It is very probable that a problem will be detected	It is very probable that the user's behavioural effect will be detected	It is very probable that the legal problem will be detected	It is very probable that the organizational problem will be detected
1-2 (very high)	It is certain that a problem will be detected	It is certain that the user's behavioural effect will be detected	It is certain that the legal problem will be detected	It is certain that the organizational problem will be detected

Table 4. Recoverability (R) level analysis

Recoverability level	Technical issue	Behavioural issue	Legal issues	Organisational issues
9-10 (null)	No recovery action is provided	System is (in)flexible to user's behavioural effects	System is either accepted or rejected by the legal framework	System requires a fixed organizational environment to operate
6-8 (low)	The user is only advised on the failure	Behavioural effects are taken into account by the system	System may be slightly adapted to	System requires a fixed organizational

			meet legal restrictions	framework with limited adaptations
3-5 **(high)**	Effective recovery action is provided	System customization might compensate for user's behavioural effects	System encompasses different versions to meet particular legal demands	System may operate within various organizational frameworks
1-2 **(full recoverability)**	The failure effect is completely avoided by the recovery action	System does not allow user's behavioural effects	System is easily reconfigurable to meet legal demands	System does not require organizational changes

Using the values in the above tables, the appropriate RPN must be calculated for each identified risk item in the PLUG-N-HARVEST system.

2.7.2 Identification of Total Risk Estimate and Critical Items

The calculation of the RPN for each item can highlight potentially problematic areas in which the developers are required to put more effort in to resolve (i.e. to offer mitigation strategies). Results should reveal the most problematic areas, and the highest RPNs should get highest priority for corrective measures. These measures can include a variety of actions: new inspections, tests or procedures, design changes, different components, added redundancy, modified limits, etc. The value of each individual RPN calculated above is initially matched to five levels of severity, as defined in the following table (values are indicative only):

Table 5. Correlation of Overall risk factor with overall risk severity level

Calculated RPN	Overall severity
512-1000	I - Extremely severe
216-512	II - Severe
64-216	III - Moderate
8-64	IV - Slight
1-8	V - Insignificant

It is also useful to calculate the Total Risk Estimate (TRE) (Equation 2) for the overall project, as proposed by *Bluvband and Grabov* (2009)[8]:

$$TRE = \frac{\sum_{i=1}^{n} RPN_i}{1000n} \times 100\% \qquad (Eq.\ 2)$$

Where: RPN_i : individual RPN values for each item

n: total number of items in the EFMEA analysis.

TRE values range between 0.1% (no risk at all) and 100% (extremely risky), but it is unlikely that either of these extreme values will be obtained. *Bluvband and Grabov*[8] suggest that any

TRE>17% indicates a '**risky'** project as this is where the individual T/B/L/ORPN values are 5.5 i.e. the middle of the 1 to 10 scale used in the tables, or higher.

The next step is to attempt to prioritise the risks in order of their criticality. It is important to not adhere to pre-specified thresholds (e.g. RPN >= *X),* as too low a threshold can lead to substantial corrective work, some of which may not be required. Selecting a top 10, or the highest 5% can also be problematic, and so all items are to be ordered in a list, from the highest RPN to the lowest RPN and then plotted as a 'screen plot' (see Figure 2 below). The uppermost values (i.e. those not on the lower trend line) are marked and potential mitigation strategies for these specific items are then determined.

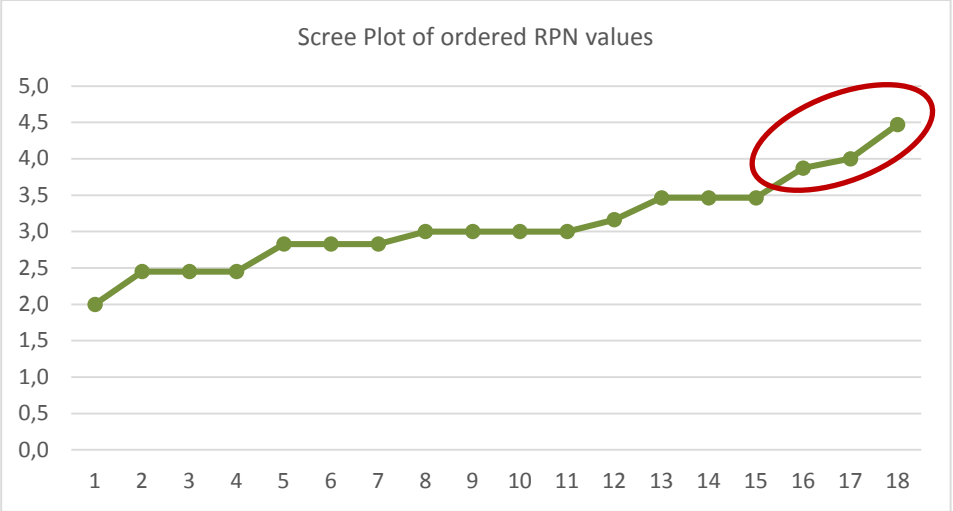

Figure 2. Example of Scree Plot Analysis of RPN Values

2.7.3 Corrective actions

Once the critical items have been identified, the next step is to attempt to identify possible corrective actions or mitigating strategies. The possible success of these actions/strategies should also be identified and, where possible, quantified. There may be several possible options for each issue, and any risk reduction is an iterative process involving dependencies between the different issues.

In terms of corrective actions, risk can be reduced in a number of generic ways:

- reducing the magnitude (severity) of the consequences of the potential risk;
- reducing the probability of the risk occurring;
- increasing failure detection speed and probability;
- protecting against the risk, mitigating strategies to compensate for a failure;
- transferring the risk to another Party.

Traditional FMEA does not issue adequate guidance for selecting the optimal choice of corrective action, as actions required to lower existing RPN values may not be appropriate, achievable or feasible under project constraints (time, resource, budget etc.) Therefore, *Bluvband and Grabov (2009)*[8] proposed a comparison evaluation of each pre- and post-correction RPN, also taking into account the 'feasibility' of each action. The 'feasibility' of each action is ranked on a scale from 1 (Best Case) to 10 (Worst Case), using the following guidelines:

Table 6. Feasibility of Corrective Actions

Feasibility of Corrective Action Implementation	Ranking
Safety problem and/or non-compliance to Government regulations	10

Unavailable necessary resources Unacceptable cost/time/resource consumption Zero chance of success 100% probability of undesirable impact	
Very remote availability of necessary resources Almost unacceptable cost/time/resource consumption Very low chance of success; ~90% probability of undesirable impact	9
Remote availability of necessary resources; Near unacceptable cost/time/resource consumption; Remote chance of success; ~80% probability of undesirable impact	8
Very low availability of necessary resources Very high cost/time/resource consumption Very low chance of success ~70% probability of undesirable impact	7
Low availability of necessary resources High cost/time/resource consumption Low chance of success ~60% probability of undesirable impact	6
Rather low availability of necessary resources Relatively high cost/time/resource consumption Rather low chance of success ~50% probability of undesirable impact	5
Moderate availability of necessary resources Medium cost/time/resource consumption Moderate chance of success ~40% probability of undesirable impact	4
Some availability of necessary resources Rather low cost/time/resource consumption Some chance of success ~30% probability of undesirable impact	3
Good availability of necessary resources Low cost/time/resource consumption Good chance of success ~20% probability of undesirable impact	2
Full availability of necessary resources Very low cost/time/resource consumption High chance of success 0-10% probability of undesirable impact	1

Once the pre- and post-correction RPN, and the feasibility rank have been determined for each item, Equation 3 is used to identify the most suitable action(s) to apply:

$$\frac{RPN_{iBefore} - RPN_{iAfter}}{F_i} = \frac{\Delta RPN_i}{F_i} \qquad (Eq.\ 3)$$

Where: $RPN_{iBefore}$ = pre-correction RPN value;

RPN_{iAfter} = post-correction RPN value;

F_i = Feasibility Rank (from the table).

The corrective action with the **largest** value of [$\Delta RPN_i/F_i$] is the one that can be said to be most suitable or preferable to implement.

2.7.4 Evaluation of corrective actions

Once the initial RPNs have been calculated, and the optimal post-correction RPNs have been determined for each item, it is useful to return to the overall project and evaluate the effectiveness of the interactions using a normalised improvement estimate[8]:

$$\Delta RPN = \frac{\sum RPN_{iBefore} - \sum RPN_{iAfter}}{\sum RPN_{iBefore}} \times 100\% \qquad \textit{(Eq. 4)}$$

It has been suggested that a risk reduction of up to 30% can be achieved through the completion of a full EFMEA[8], but this naturally depends on the initial TRE value.

3 PLUG-N-HARVEST (Expanded) Failure Mode and Effect Analysis

3.1 Methodology

In EFMEA, risk analysis is conducted in two stages: Project Risk Identification and Mitigation and Technical Risk Identification and Mitigation. In Risk identification various risks associated with the PLUG-N-HARVEST system were identified and RPN values were calculated for each risk based on the respective severity, occurrence, detectability and recoverability values. In Risk Mitigation, both critical (the ones with the highest RPNs in the scree plot) and non-critical risks were addressed through appropriate mitigation plans.

Tables 7-10 present the major **General, Organizational, Behavioural and Ethical (legal)** identified project risks.

Table 7. Initial General Risks and RPN Calculations

No	Risk Description	Impact to WPs	S	O	D	R	RPN	Risk Level
A. General								
1	Poor Framework Performance during tests resulting to failure of the Trials	WP2, WP3,WP4	6	6	3	4	126	3 - Moderate
2	Poor quality of data to validate the results	WP4	3	4	5	4	54	4 - Slight
3	Cooperation problems between the different components of the PLUG-N-HARVEST	WP4	5	7	7	4	192	3 - Moderate
4	Lack of interest on the PLUG-N-HARVEST project by external stakeholders	WP5	6	3	3	4	63	4 - Slight
5	Lack of interest from End Users in Pilot Sites	WP4	5	6	3	3	90	3 - Moderate
6	Failure to successfully transfer knowledge and experience from business to academia technology providers and vice versa	All	3	5	4	4	60	4 - Slight
7	Pilot tests fail in providing the anticipated results or turn out to be inadequate	WP4	7	6	3	6	189	3 - Moderate

8	Technical results of low quality/relevance to targeted users and market	WP4	6	5	4	5	135	3 - Moderate
9	Requirements are too generic or incomplete	WP1	7	6	3	6	189	3 - Moderate

Table 8. Organizational Risks and RPN Calculations

No	Risk Description	Impact to WPs	S	O	D	R	RPN	Risk Level
	B. Organizational							
1	Consortium has no harmony	WP6	5	5	2	3	63	4 - Slight
2	Partner leaves consortium	WP6	5	6	1	2	45	4 - Slight
3	Key staff illness / leave during critical phase	WP6	5	6	1	2	45	4 - Slight
4	Poor quality of deliverables and delay in meeting the deadlines	WP6	6	4	2	3	60	4 - Slight
5	Budget and resource allocation risks	All	6	5	7	2	135	3- Moderate
6	Unrealistic project time schedule and deadlines	All	6	6	3	5	144	3- Moderate
7	Partner underperforming	All	5	5	2	3	62.5	4 - Slight
8	Relevant events are not falling within the project life span or overlap with important phases of the project, hindering partners to attend	All	3	6	4	3	63	4 - Slight
9	Unanticipated Project Manager workload and Personnel unavailability	All	5	4	3	3	60	4 - Slight

Table 9. Behavioural Risks and RPN Calculations

No	Risk Description	Impact to WPs	S	O	D	R	RPN	Risk Level
	C. Behavioural							
1	Personnel behavioural issues	All	7	4	5	1	84	3 - Moderate

2	The IT – Equipment effects the behaviour and the performance of the personnel	All	6	4	6	5	132	3 - Moderate
3	Disputes over ownership of IPR amongst consortium partners	All	4	3	4	6	60	4 - Slight
4	Breach of IPR conditions within consortium	All	5	3	4	6	75	3 - Moderate
5	Lack of interest on the PLUG-N-HARVEST project by external stakeholders	WP5	6	3	3	4	63	4 - Slight
6	Emerging Competitors	All	5	5	5	6	137	3 - Moderate

Table 10. Ethical Risks and RPN Calculations

No	Risk Description	Impact to WPs	S	O	D	R	RPN	Risk Level
	D. Ethical							
1	Storage and process of occupant-related privacy data towards person localization and extraction of patterns and flows within selected pilot tests.	WP4	6	4	6	6	144	3 - Moderate
2	Difficulties in ensuring the security of shared personal/ private data in the pilot tests.	WP4	5	5	7	5	150	3 - Moderate
3	Difficulty in ensuring the security of human data collected during the execution of the trials.	WP4	7	5	5	5	175	3 - Moderate
4	Lack of Transparency	WP4	6	6	4	4	144	3 - Moderate
5	Delegation of Control Privacy. Incidental Findings	WP4	5	5	4	2	75	3 - Moderate
6	Improper use of IT Equipment	WP4	7	6	3	2	105	3 - Moderate

Based on Tables 7-10 and Equation 2, the Total Risk Estimate value for **project risks** is:

$$TRE = \frac{\sum_{i=1}^{n} RPN_i}{1000n} \times 100\% =$$

TRE = 10.39%

This value is lower than 17%, thus according to *Bluvband and Grabov*[8] it suggests that PLUG-N-HARVEST is not a risky project regarding project risks. However, this value can be further reduced (diminishing even more possible risk effects) if needed and if appropriate mitigation strategies are taken into account, as described below.

Reordering the individual risks by their respective RPN values and plotting them on a scree plot (Figure 3) allows the identification of the RPN threshold. Any risks above this limit are deemed to be critical and require greater attention in their mitigation plans.

As shown in the Figure 3, the threshold for the risks identified in the PLUG-N-HARVEST Risk Assessment is RPN > 250. No risks are over this limit regarding general, ethical, behavioural and organizational ones.

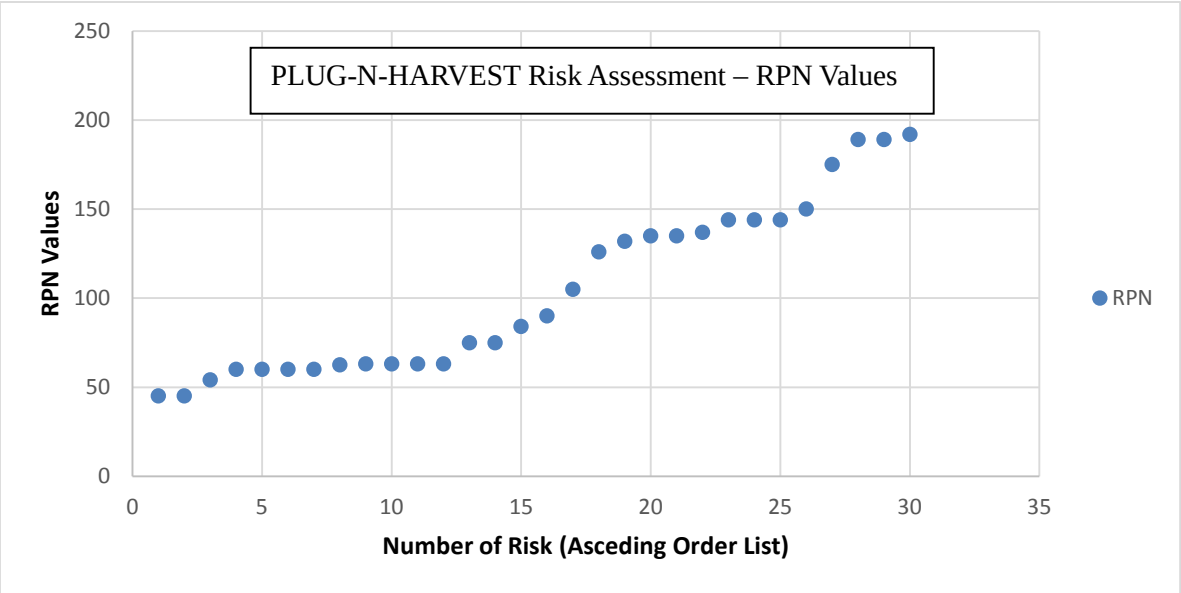

Figure 3. RPN Screen Plot for the PLUG-N-HARVEST Project

3.2 Project Risk Mitigation

Once all the risks had been ranked, the next step is to establish mitigation strategies or contingency plans for each one. Beside the description of the mitigation strategy, a mitigation possibility is also given according to Table 11.

Table 11. Definition of Mitigation Possibility Levels for Assigning to Risk Items

Mitigation Possibility	Definition
High	A solution is available at relatively little cost
Medium	An achievable solution may be possible at reasonable cost, or a reasonable solution is available at modest cost
Low	An expensive solution may be possible, but system benefits may not justify these, and/or a solution needs further investigation or is highly complicated
Improbable	Solutions are too expensive (likely to remain so) in relation to the reduction of risk(s) and the benefits gained from the functionality of the system, and/or a solution is not available for the (extremely) severe risk that has been identified

Applying the various mitigation actions the following mitigation strategies were adopted as possible contingency plans. Table 12 presents mitigation strategies and probabilities for each risk. Critical risk items are highlighted.

Table 12. Mitigation Strategies for General Risk Items

No.	Risk Description	RPN	Severity	Mitigation Strategy	Mitigation Possibility
A. General					
1	Poor Framework Performance during tests resulting to failure of the Trials	126	3-Moderate	All Pilot operators will constantly monitor the pilot's conditions in order for such bad performance problems to be depicted at early stages & an adequate and effective solution to the problem to be provided. Moreover, the system developers will study the reasons of the deterioration in order to find a way to prevent same problems in the future.	Medium
2	Poor quality of data to validate the results	54	4-Slight	Pilot sites have already been carefully selected to ensure that they are suitable for the demonstrations. P-n-H will analyse pilot sites and existing infrastructure so as to guarantee the Use Case Requirements during the pilot execution. In addition, regular remote meetings will be held to check all pilot teams are aligned.	Medium
3	Cooperation problems between the different components of the PLUG-N-HARVEST Framework	192	3-Moderate	Extensive tests will be carried out for all components separately prior to the official testing and their integration to the PLUG-N-HARVEST Framework in order to ensure that they were designed and developed according to the project's needs. In this way the proper cooperation among the different components will be ensured. The care given to interoperability further minimizes the risk of such a situation.	Medium
4	Lack of interest on the PLUG-N-HARVEST project by external stakeholders	63	4-Slight	The Task partners on this part of the project will manage a continuous operation on communication channels in order to keep in touch with multiple stakeholders.	Medium
5	Lack of interest from End Users in Pilot Sites	90	3-Moderate	The Pilot Site partners are responsible for raising early in the project End Users awareness for PLUG-N-HARVEST concept and objectives and informing them about how they could contribute during the pilot procedure. To mitigate this risk PLUG-N-HARVEST will use corroborating sources of evidence in order to detect human or machinery related incidents with important inaccuracies.	Medium
6	Failure to successfully transfer knowledge and experience from business to	60	4-Slight	The project management is structured to ensure smooth communication between technology providers, academia and users,	Medium

	academia technology providers and vice versa			monitoring of progress and keep up to date with evolution. Furthermore, each partner has the expertise and policies to make the transfer of the knowledge to the key stakeholders in its areas of expertise.	
7	Pilot tests fail in providing the anticipated results or turn out to be inadequate	189	3-Moderate	During the Pilots the Manager of the projects may alter the conditions and the Pilot Sites in order to ameliorate the possibilities of a successful outcome. The consortium partners have the expertise to make the appropriate installation for the purposes of the pilots. Most of the partners have participated in several National and European projects related to similar activities involved in the Pilot. Besides this, the involvement of ALUMIL, a company with huge expertise in this type of implementations, reduces the possibility of such a risk to the minimum.	Medium
8	Technical results of low quality/relevance to targeted users and market	135	3-Moderate	A close inspection of the results on every level on any stage of the project can ensure that any low quality results, or any outcomes that deviate from the original purpose can be corrected or altered in a way that the outcome will serve the goals of the PLUG-N-HARVEST consortium.	Medium
9	Requirements are too generic or incomplete	189	3-Moderate	From the beginning of the project requirements are set and will be adapted to the project's needs.	Medium

Table 13. Mitigation Strategies for Organizational Risk Items

No.	Risk Description	RPN	Severity	Mitigation Strategy	Mitigation Possibility
C. Organizational					
1	Consortium has no harmony	63	4 - Slight	The PC will continuously be in contact with all partners. This guarantees that any team problems are identified and solved before they escalate.	Medium
2	Partner leaves consortium	45	4 - Slight	Consortium is of sufficient strength and diversity so that partners can be replaced if required. Also, the coordinator will ensure appropriate control and management of the work in progress so that the remaining partners can complete the work, until a new partner is found (in case that is considered necessary).	Medium
3	Key staff illness / leave during critical phase	45	4 - Slight	All partners have experienced staff that may replace and take over the work assigned to the leaving member, either temporarily or permanently.	Medium

4	Poor quality of deliverables and delay in meeting the deadlines	60	4 - Slight	The Scientific & Technical Manager will provide templates & guidelines documented in a project management handbook for all significant items (e.g. deliverables). Proper internal peer review procedures will be in place, to ensure quality of the deliverables and their preparation in a timely manner. Regular WP & technical meetings will be held to ensure that activities are streamlined and that lessons learnt are shared. If necessary, the involvement of independent, internationally recognized reviewers will be sought for key deliverables.	Medium
5	Budget and resource allocation risks	135	3 - Moderate	A careful planning has been carried out to minimise the risk of underestimation of resources. The partners will review their expenditure / budget on a six monthly base. Package leaders will monitor partner's resource spending and report unexpected deviations, preparing a detailed activity plan with unambiguous definitions of responsibilities and effort. The Plenary Board will help with internal redistributions/modifications.	Medium
6	Unrealistic project time schedule and deadlines	144	3 - Moderate	According to the real time estimations in regard with the problems and the delays, a new schedule will be issued to cover any loss time or deadlines. The necessary communication actions will be made early on the estimations to avoid losing deadlines.	Medium
7	Partner underperforming	62.5	4 - Slight	The consortium of PLUG-N-HARVEST is a strong assembly of well-known research institutes, SMEs and industrial organizations. Based on the current R&D interests of the Consortium Partners they are willing to invest additional work/efforts on specific themes, thus reducing this risk.	Medium
8	Relevant events are not falling within the project life span or overlap with important phases of the project, hindering partners to attend	63	4 - Slight	A first draft of the scheduled meetings and activities could be delivered at the beginning of the project.	Medium
9	Unanticipated Project Manager workload and Personnel unavailability	60	4 - Slight	The personnel will work together to share knowledge so that no one person is critical to the project's success. Detailed documentation will minimize the time needed for a new person to join the team.	Medium

Table 14. Mitigation Strategies for Behavioural Risk Items

No.	Risk Description	RPN	Severity	Mitigation Strategy	Mitigation Possibility
D. Behavioural					
1	Personnel behavioural issues	84	3 - Moderate	The performance of a European Project is based on the cooperation of the individual partners. A well-established cooperation can ensure the normal flow of the project. Based on the professionalism of the partners in the PLUG-N-HARVEST project such problem can be isolated in the interior of each partner without influencing the relationship among the partners and as such the normal flow of the project.	High
2	The IT – Equipment effects the behaviour and the performance of the personnel	132	3 - Moderate	The PLUG-N-HARVEST Helpdesk will inform and support the participants or any other involved party, reassuring that the ethical guidelines of the European Research in FP7 are being met and all the effort is being done with respect to the human factor.	Medium
3	Disputes over ownership of IPR amongst consortium partners	60	4 - Slight	Standard IPR and access rights clauses will be included in the CA, will be signed before work starts in order to avoid future disputes. The consortium has already discussed these aspects during the proposal phase for avoiding such problems.	Medium
4	Breach of IPR conditions within consortium	75	3 - Moderate	Ensuring that IPR clauses are properly understood before signing the CA. Clauses which present difficulties will be negotiated beforehand among partners.	Medium
5	Lack of interest on the PLUG-N-HARVEST project by external stakeholders	63	4 - Slight	Partners on this part of the project will manage a continuous operation on communication channels in order to keep in touch with multiple stakeholders. Also, various dissemination activities will be carried out to raise the awareness and increase the interest into the results of the project. PLUG-N-HARVEST consortium has strong links with groups of stakeholders, which already indicated their interest by Letters of Support.	Medium
6	Emerging Competitors	137	3 - Moderate	PLUG-N-HARVEST, by its design, is positioned to have a strong market with its capabilities. In case of strong competitors in the market, the exploitation plan will be updated to reduce the risk and new ways of exploitation will be evaluated.	Medium

Table 15. Mitigation Strategies for Ethical Risk Items

No.	Risk Description	RPN	Severity	Mitigation Strategy	Mitigation Possibility
E. Ethical					
1	Storage and process of occupant-related privacy data towards person localization and extraction of patterns and flows within selected pilot tests.	144	3 - Moderate	For humans, localization privacy-preserving sensors will be utilized and data processing will be performed in a totally anonymous and unobtrusive manner. Also, the provided identification tags will be assigned to roles (e.g. occupant, workers, etc.) and not to particular (named) people. Any original records or data will be destroyed after that, if this is not forbidden by law of the country in which the information was collected, stored and analysed. Issues of privacy will be addressed with emphasis at the elicitation of requirements.	High
2	Difficulties in ensuring the security of shared personal/ private data in the pilot tests.	150	3 - Moderate	Special attention will be given to ensure confidentiality and for incorporating Privacy Enhancing Technologies (PET) such as data anonymization & pseudonymization to ensure protection from data breaches. PLUG-N-HARVEST partners have proven capacity and the experience to cope with the delivery of advanced security mechanisms, if needed.	Medium
3	Difficulty in ensuring the security of human data collected during the execution of the trials.	175	3 - Moderate	PLUG-N-HARVEST partners have the expertise and the know-how from similar past and ongoing research projects, towards providing the necessary ethical guidelines that should be adopted during the execution of the pilots. Pilot-related ethical responsible members (and the National committees, if considered necessary) will be formed by each responsible partner and will be informed towards getting an official permission for the execution of the selected Pilots. Thus, the respective test's transparency will be maximized.	Medium
4	Lack of Transparency	144	3 - Moderate	The Ethical Advisory Board will provide the necessary documents (e.g. ethics manual) in order to minimize this risk (as well any other similar that may arise during the project lifetime) and being in compliance with National and European legislation. A detailed informed consent form will be carefully prepared for each pilot site by the local ethical committees, fully outlining the scope of the trial and	Medium

				its purposes along with the data collected and analysed.	
5	Delegation of Control Privacy. Incidental Findings	75	3 - Moderate	Within the project a sub-activity has been included to address local and European legislation. In that context, all the Pilot Use Cases will be performed according to them and relevant data protection authorities will be informed on time.	Medium
6	Improper use of IT Equipment	105	3 - Moderate	The consortium partners have the expertise to make the appropriate installation for the purposes of the pilots. Data routing equipment that will be used already has reliable embedded security mechanisms. In addition, most of the partners have participated in several National and European projects related to integration of sensors for research purposes and their use in ethical compliance with National and European legislations. The PLUG-N-HARVEST Ethical Advisory Board will monitor pilot realization ensuring the appropriate use of IT equipment.	Medium

There is no need for mitigation strategies as far as the project risks are concerned because no risk is critical (RPN>250).

3.3 Technical Risk Identification

Table 16. Initial General Risks and RPN Calculations

No	Risk Description	Impact to WPs	S	O	D	R	RPN	Risk Level
Scientific & Technological Risks								
1	Internet Failure	WP3, WP4	8	9	1	1	72	3-Moderate
2	Communication failure among PLUG-N-HARVEST sub-systems (Middleware, Platform etc.)	All	7	5	6	6	210	3 - Moderate
3	Interoperability problems among the various different components of the PLUG-N-HARVEST Framework	WP3, WP4	6	5	2	3	75	3 - Moderate
4	High amount of data especially to M2M & Field level	WP4, WP5	5	5	2	3	62.5	3 - Moderate
5	PLUG-N-HARVEST Framework performance is low due to complexity in implementation	All	6	5	2	4	90	3 - Moderate
6	Unavailability of technology	All	6	4	4	4	96	3 - Moderate

7	Need to redesign the system due to technological changes,	All	6	6	5	5	180	3 - Moderate
8	optimization and control may not take into account all scenarios available	All	7	7	2	3	122.5	3 - Moderate
9	Integration with existing building fails	WP4	6	5	4	5	135	3 - Moderate
10	Performances issues (too slow)	All	4	4	2	3	40	2 - Slight
11	Not properly defined KPI's and thus not optimal evaluation of project results	All	4	5	4	4	80	3 - Moderate
12	Possible damaged sensor or meter device (e.g. energy monitoring devices, brakers) - false data acquisition	All	3	4	2	3	30	2 - Slight
13	Lack of weather data	All	7	7	4	4	196	3 - Moderate
14	User Interface Failure	All	5	5	5	6	137.5	3 - Moderate
15	Not right tuning of stability and/or overload	All	5	5	6	6	150	3 - Moderate
16	Lack of IoT protocol interoperability	All	4	4	4	3	56	2 - Slight
17	Appropriate users are not available to validate the system platform.	All	7	3	3	5	84	3 - Moderate
18	Installation and use of equipment on the pilot sites	WP4	4	5	4	5	90	3 - Moderate
19	Safety issues related to the ADBE	WP4	4	4	3	3	48	2 - Slight
20	ADBE tenders and Installation take significantly more time than expected	WP4	5	5	6	6	150	3 - Moderate
21	ADBE equipment (Ventilation Units, Batteries, etc.) that is compatible to the PLUG-N-HARVEST solution is difficult to be found	WP4	4	4	3	4	56	2 - Slight
22	Actuators for radiators and electrical points that is compatible to the PnH solution is difficult to be found	WP4	4	4	3	3	48	2 - Slight
23	Lack of certain market actors or roles required for the PLUG-N-HARVEST exploitation to be successful	WP5	8	2	2	6	64	4 - Slight

24	Components are not easily disassemble or replaced due to wrong installation practices.	WP4, WP5	4	4	3	4	56	4 - Slight
25	Maintenance and/or upgrade of the system don't work properly due to the lack of local service providers	WP5	4	4	3	3	48	4 - Slight

Based on Table 16 and Equation 2, the Total Risk Estimate value for **technological and scientific risks** is:

TRE = 9.506%

This value is lower than 17%, thus according to *Bluvband and Grabov* it suggests that PLUG-N-HARVEST is not a risky project regarding Technological & Scientific risks. However, this value can be further reduced (diminishing even more possible risk effects) if appropriate mitigation strategies are taken into account, as described below.

Reordering the individual risks by their respective RPN values, and plotting them on a screen plot (Figure 3) allows for the identification of the RPN threshold. Any risks above this limit are deemed to be critical and require greater attention in their mitigation plans. As shown in the Figure 3, the threshold for the technological risks identified in the PLUG-N-HARVEST Risk Assessment is RPN<250.

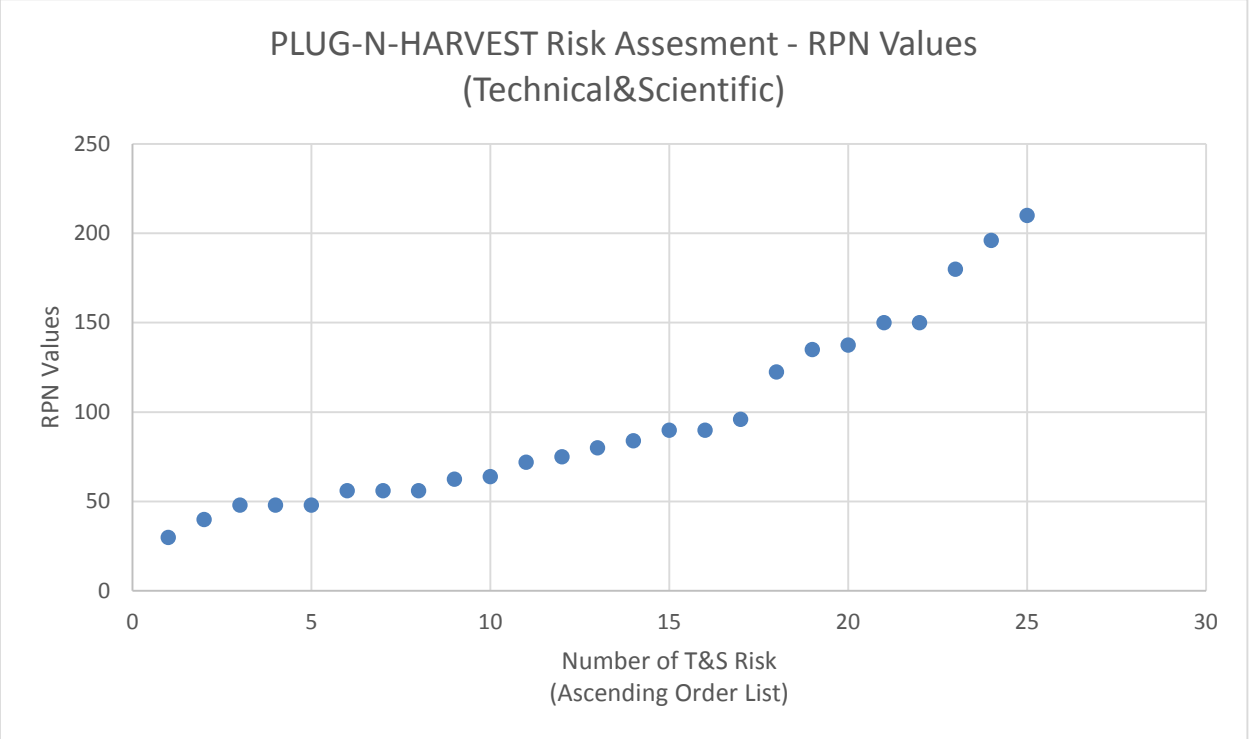

Figure 4. RPN Scree Plot for the PLUG-N-HARVEST Project

3.4 Technical Risk Mitigation

Based on Table 11 of Section 3.2, Table 17 presents mitigation strategies and probabilities for scientific and technological risks. Critical risk items are highlighted.

Table 17. Mitigation Strategies for Scientific & Technological Risks

No.	Risk Description	RPN	Severity	Mitigation Strategy	Mitigation Possibility
Scientific & Technological Risks					
1	Internet Failure	72	3 - Moderate	It should be noticed that the only thing that Internet Failure affects towards PLUG-N-HARVEST is the lack of information considering weather data. In such case PLUG-N-HARVEST will utilize offline data of concordant days. It needs to be emphasized that the internet use is about 5-6 connections/hour and that the system doesn't need a permanent connection with the internet.	Medium
2	Communication failure among PLUG-N-HARVEST sub-systems (Middleware, Platform etc.)	210	3 - Moderate	The PUG-N-HARVEST is able to function properly in offline mode using rule based control strategies, which however will offer some basic functionalities of P-n-H	Medium
3	Interoperability problems among the various different components of the PLUG-N-HARVEST Framework	75	3 - Moderate	Due to the use and combination of heterogeneous technologies, high focus has been given to interoperability within PLUG-N-HARVEST, therefore all components will be extensively tested prior to their integration in the PLUG-N-HARVEST Framework. Also, possible technical inconsistencies will be inspected in order to provide the best possible resolution in time. Finally, an open architecture will be used for minimizing the risk of interoperability.	Medium
4	High amount of data especially to M2M & Field level	62.5	3 - Moderate	The PLUG-N-HARVEST modules require the minimum possible exchange of data and thus the possibility of such risk is practically low	High
5	PLUG-N-HARVEST Framework performance is low due to complexity in implementation	90	3 - Moderate	All the required infrastructure & tools have already been implemented in previous projects and are operating in Pilots. Furthermore, all consortium members have long experience in large research projects as well as in the implementation of large and complex systems, thus the possibilities of such problems compromising the project are low.	Medium

6	Unavailability of technology	96	3 - Moderate	All required critical components of the PLUG-N-HARVEST architecture are already available with high-level TRL levels by partners.	Medium
7	The need to redesign the system due to technological changes	180	3 - Moderate	Technological changes are expected to provide more opportunities to the project, as technology innovations awareness is of great significance. Therefore, Partners will continuously monitor all technological developments in order to take advantage of what they have to offer and use it for improving the tools delivered by this project	Medium
8	Demand Response optimization and shifting may not take into account all scenarios available	122.5	3 - Moderate	In WP1, PLUG-N-HARVEST partners, will make sure that all different scenarios will be identified	Medium
9	Integration with existing building fails	135	3 - Moderate	The design and implementation of components should be strictly decoupled from all tool-specific details. S/W and communication interfaces should be compatible with the existing standards.	High
10	Performances issues (too slow)	40	2 - Slight	All PLUG-N-HARVEST modules use highly computational efficient algorithms with very low computational requirements	Medium
11	Not properly defined KPI's and thus not optimal evaluation of project results	80	3 - Moderate	A very intensive procedure involving all different crucial stakeholders will take place in WP1, for avoiding such a risk	Medium
12	Possible damaged sensor or meter device (e.g. energy monitoring devices, brakers) - false data acquisition	30	2 - Slight	Due to Plug-n-Play nature of PLUG-N-HARVEST and the use of fault detection algorithms the early detection and replacement of faulty equipment will be made possible	Medium
13	Lack of market price and weather data for renewable forecasting	196	3 - Moderate	It should be mentioned that in all pilots these data are already available either in online or in offline mode	Medium
14	Human Machine Interaction (HMI) failure	137.5	3 - Moderate	The PLUG-N-HARVEST system – due to its high autonomy – can be fully functional even when the HMI is not working	Medium

15	Not right tuning of stability and/or overload	150	3 - Moderate	The PLUG-N-HARVEST system embeds highly stable and robust mechanisms	Medium
16	Lack of IoT protocol interoperability	56	2 - Slight	PLUG-N-HARVEST will mitigate this risk by establishing new open general specifications, so that system vendors can easily get connected with the help of open source samples for adapter implementations without the necessity to share their specifications and source codes.	Medium
17	Appropriate users are not available to validate the system platform.	84	3 - Moderate	User partners have already been carefully selected to ensure that they are suitable for the pilot tests. Additional users will be identified as part of the use case demonstration process and will be kept as potential backup if required.	Medium
18	Installation and use of equipment on the pilot sites	90	3 - Moderate	The consortium partners have the expertise to make the appropriate installation for the purposes of the pilots. Most of the partners have participated in several National and European projects related to similar activities involved in the Pilot. Besides this, the involvement of ALUMIL, a company with huge expertise in this type of implementations, reduces the possibility of such a risk to the minimum.	Medium
19	Safety issues related to the ADBE	48	2 - Slight	The design of the ADBE is specially focusing on maximizing safety for the building and its occupants. Moreover, the presence of partners with huge experience in the installation and operation of similar - or even significantly more elaborate and large-scale - systems guarantees the safety of operations both during the installation and during the operation of the PLUG-N-HARVEST ADBE	Medium
20	ADBE tenders and Installation take significantly more time than expected	150	3 - Moderate	This is the reason why the whole procedure of tenders will start very early in the project	Medium

21	ADBE equipment (Ventilation Units, Batteries, etc.) that is compatible to the PLUG-N-HARVEST solution is difficult to be found	56	2 - Slight	Due to PLUG-N-HARVEST Modular and Plug-n-Play nature the possibility of such a risk is negligible	Medium
22	Actuators for radiators and electrical points that is compatible to the PnH solution is difficult to be found	48	2 - Slight	The consortium partners have the expertise to integrate commercial products from other manufactures. Besides this, the involvement of OdinS, a company with huge expertise in this type of integrations, reduces the possibility of such a risk to the minimum.	High
23	Lack of certain market actors or roles required for the PLUG-N-HARVEST exploitation to be successful	64	2 - Slight	Within business models and Exploitation Plans design task, the analysis of the exploitation value chain will be carried out and, if required, external parties will be sought beforehand	Medium
24	Components are not easily disassemble or replaced due to wrong installation practices.	56	2 - Slight	The consortium will develop clear guidelines to install the system properly. Service providers beyond the consortium are to be identified and involved to avoid this.	Medium
25	Maintenance and/or upgrade of the system don't work properly due to the lack of local service providers	48	2 - Slight	Service providers for each exploitation model proposed are to be identified. As the system will be designed to exploit this service, the design will enable an easy maintenance making this risk negligible.	Medium

Since no technological risk identified as critical (RPN>250), no further special mitigation strategies need to be included in the particular deliverable.

3.5 EFMEA Conclusions

According to the results of the EFMEA risk methodology, the PLUG-N-HARVEST project does not have a high risk probability. However, even the moderate risks must be taken into consideration in order to avoid possible future problems. Applying the EFMEA approach has enabled the risks to be identified and the appropriate contingency plans to be proposed. Finally, the application of the risk mitigation plans to the risks as well could provide a further reduction of the TRE coefficient. It should to be emphasized that during the procedure no critical risk (RPN>250) occurred. Also, it is essential to underline the fact that the Risk Assessment and Mitigation Planning is an ongoing process throughout the lifecycle of the project. Having that in mind and taking into consideration the problems that may occur if extra risks are revealed, the PLUG-N-HARVEST managing team and the Ethical Helpdesk will be in alert to identify and appropriately encounter such occasions.

3.6 Risk Monitoring

This section is an assessment of the proposed risk management plan, as far as its employment during project run is concerned, mentioning whether any of the possible risks identified actually occurred and how it was encountered according to the respective mitigation plans or whether a new risk not covered in the given list was revealed. As the Risk Register is a living document, it is important to record the date that risks are identified or modified. Optional dates to include are the target and completion dates. As mentioned in previous sections of this deliverable the Risk Register is maintained at SCIEBO Repository and can be found in the following path on SCIEBO:

\Sciebo\Plug-N-Harvest\WP7\Auxiliary Documents\

4 References

[1] Risk Assessment http://www.healthyworkinglives.com/advice/Legislation-and-policy/Workplace-Health-and-Safety/risk-assessment#what

[2] The use of current risk analysis tools evaluated towards preventing external domino accidents. G.L.L. Reniers, W.Dullaert, B.J.M. Ale, K.Soudan., s.l. : Elsevier Journal of Loss Prevention in the Process Industries, 2005, Vol. 18, No 3, pp.119-126, 2005.

[3] What Is HAZOP https://www.graphicproducts.com/articles/what-is-hazop/

[4] https://www.isixsigma.com/tools-templates/fmea/quick-guide-failure-mode-and-effects-analysis/

[5] https://www.linkedin.com/pulse/failure-mode-effects-analysis-fmea-anes-elabbani/

[6] "Your Guide for FMEA Information". http://fmea-fmeca.com/

[7] Expanded FMEA (EFMEA).Z.Bluvband, P.Grabov, O.Nakar. Annual Symposium on Reliability and Maintainability, (RAMS '04), pp 31-36, 2004

[8] "Failure analysis of FMEA". Z.Bluvband, P.Grabov. Annual Symposium on Reliability and Maintainability, (RAMS '09), pp 344-347.

[9] http://www.cholarisk.com/services/process-safety/qra-hazop/what-if-analysis/

[10] Risk Analysis in research environments. A.Groso, A.Ouedraogo, T.Meyer., Journal of Risk Research, vol. 15, pp. 187-208, London, 2012.

[11] Failure Modes and Effects Analysis Guide, Manufacturing Technology Committee – Risk Management Working Group, Product Quality Research Institute http://www.pqri.org/pdfs/MTC/FMEA_Training_Guide.pdf

[12] http://www.fmea-fmeca.com/fmea-rpn.html