Project No. 957406

Project acronym: TERMINET

Project title:

nexT gEneRation sMart INterconnectEd ioT

Deliverable 1.2

Risk Management Manual

Programme: H2020-ICT-2020-1
Start date of project: November 01, 2020
Duration: 36 months

Editor: CERTH

Due date of deliverable: February 28, 2021 **Actual submission date:** February 28, 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957406

Document Control Page

Deliverable Name	Risk Management Manual
Deliverable Number	1.2
Work Package	WP1
Associated Task	T1.2
Covered Period	M01-M04
Due Date	February 28, 2021
Completion Date	February 28, 2021
Submission Date	February 28, 2021
Deliverable Lead Partner	CERTH
Deliverable Author(s)	Georgios Stavropoulos, Dimosthenis Ioannidis, Ioannis Schoinas
Version	1.0

Dissemination Level		
PU	Public	X
CO	Confidential to a group specified by the consortium (including the Commission Services)	

Document History

Version	Date	Change History	Author(s)	Organisation
0.1	February 02, 2021	ToC Creation	Georgios Stavropoulos	CERTH
0.2	February 12, 2021	Risk identification completed	Georgios Stavropoulos	CERTH
0.3	February 15, 2021	Input and comments from partners	-	UOWM, AUTH, SCHN, INTRASOFT, WTG, SID, MARTEL
0.8	February 22, 2021	Final version submitted for internal review	Georgios Stavropoulos	CERTH
1.2	February 22, 2021	Final version after internal review	Georgios Stavropoulos	CERTH

Internal Review History

Name	Institution	Date
Ioannis Neokosmidis	INC	February 26, 2021
Stefanos Tsantilas	8BELLS	February 26, 2021

Quality & Risk Manager Revision

Name	Institution	Date
Dimosthenis Ioannidis (CERTH), Panagiotis Sarigiannidis (UOWM)	CERTH, UOWM	February 26, 2021

Legal Notice

Table of Contents

List of Figures

List of Tables

Acronyms

Acronym	Explanation
EFMEA	Extended Failure Modes and Effect Analysis
FMEA	Failure Modes and Effect Analysis
HAZOP	Hazard and Operability Studies
KPI	Key Performance Indicator
PC	Project Coordinator
PCC	Project Coordination Committee
PO	Project Office
RADM	Risk Assessment and Decision Matrix Analysis
RIPM	Risk Identification and Plan Management
RPN	Risk Priority Number
SB	Sustainability Board
STC	Scientific and Technical Committee
TRE	Total Risk Estimate
WP	Work Package

1. Introduction

1.1 Purpose of the Deliverable

The present deliverable intents to identify the potential risks that TERMINET consortium might face during the project's lifecycle. It will try to determine the severity of these risks and identify possible mitigation strategies that will ensure a successful outcome for the project.

This deliverable is part of WP1 and Task 1.2 and will serve as a guideline for the consortium partners throughout the project's lifecycle on how to mitigate risks, should any arise.

Besides quantifying the impact of the potential risks to the project, it also describes the necessary steps to mitigate the risk and allow the consortium to further proceed with the project developments.

1.2 Structure of the Document

The document is structured as follows:

Section 2 describes the methodology that is followed for risk identification, classification and quantification, along with the methods to calculate all the parameters associated with each risk, as well as the overall risk factor for the project.

Section 3 presents the risks that have been identified for TERMINET, their calculated impacts, and the respective mitigation strategies. The overall risk factor for the managerial and the technical aspects of the project are presented, along with the final assessment of the project's risk value.

2. Risk management

2.1 Introduction

Risk management and analysis is a fundamental requirement in research and industry. During the lifetime of project various types of risks can emerge and need to be addressed by the consortium. Risk management process includes identification, analysis about the severity of the risk and the harm they can inflict, probability of a threat to occur and the realization of the appropriate response for that case. Finally, statements about critical risks are recorded. For the risk management plan to be effective it should reduce the possibility of such risks occurring and reduce any potential impact to the project.

The proposed risk management plan as well as mitigation actions to address risks that could emerge within TERMINET are presented in this section. First, details about the methodology followed (EFMEA) [1], for identification and severity assessment are presented. Following this, lists of recorded risks and actions are presented, divided in two main categories Project risks and Technical risks. In the next sections, details regarding the risk identification process and the format of the Risk Register that will be used are presented. In the last section the chosen methodology, Expanded Failure Modes and Effects Analysis, is described in detail.

It is essential to keep in mind that Risk Analysis is an iterative process meaning that the lists of identified risks, impact and mitigation actions will be constantly updated until completion of the TERMINET project. It should also be mentioned that it is impossible to eliminate the possibility of a risk occurring. The main objectives of the risk management plan is to prepare for any possible risks, minimize as much as possible the possibility to occur and minimise any negative impact to the project.

2.2 Risk Management Plan

The plan adopted within TERMINET project includes 5 stages, those of identification, quantification, response, monitoring and documentation to be implemented in cases that the project needs to address an issue.

- **Risk Identification** includes the detailed documentation of possible risks that could affect the project
- **Risk Quantification** processes identified risks and estimates their importance based on the impact they pose. In addition, generates data to be used to decide the proper response.
- **Risk Response Development** uses information during risk estimation to develop strategies and plan mitigation actions
- **Risk Monitoring and Control** keeps record of identified risks, ensures execution of risk plans, evaluates effectiveness of actions taken and updates the risk management plan
- **Risk Documentation** includes the objectives, information sources, assumptions, decisions, and actions taken upon emerged risks

The first three stages are covered by the most of Risk Analysis and Assessment methods. There is an abundance of such methods available. Some of the shared characteristics between these techniques are identification of causality, impact or hurt from a risk, safeguards, and recommendations. The methodology selected to be implemented within the TERMINET project is entitled “Expanded Failure Modes and Effects Analysis”. The selected method will be further presented in the following sections.

2.3 Risk analysis and assessment methods

As already stated, there is an abundance of Risk analysis and assessment methods. In this section we will describe and compare five of them, “Hazard and Operability Analysis” (HAZOP) [2], “Failure Modes and Effects Analysis” (FMEA) [3][4], “What if” [5][6], “Risk Assessment Decision Matrix Analysis” (RADM) [7] and “Expanded Failure Modes and Effects Analysis” (EFMEA) [1] that will be used in TERMINET.

2.3.1 Hazard and Operability Analysis (HAZOP)

Hazard and Operability Analysis or HAZOP in short, is an established and well documented risk analysis method, which is used with great success in the Chemical and Piping industry. The purpose of HAZOP as well as of the rest of the analysis methods are to discover the points which could go wrong and regard the involved personnel, equipment or overall operability of a process or work. The assessment process is broken down into simple steps and every parameter and variation that is involved is taken into consideration. According to the analysis, hazards occur from the deviation to standard procedure. The intention of this method is to discover potential design and engineering issues by analysing the initial complex design in smaller steps that are called `nodes`. Reviewing each node separately makes the identification of potential failure easier and straightforward.

2.3.2 Failure Modes and Effects Analysis (FMEA)

Failure Modes and Effects Analysis (FMEA) is another systematic approach that aims to identify and document all failures during the design process. It is also used in the later stages of the project to monitor, assess, and control any emerged risks. In addition, FMEA performs evaluation of potential effect from the identified failures modes. It is based on the questions of “What can fail?”, “How it failed?”, “How often it fails?”, “In which way the failure affects the process?” and “Are there any reliability or safety consequences from the failure?” Failure modes include the ways or cases that something could go wrong while effects analysis includes the documentation of potential effects.

2.3.3 What-if Analysis

What-if analysis is a more intuitive than systematic analysis method. It is a simulation which aims to inspect the behaviour of a complex system or a project in specific cases. It is based on the formulation of

specific hypotheses also called scenarios and measures how the change of certain parameters could affect the system. To formulate the scenarios usually the question “what if” is raised and the potential outcome is recorded.

2.3.4 Risk Assessment Decision Matrix Analysis (RADM)

Decision Matrix Analysis is a helpful technique that helps with decision making and can be used in risk assessment. It includes graphic representations with information about potential risks, their impact, and their probability to occur. It is better to be viewed as a tool to quick view and rank the risks that can be used alongside other risk analysis methods rather than a standalone risk analysis method.

2.3.5 Expanded Failure Modes and Effects Analysis (EFMEA)

Expanded Failure Modes and Effects Analysis is based on the FMEA method that is mentioned above and is designed to overcome its limitations. Applying this method will enable managers to identify critical failure points in the system. Also, it provides tools for discovery and evaluation of suitable mitigation strategies and actions. The analysis is conducted in two phases ***Risk Identification*** and ***Risk Mitigation.***

Additionally, EFMEA methodology distinguishes risks in the following types:

- Technical (Risk associated with the implementation of the project or system)
- Legal (Regarding issues associated with current legislation framework in the country)
- Behavioural (Regarding user or partners behaviour)
- Organizational (Risks associated with management and the organizational structure)

2.3.6 Conclusion

After careful consideration about the characteristics of various risk analysis methods and in accordance to the recommendation in the literature[8], EFMEA stands out as the most appropriate method for the TERMINET project. It is a systematic approach which is commonly used in various sectors and holds the ability to be applied even in systems with increased complexity. One of the characteristics that separate it from the rest is that also includes an analysis of risks sources and the strategies that can be used to mitigate them.

EFMEA is a valuable tool with numerous advantages that assists with the management of complex projects such as TERMINET. The result of applied mitigation actions and their effect can be estimated and provides a metric about the improvement achieved. Moreover, offers detailed documentation of the improvements that took place due to corrective actions and helpful insights and information about testing and monitoring procedures. Finally offers historic information useful to consecutive iterations of risk analysis that take place further down in the evolvement of the project.

2.4 Risk Identification

The Risk management of the project has in its core the Risk Register. A valuable tool in the hands of the project managers which is used to monitor all processes associated with risk management such as identification, assessment, and management of risks to a level viable for the project goals. This process includes periodic reviews and updates. The purpose of the Risk Register is to keep track of the risks identified as well as details regarding their analysis and the agreed corrective actions to address them.

Maintenance of the register will offer to the consortium the ability to identify and manage risks and record mitigation actions as the project progresses. Specifically, it contains all the risks that have been identified, information about the area they concern, level of the risk, which WPs are affected and actions to remedy impact. It is thus can be used to inform relevant stakeholders about potential future issues.

The coordinator of the project will host a shared repository to hold the register and the consortium will use, maintain, and update it.

In the case that a member identifies a new risk a specific process needs to be followed. The steps of this process are described below:

1. Members which identify a possible risk or harm about the work of the project, first discuss it with the WP leader that the work belongs, the PC, the QM, and the management board through the PO. WP leader, PC and QM are responsible to update the Risk Register with details and actions about the new risk
2. Periodic discussion about risks is planned and takes place in a two-month basis. In this process the monitoring and update status is changed. Risks and mitigation plans are also discussed during Project Coordination Committee (PCC) meetings. Any new risks which are discovered in these meetings should be recorded.
3. WP leaders, management board and the persons associated with a specific risk are responsible to come up with a sufficient plan with corrective actions. Importance and impact of the risk dictates the level of detail that will be included in the plan of action.
   a. In cases where the risk is unlikely to occur some options regarding mitigation actions will be discussed and documented
   b. In cases where there is a high probability for the risk to occur, plans regarding mitigation actions need to be exact, detailed, and unambiguous.

Type	WP	Risk Event	Mitigation Action Plan	S	O	D	R	RPN	Risk Level
Communication	All	Disagreements between partners in WP	A sustained disagreement is resolved by the WP leader. In case that the disagreement persists, the PC is called to resolve the situation. STC is responsible for the final decision in case that no consensus has been arrived.	6	4	3	5	96	III - Moderate
Communication	WP10	Lack of commitment by Stakeholders regarding the project goals	Engagement and promotion of the benefits of the project for society, economy and environment	3	4	3	2	30	IV – Slight
Communication	WP10	Poor teamwork and knowledge sharing mentality among project memebers	Enhance teamwork and feedback sharing among partners by organising workshops and including multiple channels from the early planning phase	4	3	8	7	90	III – Moderate

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957406

Ethics	All	TERMINET developed systems(s) are not compliant with national and EU legislation	WP11 will ensure an early in-depth analysis of the relevant legislation and integration into TERMINET systems.	7	6	1	6	147	III _ Moderate
Ethics	WP11	Changes in EU and national legislation that impact the developments within TERMINET	The TERMINET consortium will continuously monitor all relevant regulations to make sure that they are followed.	9	9	2	6	324	II - Severe
General	All	Required background input from other projects that is not available at the specific moment.	Avoid major impact to the project by relying to relevant knowledge of other partners until a new one with a more fitting expertise is introduced to the project.	4	6	3	3	72	III- Moderate
General	All	Dependencies with other projects that are not included in the initial software design and development.	Technical assessment regarding potential interdependencies will be conducted alongside the whole development process by the project coordinator and technical	4	6	5	3	96	III- Moderate

			manager. Relevant extensions and customizations will be developed to satisfy any discovered dependencies with other projects.						
General	WP10	Lack of interest and involvement by Policy makers.	Ensure maximum involvement in project's training sessions and activities such as workshops and seminars.	5	6	5	4	135	III-Moderate
Managerial	All	Inadequate resource and budget forecasting.	Careful planning regarding resource spending aims to minimize that risk. Partners' expenditure / budget will be reviewed by them on a semi-annual basis. Package leaders will be responsible to prepare detailed activity plans that specifically define responsibilities and effort.	1	5	4	3	17,5	IV-Slight

Managerial	All	Inadequate time estimation and difficulty to follow projects time schedule and deadlines.	Assessment of the problems, of the delays and real time estimations will lead to issuance of new schedules to address loss of time or deadline. Necessary communications is required in the early phrases of estimations to avoid shortcoming.	5	3	3	3	45	IV-Slight

Managerial	All	Problems and issues emerged due to partner quitting the project	Reliance to other partners relevant knowledge until a partner with a more fitting expertise is discovered	8	5	1	4	100	III - Moderate
Managerial	All	Missing deadline for a specific work, report or deliverable	STC and PCC can consider taking drastic measures that include shifting of responsibilities and resources for cases that delays are not justified or not remedied straight away. Report regarding delays and spenditure should also include a plan of mitigation actions to resolve them.	5	4	2	3	50	IV – Slight

Managerial	All	Problems and issues in management due to the large volume of partners	Project coordinator and assigned WP leaders expertise and experience in similar assignments ensures efficiency in management. Specific attention to the project governance instruments and modalities is given.	7	4	2	3	70	III - Moderate
Managerial	WP10	Inadequate organisation of dissemination events and activities	Make a first draft of the dissemination plan (D10.2) early in the project (i.e. M06 of the project) so each representative can promote properly.	6	3	4	3	63	IV - Slight
Managerial	WP8	Inadequate or improper technological facilities to support the actions required by the project	TERMINET end users (AFS, FPG, PPC, KI, MEVGAL) will ensure that facilities selected for the pilots have dedicated premises and infrastructure for the scopes of the project.	2	3	2	3	15	IV - Slight

Figure 1. Sample of TERMINET's risk register

2.5 Risk Register Format

The Risk Register is a spreadsheet document with a number of columns that hold different information about risks. Its tabular form allows grouping and ordering of the risks based on their details. The columns of the register are presented in the following table:

Risk identification number	**A number defined upon recording a certain risk to uniquely identify it.**
Type	With this column a distinction between the risks is made based on their type. The types in which the risks are distinguished are: • General • Technical • Managerial • Communication • Ethics
WP	The work package associated and affected by that risk.
Risk event	Explanation of the issue that might occur and its cause.
S	**S**everity of the risk
O	**O**ccurrence of the risk
D	**D**etectability of the risk
R	**R**ecoverability of the risk
RPN	**R**isk **P**riority **N**umber. Used to prioritize risks
Risk Level	Depicts the level of the risk and the scale used: I. Extremely Severe II. Severe III. Moderate IV. Slight V. Insignificant
Mitigation Action Plan	This cell holds the agreed mitigation actions that aim to minimize the probability of the risk to occur as well as to reduce the impact
Mitigation Action Feasibility	Depicts the level at which the actions can reduce the impact of the risk. A scale from 1-5 is used with 1 being the highest and 5 the lowest.
Status	Status of the risk. Updated when a risk occurs and when the relevant actions have been followed.

Figure 2 Risk Register spreadsheet columns

2.6 Use of Risk Register

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957406

The Register is updated whenever a new risk is identified and reported following the procedure described earlier. In addition, the Register needs to be reviewed at each plenary meeting of the project and perform the following tasks to ensure that it is properly maintained and serves its purpose throughout the project:

- That risks and their impact are clear and unambiguous
- That every involved partner is informed about negative impact of risks in their work
- That the mitigation action plans are well defined, adequate and can properly address the issue
- That involved parties are informed about the actions they need to take in case a risk occurs

2.7 Expanded Failure Modes and Effects Analysis

This section aims to present the "Expanded Failure Modes and Effects Analysis" methodology that will be used in TERMINET for risk management. It is based on and designed to overcome the shortcomings of FMEA analysis method.

FMEA was developed to help and provide tools necessary for the qualitative and systematic analysis of risks. It aims to improve preparedness and prevent unexpected problems from emerging. Besides the identification of possible points of failure, it also focuses on what caused them and the proactive actions and recommendations that can help avoid them or compensate them.

It is widely used in various sectors since its characteristics enable the analysis of potential problems from the early stages of development. Early analysis makes it ideal since managers can timely proceed with corrective actions to mitigate them. Anticipation of failures from early stages also offers the advantage to plan and avoid failures through proper design and plan.

FMEA analysis records and documents the effect of each identified failure distinguishing failure nodes that are critical. In addition to how critical the effect can be, failure nodes are also ranked based on the probability they might occur. This process allows past knowledge in similar products or processes to effectively aid the identification of failure modes. Since these are available even in the stages before design, they can be included in the design process avoiding them or minimizing negative impact seamlessly and without added costs.

Failure Modes	**All those that could go wrong or fail. Includes any errors and defects either potential or actual.**
Effect Analysis	The study of the effects that **Failure Modes** pose and actions and strategies or actions that can be used to address them

Figure 3 FMEA Definitions

Failure Modes Effects Analysis is used:

- During design procedure of a product, service, or process
- When a product, service or process is about to be applied in a new way with uncertain outcome
- Prior to the development of control plans for a new or modified process
- When planning improvements for a product, service, or process
- During failure analysis of a product, service, or process

- Periodically to ensure seamless operation of a product, service, or process

Failures are also prioritized based on several features. These features include harmfulness, probability of occurrence and ease of detection. These three key points are used to define the Risk Priority Number (RPN) for each failure mode. FMEA aims to develop strategies to eliminate or address these failures prioritizing them based on the RPN. FMEA procedure is depicted in Figure 4.

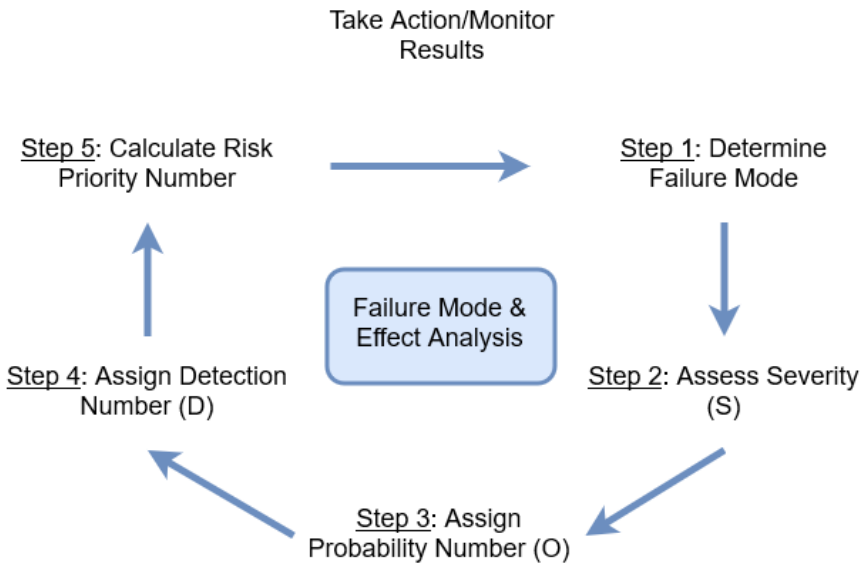

Figure 4 FMEA Process Cycle

To conclude FMEA is a popular and broadly applied Risk Analysis method. On the other hand, it has some limitations. It has been characterized as being tedious in the calculation process, and lacking important failures and difficulty to play an important role in decision making if applied late. The Expanded version of the method, EFMA, is designed to alleviate some of these shortcomings and extend its abilities and usage. EFMA is described in detail in section 3.

2.7.1 Risk Priority Number Calculation

To distinguish critical failure and prioritize the identified nodes the **Risk Priority Number (RPN)** is used. The scale used ranges from 1 as the best rank to 1000 which represents the worst possible rank.

The process of this analysis includes a number of factors that are used to determine the criticality of the failure. These are the severity, occurrence, detectability, and recoverability. Severity depicts how severe the effects of such failure would be, occurrence depicts the probability of the failure to occur and detectability shows how likely it is for the failure to be detected before it affects end users.

These concern all types of failures technical, behavioural, legal, or organizational. Technical risks concern any potential technical issues that could emerge during the project. Behavioural risks are related with the behaviour of the users, their response to the system and potential wrong reaction. Legal risks concern

about country's legislation and alignment of the system with it. At the end organizational risks include issues in the organizational structure and the processes being followed.

The Risk Priority Number is calculated for each risk with the following equation:

$$RPN = S \times O \times \frac{D + R}{2}$$

Figure 5 Risk Priority Number

Denoting with ***S*** the Severity, ***O*** for Occurrence, ***D*** for Detectability and ***R*** for Recoverability.

For consistency of the results, considering that TERMINET is a multinational consortium in which each partner works independently, ways to preserve a certain level of consistency are required. To preserve the consistency we use the work of Bluvband and Grabov [1]. We introduce the following list based on the question "What can go wrong?" as a standard way for the identification of potential Failure Modes.

1. The intended function is not performed at all.
2. The intended function is not performed adhering to the expected safety standards or regulations regarding its performance.
3. The intended function is not performed in the expected timeframe (availability problems).
4. The intended function is not performed in the expected place (position in the system).
5. The intended function is not performed in the expected way (efficiency problems).
6. The intended function has lower performance than expected.
7. The intended function has higher cost than the expected (additional maintenance, repair, power consumption etc.).
8. Functions performed unexpectedly and without intention.
9. Lifetime of the intended function performance is lower than expected (reliability issues).
10. Partial, or no available at all, support or for the intended function (maintenance, repair, service issues etc.).

The following tables have been developed to aid and further standardize the estimation of the risk level and the proper calculation and assignment of RPN. Detailed information about the methodology followed as well as about parameters used in the calculations can be found in the literature [1], [9], [10]

Table 1 (S)everity Level Analysis

Level of severity	Technological issues	Behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (extremely severe)	The failure could endanger user safety, possibly causing injury or fatality	User-generated errors in system operations could lead to an incident (i.e., safety effects)	National or international laws that prohibit the use of the system	Organizational framework needed that is completely missing (i.e., new services)	General issues considered vital for the system.
7-8 (severe)	The failure results to complete loss of system functions, resulting in user's dissatisfaction	Errors caused by user behaviour may negate system benefits	The existing legislation cannot support the system implementation and relevant work needs to be done.	Organizational framework adaptation is needed (some initial actions have been taken on this domain)	General issues considered severe for the system.
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 legislation is required for system implementation and work required has already been performed	Organizational framework adaptation is needed which has already started being realized	General issues considered slightly severe for the system.
3-4 (significant)	The failure leads to slight user dissatisfaction	Changes to User behaviour may affect the positive system aspects	New legislation is needed for system implementation, but consensus exist	There is a necessity for adopting a limited number of organisational changes	General issues considered significant for the system.
1-2 (insignificant)	The failure does not conceivably affect the system function and user's satisfaction	Changes to user behaviour is not expected to affect the system benefits, may even further enhance them	No new legislation is needed for implementation	There is no necessity for organizational changes	General issues considered insignificant for the system

Table 2 (O)ccurence level analysis

Occurrence level	Technological issues	behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (very high)	It is virtually certain that some errors/failures will happen	It is virtually certain that behavioural effects will happen (by the system users)	It is virtually certain that some legal issues/ problems will happen	It is virtually certain that there will be a need for organizational restructuring	It is virtually certain that some general issues/problems will happen
6-8 (medium-high)	An error/failure can well happen.	Certain behavioural effects can happen	Possible legal problems/issues could happen	Organizational restructuring is required (depending on needs of service, after system is operational)	General difficulties and problems/issues could well happen
3-5 (medium-low)	It is unlikely that a failure/error will happen	It is doubtful that any behavioural effects will happen	It is improbable that any legal issues/problems will happen	It is improbable that a need for organizational restructuring will happen	It is improbable that general problems/issues and difficulties could happen
1-2 (highly improbable)	It is improbable that an error/fault will happen	It is very improbable that any behavioural effects will happen	It is very unlikely that any legal issues/problems will happen	It is very unlikely that a need for organizational restructuring will happen	It is very unlikely that general issues/problems could happen

Table 3 (D)etectability level analysis

Detectability level	Technological issues	behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (improbable)	It is unlikely or not possible to detect a problematic area	It is unlikely or not possible to detect a user's behavioural effect	It is unlikely or not possible to detect a legal problem	It is unlikely or not possible to detect an organizational problem	It is unlikely or not possible to detect a general issue
7-8 (slight)	The detection of the problematic area is achieved only in particular cases	The detection of a user's behavioural effect is achieved only in particular cases	The detection of a legal problem is achieved only in particular cases	The detection of an organizational problem is achieved only in particular cases	The detection of a general issue is achieved only in particular cases
5-6 (moderate)	It is likely to detect the problem (depending on the situation)	It is likely to detect the user's behavioural effect	It is likely to detect the legal problem	It is likely to detect the organizational problem	It is likely to detect a general issue
3-4 (high)	It is very likely to detect the problem	It is very likely to detect the user's behavioural effect	It is very likely to detect the legal problem	It is very likely to detect the organizational problem	It is very likely to detect a general issue
1-2 (very high)	It is certain to detect the problem	It is certain to detect the user's behavioural effect	It is certain to detect the legal problem	It is certain to detect the organizational problem	It is certain to detect a general issue

Table 4 (R)ecoverability level analysis

Recoverability level	Technological issues	behavioural issues	Ethical issues	Organizational issues	General issues
9-10 (null)	No action is issued for recovery	The system does or does not comply with the user's behavioural effects	The legal framework accepts or rejects the system	A fixed organizational environment is necessary for the system to operate	No recovery action is provided for a general issue
6-8 (low)	Only on the case of failure is the user advised	The system takes under consideration the behavioural effects	The system may be slightly adapted to comply with legal restrictions	The system is in need of a fixed organizational framework with limited adaptations	System may be slightly adapted to meet a general issue
3-5 (high)	Effective action is issued for recovery	The system modification might compensate for user's behavioural effects	The system encloses different versions to meet legal demands	The system may be functioning within various organizational frameworks	Effective recovery action is provided for a general issue
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	The effect of a general issue is completely avoided by the recovery action

The appropriate RPN is calculated for each risk using the values in the table above.

2.7.2 Total risk Estimate and Critical Items Identification

The calculated RPN is used by the involved partners to know which areas are prone to failure and thus take preventive measures to avoid potential shortcoming. High values of RPN show critical areas and should be prioritized. There is an abundance in preventive measures and mitigation actions that can be used to address them such as changes in the design, modification of various parameters, added inspections, test and re-evaluation to preserve quality and many others. An indicative mapping of the level of severity with the RPN number is presented in the following table:

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

Literature [11] suggests that is also important to calculate projects overall risk estimate **Total Risk Estimate (TRE)**

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

Equation 1 Total Risk Estimation Formula

The value of RPN for each identified risk is denoted with $\boldsymbol{RPN_i}$ and $\boldsymbol{n}$ denotes the total number of identified risks.

TRE values range from 0% to 100% representing the total probability of risk regarding a project. TRE values above 17% are considered as 'risky' [12]. Below an example scree plot of ordered RPN values is depicted

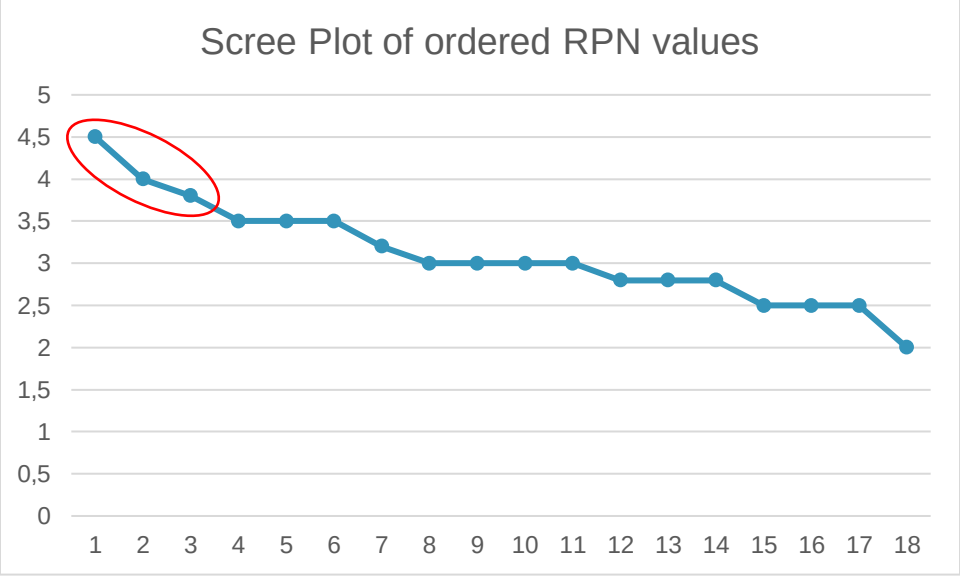

Figure 6 Example of Scree Plot Analysis of RPN values

After analysis of the RPN values, risks are ordered based on their criticality. It is important to include all risks in the list regardless of their level. They are ordered based on the resulted RPN value starting from the highest values and in descending order and a scree plot similar to the figure above is plotted.

2.7.3 Mitigation Actions

Following the identification of critical points, the realization of the strategies and actions that will be used to prevent or remedy the risks takes place. These actions and strategies should also be evaluated based on their success. Usually, risks can be addressed in various ways while many of them might be depended on others. Some general actions for risk mitigation are presented below:

- Actions to eradicate or minimize negative impact of a risk
- Minimize occurrence probability of a risk
- Device actions for early and timely detection of failure

A mechanism for proper selection of these strategies is one of the limitations in FMEA method. Many important factors are not considered like the feasibility or suitability of the proposed strategies and measures. Again the work of Bluvband and Grabov [1] offers a way to evaluate the success of these actions. The first tool regards ranking of each action based on their 'feasibility'. And the second suggestion is a comparison of RPN values before and after remedy.

Feasibility is ranked from 1 to 10 with 1 being the best and 10 the worst.

Table 6 Feasibility of corrective actions

Feasibility of Corrective Action Implementation	**Ranking**
Safety issue and/or non-compliance to regulations No resources available Unacceptable consumption of time/cost/resources Zero chance of success 100% probability of unwanted impact	10
Very remote availability of required resources Almost unacceptable consumption of time/cost/resources Very low chance of success ~90% probability of unwanted impact	9
Remote availability of required resources Near unacceptable consumption of time/cost/resources Remote chance of success ~80% probability of unwanted impact	8
Very low availability of required resources Very high consumption of time/cost/resources Very low chance of success ~70% probability of unwanted impact	7
Low availability of required resources High consumption of time/cost/resources Low chance of success ~60% probability of unwanted impact	6
Rather low availability of required resources Relatively high consumption of time/cost/resources	5

Rather low chance of success ~50% probability of unwanted impact	
Moderate availability of required resources Medium consumption of time/cost/resources Moderate chance of success ~40% probability of unwanted impact	4
Some availability of required resources Rather low consumption of time/cost/resources Some chance of success ~30% probability of unwanted impact	3
Good availability of required resources Low consumption of time/cost/resources Good chance of success ~20% probability of unwanted impact	2
Full availability of required resources Very low consumption of time/cost/resources High chance of success 0-10% probability of unwanted impact	1

When the calculation of the new RPN, after the corrective actions, and the feasibility estimation have been carried out, the following equation can be used to calculate the suitability of the actions

$$\frac{RPN_{iBefore} - RPN_{iAfter}}{F_i} = \frac{\Delta RPN_i}{F_i}$$

Equation 2 Suitability calculation

In the above equation we denote the RPN before and after corrective actions with $\boldsymbol{RPN_{iBefore}}$ and $\boldsymbol{RPN_{iAfter}}$ respectively and with $\boldsymbol{F_i}$ the estimated Feasibility rank. Most suitable actions will have higher number of suitability.

2.7.4 Evaluation of Corrective Actions

After calculating the initial RPN, an evaluation of its effectiveness is required. The calculated RPN and the optimal post-correction RPNs can be used in the following normalized improvement estimate for this purpose:

$$\Delta RPN = \frac{\sum RPN_{iBefore} - \sum RPN_{iAfter}}{\sum RPN_{iBefore}} \times 100\%$$

Equation 3 RPN evaluation equation

A complete and full implementation of EFMEA promises reduction of risks of up to 30%.

3. TERMINET – Expanded Failure Mode and Effect Analysis

3.1 Methodology

The methodology followed within the project is based on the expanded version of FMEA entitled "Expanded Failure Mode Effect Analysis (EFMA)". The process is executed in two stages. The first concerns the identification and mitigation of risks associated with the managerial aspect of the project and includes risks that fall in the types of either general, organizational, behavioural or ethical risks. This forms the ***Project Risk Identification and Mitigation***. The second stage is dedicated to risks and actions associated with the technical part of the project and form the ***Technical Risk Identification and Mitigation*** of the project. Risk identification part includes the calculation of the RPNs and the **S**everity, **O**ccurrence, **D**etectability and **R**ecoverability values. The Mitigation part concerns the realization of suitable action plans and strategies regardless of criticality and the distinction of critical points of failure based on the RPNs scree plot.

3.2 Project Risk Identification

The identified Project Risks for TERMINET can be found in the following tables. The risks are identified using empirical knowledge as well as existing risk lists from previous works that have been adapted for the purposes of TERMINET.

Table 7 General Risk RNP Calculation

WP	Risk event	S	O	D	R	RPN	Risk Level
All	Required background input from other projects that is not available at the specific moment.	4	6	3	3	72	III - Moderate
All	Dependencies with other projects that are not included in the initial software design and development	5	5	6	3	112.5	III - Moderate
WP10	Lack of interest and involvement by Policy makers.	4	6	4	4	96	III - Moderate

Table 8 Managerial Risk RNP Calculation

WP	Risk event	S	O	D	R	RPN	Risk Level
All	Inadequate resource and budget forecasting.	3	5	3	3	30	IV - Slight

All	Inaccurate time estimation and difficulty to follow projects time schedule and deadlines.	5	3	3	3	45	IV - Slight
All	Problems and issues emerged due to partner quitting the project	7	5	1	4	87.5	III - Moderate
All	Missing deadline for a specific work, report, or deliverable	4	4	2	4	48	IV - Slight
All	Problems and issues in management due to the large volume of partners	8	4	2	4	96	III - Moderate
WP10	Inadequate organisation of dissemination events and activities	6	3	4	3	63	IV - Slight
WP8	Inadequate or improper technological facilities to support the actions required by the project.	2	3	2	3	15	IV - Slight

Table 9 Communication Risk RNP Calculation

WP	Risk event	S	O	D	R	RPN	Risk Level
All	Disagreement between partners in a work-package	6	4	3	4	84	III - Moderate
WP10	Lack of commitment by Stakeholders regarding project goals.	3	4	4	2	36	IV - Slight
WP10	Poor teamwork and knowledge sharing mentality among project members.	4	3	6	6	72	III - Moderate

Table 10 Ethics Risk RNP Calculation

WP	Risk event	S	O	D	R	RPN	Risk Level
All	TERMINET developed system(s) are not compliant with national and EU legislation	8	6	1	6	168	III - Moderate
WP11	Changes in EU and national legislation that impact the developments within TERMINET	9	8	2	8	360	II - Severe

The Total Risk Estimate (TRE) value is calculated using Equation 1 and equals to:

TRE = 8.993%

Considering that the value is below 17%, we can safely conclude that TERMINET has a low level of risk. Further improvement of the above metric can be achieved via the realization of adequate and suitable mitigation actions and plans and by reducing risks impact through compensation actions.

In the next step, sorting of the risks using the RPN value takes places. A threshold is used to distinguish critical areas. (Figure 7). The threshold is set to 180 based on empiric estimations and knowledge on the project's specific domain. As can be seen in Figure 7, only one of the identified risks is over the threshold, with an RPN=360. This is an Ethics risk, that is referring to changes in the EU and/or national legislations that could impact the developments within TERMINET.

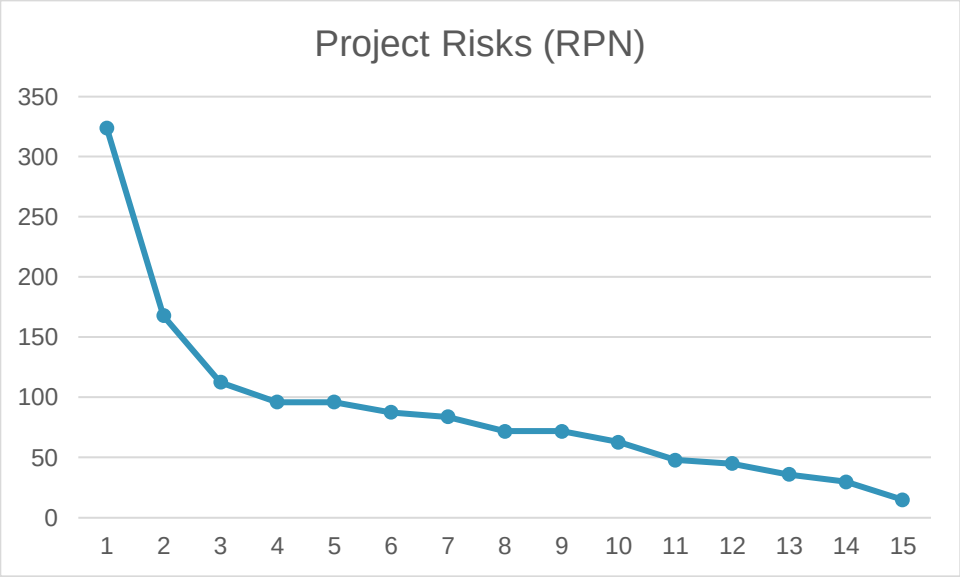

Figure 7 RPN plot for project risks

3.3 Project Risk Mitigation

Following identification and calculation of the relevant RPNs of Project Risks, the realization of mitigation actions takes place. In addition, a value to measure how possible the mitigation action is, is added based on the following table.

Table 11 Mitigation possibility definition

Mitigation Possibility	Definition
High	Little cost is required for this solution
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

The following tables represents the mitigation strategies to address the risks. The risks are divided based on their type General, Organizational, Managerial, Communication, and Ethical. The mitigation possibility and the criticality of each risk are also depicted.

Table 12 General Risks mitigation strategies

Risk event	Mitigation Action Plan	RPN	Risk Level	Mitigation Possibility
Required background input from other projects that is not available at the specific moment.	Avoid major impact to the project by relying to relevant knowledge of other partners until a new one with a more fitting expertise is introduced to the project.	72	III - Moderate	Medium
Dependencies with other projects that are not included in the initial software design and development	Technical assessment regarding potential interdependencies will be conducted alongside the whole development process by the project coordinator and technical manager. Relevant extensions and customisations will be developed to satisfy any discovered dependencies with other projects	96	III - Moderate	Medium
Lack of interest and involvement by Policy makers.	Ensure maximum involvement in projects' training sessions and activities such as workshops and seminars	135	III - Moderate	Medium

Table 13 Managerial Risks mitigation strategies

Risk event	Mitigation Action Plan	RPN	Risk Level	Mitigation Possibility

Inadequate resource and budget forecasting.	Careful planning regarding resource spending aims to minimize that risk. Partners expenditure / budget will be reviewed by them on a semi-annual basis. Package leaders will be responsible to monitor and report to the Technical Manager any deviations about spending. Package leaders will be responsible to prepare detailed activity plans that specifically define responsibilities and effort.	17,5	IV - Slight	High
Inaccurate time estimation and difficulty to follow projects time schedule and deadlines.	Assessment of the problems, of the delays and real time estimations will lead to issuance of new schedules to address loss of time or deadline. Necessary communication is required in the early phases of estimations to avoid shortcoming	45	IV - Slight	High
Problems and issues emerged due to partner quitting the project	Reliance to other partners relevant knowledge until a partner with a more fitting expertise is discovered	100	III - Moderate	High
Missing deadline for a specific work, report or deliverable	STC and PCC can consider taking drastic measures that include shifting of responsibilities and resources for cases that delays are not justified or not remedied straight away. Report regarding delays and spending should also include a plan of mitigation actions to resolve them.	50	IV - Slight	High
Problems and issues in management due to the large volume of partners	Project coordinator and assigned WP leaders expertise and experience in similar assignments ensures efficiency in management. Specific attention to the project governance instruments and modalities is given	70	III - Moderate	Medium
Inadequate organisation of dissemination events and activities	Make a first draft of the dissemination plan (D10.2) early in the project (i.e. M06 of the project) so each representative can promote properly.	63	IV - Slight	High
Inadequate or improper technological facilities to support the actions required by the project.	TERMINET end users (AFS, FPG, PPC, KI, MEVGAL) will ensure that facilities selected for the pilots have dedicated premises and infrastructure for the scopes of the project.	15	IV - Slight	High

Table 14 Communication Risk mitigation strategies

Risk event	Mitigation Action Plan	RPN	Risk Level	Mitigation Possibility
Disagreement between partners in a work-package	A sustained disagreement is resolved by the WP Leader in case that the disagreement persists the PC is called to resolve the situation. STC is responsible for the final decision in case that no consensus has been achieved	96	III - Moderate	Medium
Lack of commitment by Stakeholders regarding project goals.	Engagement and promotion of the benefits of the project for society, economy, environment.	30	IV - Slight	High
Poor teamwork and knowledge sharing mentality among project members.	Enhance teamwork and feedback sharing among partners by organizing workshops and including multiple channels from the early planning stage.	90	III - Moderate	Medium

Table 15 Ethics Risk mitigation strategies

Risk event	Mitigation Action Plan	RPN	Risk Level	Mitigation Possibility
TERMINET developed system(s) are not compliant with national and EU legislation	WP11 will ensure an early in-depth analysis of the relevant legislation and its integration into TERMINET system(s)	147	III - Moderate	Medium
Changes in EU and national legislation that impact the developments within TERMINET	The TERMINET consortium will continuously monitor all relevant legislation to make sure they are followed by.	360	II - Severe	High

3.4 Technical Risk Identification

The following table holds the identified Technological Risks

WP	Risk event	S	O	D	R	RPN	Risk Level

All	Key consortium partner abandons or is temporarily deemed unavailable due to health issues	8	3	2	2	48	IV - Slight
WP1	Poor dissemination and online presence of the project that lead to limited or no TERMINET users	4	4	4	1	40	IV - Slight
WP2	Fail to address all of the end users' needs and requirements	6	7	3	4	147	III - Moderate
WP2	Adaptation of the system does not adhere to certain engagement and satisfaction indices	5	6	5	3	120	III - Moderate
WP2	Development of components involved in laboratory tests or use cases exceed initial planning and are unable to be delivered in time for prototype and testing	4	2	2	3	20	IV - Slight
WP2, WP7	Evaluation of the pilot results does not adequately depict the quality and user acceptance of the developed system	8	5	3	2	100	III - Moderate
WP2, WP8	Lack of understanding about the usability of TERMINET technologies by target user groups and pilot developers due to lack of communication between the involved parties. (development team, partners, pilot operators)	8	5	5	3	160	III - Moderate
WP3, WP4, WP5, WP6	Fail to cover the full number of requirements (WP3, WP4, WP5, WP6)	6	7	3	4	147	III - Moderate
WP3, WP4, WP5, WP6, WP7	Problems arising from longer than anticipated development times, integration of new technologies with steep learning curve, poor performance by individual partners	9	7	1	3	126	III - Moderate
WP3, WP4, WP5, WP6, WP7	Devices and embedded systems that do not adhere to certain levels of stability and maturity or that are unavailable to the project	1	4	2	3	10	IV - Slight
WP7	Low quality of the produced integrated platform	7	3	2	3	52,5	IV - Slight

WP8	Emerge of unplanned technical or integration issues or shortcoming during pilots that could negatively affect projects goals	7	4	2	2	56	IV - Slight
WP8	IT security policies of involved partners that prevent the implementation of one or more use-cases	6	2	2	3	30	IV - Slight
WP8	Confidentiality requirements impose limitations to the information communicated from external AB to the consortium	7	2	1	3	28	IV - Slight

Equation 1 is used to calculate the Total Risk Estimate (TRE) regarding the technological risks.

TRE = 7.746%

Similarly, we can safely conclude that TERMINET is not a risky project, though the estimate can be further improved with the realization of proper mitigation action for the cases that is deemed necessary.

Ordering the RPN values and with the use of a threshold we can determine which risks are critical. (Figure 8). The threshold is set to 170 based on empiric estimations and knowledge on the project's specific domain. As can be seen in Figure 8, none of the identified risks are above the set threshold.

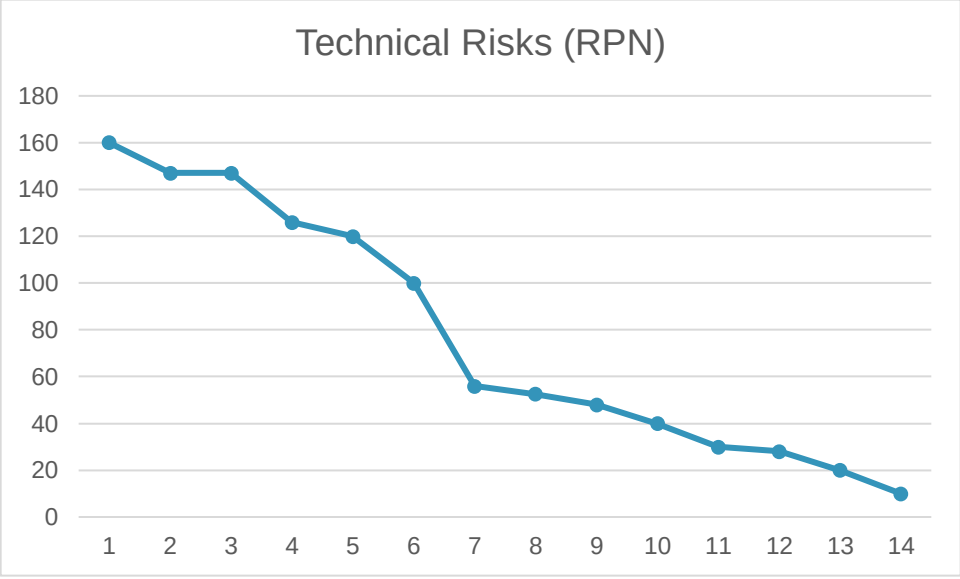

Figure 8 RPN plot for technical risks

3.5 Technical Risk Mitigation

Similar to the procedure followed about managerial risks the strategies to mitigate risks and the relevant mitigation probability is presented.

Risk event	Mitigation Action Plan	RPN	Risk Level	Mitigation Possibility
Key consortium partner abandons or is temporarily deemed unavailable due to health issues	Key areas in R&D are covered by multiple partners and emphasis is given in enhancing internal knowledge sharing to ensure that no delays will be presented until replacement of a partner. Consortium agreement dictates the procedure that a partner is obliged to follow to announce his intention to leave. The procedure will time to the consortium to discover and establish partnership with a fitted replacement of equal or greater competencies. Redundant partners in R&D position ensures that the impact will be minimum, and the new partner will be incorporated in a seamless and efficient manner. In case the unavailability concerns temporal problems redundant partners in such positions will ensure that no delays will be presented.	48	IV - Slight	Medium
Poor dissemination and online presence of the project that lead to limited or no TERMINET users	AB will be responsible for the continuous monitoring of online presence and necessary corrective actions	40	IV - Slight	Medium
Fail to address all the end users' needs and requirements	Careful identification of users and stakeholders' requirements. Assure that all identified use cases aim to satisfy at least one requirement. Assure that every requirement is satisfied by at least one use-case.	147	III - Moderate	Medium

Adaptation of the system does not adhere to certain engagement and satisfaction indices	Design and evaluation will be conducted in an iterative manner until project completion, aiming to continuously provide feedback and introduce relevant changes in the design process. Sensor intelligence and security requires integration of newly introduced concepts even in phases near the end of the project.	120	III - Moderate	Medium
Development of components involved in laboratory tests or use cases exceed initial planning and are unable to be delivered in time for prototype and testing	It is crucial to identify components that are required to test the TERMINET system in the early phases and prioritize their development. In addition, similar components can be considered to mitigate the risk.	20	IV - Slight	Medium
Evaluation of the pilot results does not adequately depict the quality and user acceptance of the developed system	Alongside integration process the proper methods for evaluation will be defined. With this process an adequate number of KPIs as well as other methods will be defined to provide a complete picture regarding the quality level and user acceptance of the developed integrated system.	100	III - Moderate	Medium
Lack of understanding about the usability of TERMINET technologies by target user groups and pilot developers due to lack of communication between the involved parties. (development team, partners, pilot operators)	Relevant training material will be available that will include documents, video as well as tutorials and will aim to introduce TERMINET to its end-users	160	III - Moderate	Medium

Fail to cover the full number of requirements (WP3, WP4, WP5, WP6)	Requirements will be set in an earlier WP, WP2, allowing WP3, WP4, WP5 and WP6 to have the requirements available during the design process. In the case where the solution still fails to meet some requirements involved partners will assess possible redesign of the component and proceed accordingly.	147	III - Moderate	Medium
Problems arising from longer than anticipated development times, integration of new technologies with steep learning curve, poor performance by individual partners	Continuous monitoring of the development progress by TM, STC and PC will allow early detection of problems and corrective actions. Delivery of the platform in time will be ensured by re-scheduling and re-evaluating PMs. Resources for technical meetings are included in resource forecasting and planning.	126	III - Moderate	Medium
Devices and embedded systems that do not adhere to certain levels of stability and maturity or that are unavailable to the project	TERMINET will support device-independent rendering to increase device coverage and simplify migration	10	V - Insignificant	Medium
Low quality of the produced integrated platform	To ensure quality of the produced solution tests will be conducted at different levels of the development and integration process. Unit tests that will ensure quality of low-level components, integration tests that will ensure that developed components are compatible with the rest of the system and end-to-end tests that will ensure quality of the overall workflow.	52,5	III - Moderate	Medium

Emerge of unplanned technical or integration issues or shortcoming during pilots that could negatively affect projects goals	Development process will be conducted in an iterative manner to continuously detect problems and improve technical and integration issues. Validation actions are planned in the early stages of the project work plan to ensure that detection of such problems and realisation of proper actions or alternative technical developments will not affect planning	56	IV - Slight	Medium
IT security policies of involved partners that prevent the implementation of one or more use-cases	Proper communication with the IT security people of demonstrator companies regarding the internals and objectives of the project as well as possible limitations in the system or the company's infrastructure. This will allow realisation of workarounds in order to achieve the required goals	30	IV - Slight	Medium
Confidentiality requirements impose limitations to the information communicated from external AB to the consortium	Consortium members are well connected with relevant managers and operators in different countries that can ensure availability of data and results in the specified timeframe. Thus, alignment of the use cases with the domain of consortium partners and companies is ensured.	28	IV - Slight	Medium

3.6 EFMEA Conclusions

After conducting Risk Analysis employing the EFMA methodology it is concluded that TERMINET does not pose significant risks. To further safeguard project goals and quality, it is deemed important to monitor "moderate" risks.

Identification of critical technological risks has been successful using the EFMEA approach, while also appropriate mitigation plans were proposed.

The TRE for managerial risks is calculated to 9.233% while for the technical risks to 7.746%, values that are considered "low risk".

The analysis of potential risks for both managerial and technical aspects of TERMINET will continue while the project develops, and any updated findings will be reported accordingly.

3.7 Risk Monitoring

Monitoring is responsible for the assessment of the risk management plan that is followed. The main objectives of this process are the continuous assessment of the proposed risk management plan, to keep record of the identified risks that actually occur, to evaluate the adequacy of the agreed mitigation actions, to document newly identified risks and to keep record of historical data about risks with the dates that they were identified or modified. Also, it would be useful to include dates about target completion wherever it is possible.

At the current moment none of the identified risks has emerged. EFMEA analysis and the iterative process of monitoring and re-evaluation of the management plan and Register safeguards that risk levels will be maintained at low levels until the completion of TERMINET project.

References

[1] Z. Bluvband, P. Grabov, and O. Nakar, "Expanded FMEA (EFMEA)," *Proc. Annu. Reliab. Maintainab. Symp.*, no. September, pp. 31–36, 2004, doi: 10.1109/rams.2004.1285419.

[2] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, "Hazard and operability (HAZOP) analysis. A literature review," *J. Hazard. Mater.*, vol. 173, no. 1–3, pp. 19–32, 2010, doi: 10.1016/j.jhazmat.2009.08.076.

[3] C. Spreafico, D. Russo, and C. Rizzi, "A state-of-the-art review of FMEA/FMECA including patents," *Comput. Sci. Rev.*, vol. 25, pp. 19–28, 2017, doi: 10.1016/j.cosrev.2017.05.002.

[4] "Failure_mode_and_effects_analysis @ en.wikipedia.org." [Online]. Available: https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis.

[5] F. I. Khan and S. A. Abbasi, "Techniques and methodologies for risk analysis in chemical process industries," *J. Loss Prev. Process Ind.*, vol. 11, no. 4, pp. 261–277, 1998, doi: 10.1016/S0950-4230(97)00051-X.

[6] "what_if_analysis_with_data_tables @ www.tutorialspoint.com." [Online]. Available: https://www.tutorialspoint.com/excel_data_analysis/what_if_analysis_with_data_tables.htm.

[7] G. L. L. Reniers, W. Dullaert, B. J. M. Ale, and K. Soudan, "The use of current risk analysis tools evaluated towards preventing external domino accidents," *J. Loss Prev. Process Ind.*, vol. 18, no. 3, pp. 119–126, 2005, doi: 10.1016/j.jlp.2005.03.001.

[8] A. Groso, A. Ouedraogo, and T. Meyer, "Risk analysis in research environment," *J. Risk Res.*, vol. 15, no. 2, pp. 187–208, 2012, doi: 10.1080/13669877.2011.634513.

[9] "45d5fa93fe6ecc8b64e989331d181aa220ce04eb @ quality-one.com." [Online]. Available: https://quality-one.com/fmeca/.

[10] "6ea549a639af88c3b0df3e477399c891c6eb1d16 @ www.isixsigma.com." [Online]. Available: https://www.isixsigma.com/tools-templates/fmea/quick-guide-failure-mode-and-effects-analysis/.

[11] Z. Bluvband and P. Grabov, "Failure analysis of FMEA," *Proc. - Annu. Reliab. Maintainab. Symp.*, pp. 344–347, 2009, doi: 10.1109/RAMS.2009.4914700.

[12] "Failure analysis of FMEA". Z.Bluvband, P.Grabov. Reliability and Maintainability, 2009 Annual Symposium - RAMS, pp 344-347