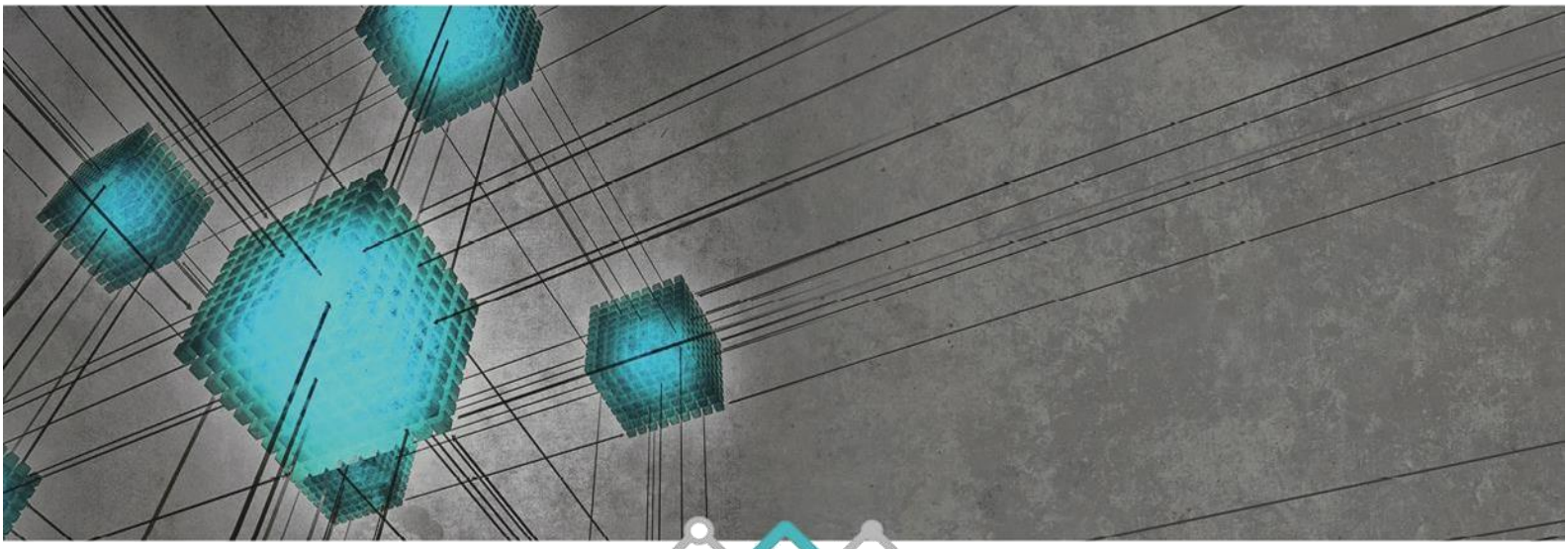

interiot

INTEROPERABILITY
OF HETEREOGENEUS
IOT PLATFORMS.

D1.3

Risk analysis

January 2017

INTER-IoT

INTER-IoT aim is to design, implement and test a framework that will allow interoperability among different Internet of Things (IoT) platforms.

Most current existing IoT developments are based on “closed-loop” concepts, focusing on a specific purpose and being isolated from the rest of the world. Integration between heterogeneous elements is usually done at device or network level, and is just limited to data gathering. Our belief is that a multi-layered approach integrating different IoT devices, networks, platforms, services and applications will allow a global continuum of data, infrastructures and services that will enhance different IoT scenarios. Moreover, reuse and integration of existing and future IoT systems will be facilitated, creating a de facto global ecosystem of interoperable IoT platforms.

In the absence of global IoT standards, the INTER-IoT results will allow any company to design and develop new IoT devices or services, leveraging on the existing ecosystem, and bring them to market as fast as possible.

INTER-IoT has been financed by the Horizon 2020 initiative of the European Commission, contract 687283.

INTER-IoT

Risk Management

Version: Final

Security: Confidential

January 31. 2017

The INTER-IoT project has been financed by the Horizon 2020 initiative of the European Commission, contract 687283

Disclaimer

Executive Summary

The aim of Risk Analysis is to provide a thoughtful study of potential risks that may affect several aspects of the INTER-IoT project and threat the achievement of the expected outcomes. The Risk Analysis is a process that facilitates the identification and management of the potential problems that could undermine key initiatives and projects.

This deliverable is the result of the activity carried out in T1.3 and involves the development of an essential planning tool regarding potential threats, capable to prevent critical problems in advance, and therefore able to avoid severe negative consequences that the development of the INTER-IoT project may suffer.

This deliverable is completely devoted to the continuous monitoring and management of possible risks that may arise during the implementation of the project. Several risks may occur and proper solutions need to be undertaken in order to treat them without affecting the expected outcomes of the project. Some risks have occurred since the beginning of the project and minimization and mitigation tasks have been put in practice as planned. Risk Analysis is a complex process, in which it is necessary to draw on detailed information such as project plans, financial data, security protocols, marketing forecasts and other relevant information. For this reason, the Coordinator along with the Project Coordination Committee (PCC) support continuously monitors the INTER-IoT proceeding and the participation of the project beneficiaries in the work carried out within the project, to identify possible risks early, and be able to take fast contingency actions and decisions about them. In addition to the control and mitigation of any risk, the task is devoted to guarantee quality of the different activities and outcomes from the project.

Risk management has been revisited and reoriented after the feedback provided by the technical experts in the technical review of the project held in Vienna (Austria) in October 2016, from the submitted version in June 2016. The criteria to classify and prioritize the risks has been updated and more practical risks have been introduced, following the principles recommended by the Project Management Body Of Knowledge (PMBOK®) of the Project Management Institute (PMI). Frequent risk management meetings (15 days periodicity) have been held in order to have tight control of the execution of the project.

List of Authors

Organisation	Authors	Main organisations' contributions
UPVLC	Carlos E. Palau Benjamín Molina Eneko Olivares	Template design Initial version Final version edition Reviewed version edition
VPF	Miguel Llop, Pablo Giménez, Alexandre Sánchez, Mª Luisa Escamilla, Eduardo Olmeda	Contribution to risks analysis and internal review
PRO	Miguel Montesinos, Christophe Joubert, Amelia del Rey	Contribution to risks analysis Review of the methodology
RINICOM	Garik Markarian, Eric Carlson	Contribution to risks analysis
UNICAL	Giancarlo Fortino, Wilma Russo, Gianluca Aloi, Pasquale Pace, Raffaele Gravina	Contribution to risks analysis
NEWAYS	Ron Schram, Roel Vossen, Johan Schabbink, Frans Gevers	Contribution to risks analysis
ABC	Alessandro Bassi, Jitka Slechtova	Contribution to risks analysis
SRIPAS	Maria Ghanza, Marcin	Internal Review

Change control datasheet

Version	Changes	Chapters	Pages
1.0	Creation and completion	All	29
1.1	Contributions from partners	All	35
1.2	Review by Editor	All	41
1.3	Internal Review	All	43
1.4	Final version	All	43
2.0	Updated version to be resubmitted	All	76
2.1	Final version	All	78

Contents

List of Figures

List of Tables

Acronyms

AIOTI	Alliance for Internet of Things Innovation
BIP	Best Ideas and Projects
EC	European Commission
IERC	European Research Cluster on the Internet of Things
INTER-LAYER	INTER-IoT Layer integration tools
INTER-FW	INTER-IoT Interoperable IoT Framework
INTER-METH	INTER-IoT Engineering Methodology
INTER-LogP	INTER-IoT Platform for Transport and Logistics
INTER-Health	INTER-IoT Platform for Health monitoring
INTER-META-ARCH	INTER-IoT Architectural meta-model for IoT interoperable platforms
INTER-META-DATA	INTER-IoT Metadata-model for IoT interoperable semantics
INTER-API	INTER-IoT Programming library
INTER-CASE	INTER-IoT Computer Aided Software Engineering tool for integration
IoT	Internet of Things
ITU	International Communications Union
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
M2M	Machine to Machine
W3C	World Wide Web Consortium
ETSI	European Telecommunications Standards Institute
DSM	Digital Single Market
AIOTI	Alliance for Internet of Things Innovation
IoT-EPI	IoT European Platform Initiative
ENISA	European Union Agency for Network and Information Security
NIS	network and information security
ICT	Information and Communication Technology

1 Introduction

This document describes the risk management plan of the INTER-IoT project. The scope of the risk management report is to identify the possible risks for the project and define mitigation plans and actions for each threat or risk in order either to eliminate it or to reduce the consequent negative results that derive from them. The risk management tables provide an analysis of the impact and criticality as a function of likelihood and severity, what has allowed the consortium a more dynamic and flexible reaction when some of the risks have identified and later active.

Risk refers to future conditions or circumstances that exist beyond the control of the project team and that will cause an adverse impact on the project if they happen to occur. Whereas, an *issue* is a current problem that must be dealt with, a *risk* is a potential future problem that has not yet occurred. Risks must not be confused with problems: a *problem* is a risk that has materialized. Therefore, risk management is a proactive process, whereas problem management is reactive.

The Risk Management document is structured and organised as follows:

- Section 2 “Risk Management” describes the risk management approach, which will be used in the context of the INTER-IoT project.
- Section 3 “Identified Risks for the Project” describes the risks that the INTER-IoT consortium has identified and their mitigation plans.
- Section 4 “Conclusion” concludes this deliverable.

The risk management plan and report will be updated according to the project needs and the possible risks that the INTER-IoT consortium will identify during the whole INTER-IoT project lifetime.

2 Risk Management

According to PMBOK[1], a risk is an uncertain event or condition that, if occurs, has an effect on at least one project objective (objectives can include scope, schedule, cost and quality).The existence of risks is unavoidable in any project, as it is intrinsic to the development and implementation phase, whether those threats arise from external or internal causes.

Risk management is a proactive process that is invoked in an attempt to eliminate these potential problems before they occur, and therefore increase the likelihood of success of the project.

The goals of risk management are the following:

- Proactively assess what could go wrong with the project,
- Determine which risks are important to deal with,
- Implement strategies to deal with those risks.

In a project with the complexity of INTER-IoT, it is impractical to rely on light analysis in order to determine where risks lie, which risks are acceptable and which require to apply mitigating actions. It is necessary to use a risk management structured approach or procedures in order to expose risks and address them objectively and consistently.

In the INTER-IoT project, the management approach provides mechanisms to identify and resolve various potential project risks, which can be considered as particular internal or external factors, ensuring efficient implementation of necessary corrective actions. Even if it is not possible to predict all possible risks, it is advisable to identify and assess a set of potential risks related to the project. In this respect, the general INTER-IoT philosophy includes the following pillars:

- **Effective project management**: The management structures and procedures ensure that project management can closely supervise the delivery of the expected results. The INTER-IoT Consortium is composed of organisations which have already successfully carried out several EU projects.
- **Contingency planning**: The work plan has been designed to allow for effective contingency planning in case of all major risks. For every risk a strategy will be developed considering the possibility to avoid the risk, the plan for reducing the probability of its occurrence and in the case of materialisation of the risk, the plan for minimizing the impact on the project overall objectives and compromises.
- **Multiple loosely coupled objectives**: Finally, even if the goal of the project is to demonstrate the full operation of the INTER-IoT framework, the remaining extensions and components can be decoupled and exploited independently.

With the use of risk management procedures, the project team is able to mitigate risks, which means that it can take steps to reduce them to a level that is acceptable for the project consortium. These steps may take the form of technical measures to reduce the probability or impact of a risk occurring, or they may take the form of non-technical measures, used to overcome technical limitations.

[1] http://www.pmi.org/pmbok-guide-standards/foundational/pmbok

The use of risk management procedures is very important. Without the use of risk management procedures, the project consortium can take insufficient steps to mitigate a risk and the consequences may include failure to meet the project objectives, commercial and financial harm to the project partners and project results users, loss of reputation and potential legal actions.

On the other hand, it is equally possible that the project consortium takes unnecessarily draconian steps to mitigate risks. The impact of such unnecessary steps and procedures may include incurring additional unnecessary management effort, and from the technical point of view, reducing system performance.

The INTER-IoT project tries to take the necessary steps for all the identified risks, and avoid unnecessary procedures. The next section describes the proposed risk management processes. INTER-IoT uses a traditional approach for risk management and uses well known and established procedures. So the following paragraphs do not include knowledge produced by the project but rather existing procedures that the INTER-IoT project chose to use for managing the risks within the project.

2.1 Risk Management Procedure

The risk management procedure which will be used in the INTER-IoT project is summarized in Figure 1 and consists of the following activities and steps:

- **Step 0** – Plan: Plan Risk Management is the process of defining how to conduct risk management activities for the INTER-IoT project, preparing all the other steps or processes and providing sufficient resources and time for risk management activities and establishing an agreed-upon basis for evaluating risks.
- **Step 1** - Identify: The project searches for possible risks and identifies the risks before they become problems.
- **Step 2** - Estimate: The project transforms each risk into useful information. This includes evaluating impact, probability, timeframe, classification and priority of every risk. This information can be used for making decisions.
- **Step 3** - Mitigate: The project creates mitigation actions both for the present and the future in order to prevent, reduce or eliminate negative results of the risk. In addition, the project creates implementation plans for these mitigation actions.
- **Step 4** - Monitor: Each partner responsible for a risk monitors the risk's indication and mitigation plan. If the risk for some reason is not mitigated correctly, according to the mitigation plan, or the risk information has changed, the project identifies it as a new risk and the procedure restarts from the Step 1.

Moreover, communication happens throughout all the activities of the risk management. Through the communication, project partners provide information and feedback, both internal and external to the project, relating to the risk activities, as well as identification and mitigation of current and emerging risks.

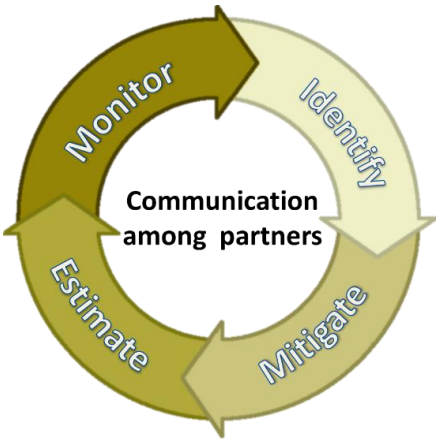

Figure 1: INTER-IoT Risk Management procedure

2.2 Risk Identification

Risk identification is an iterative process that has the aim of determining which risks may affect the project and documenting its characteristics. All INTER-IoT partners are concerned with risk detection and identification. When a risk is detected, it is reported to the Project Coordinator or to the concerned Work Package Leader depending on the context of the risk.

The Project Coordinator or the Work Package leader is responsible for cataloguing the risk according to a defined template, created in a Google sheet for the whole INTER-IoT project. The person responsible for cataloguing the risk is also on duty on performing the risk estimation, mitigation and monitoring processes. Each time a new risk is detected, the Project Coordinator, along with the Project Management Committee, shall manage it.

In order to help the identification process, project risks will be divided into classes listed below:

- **Project Management and Organisation**: Likelihood of failure to meet project milestones. This class of risks will be managed by the Project Coordinator,
- **Technical**: Likelihood of failure of development process. This class of risks will be managed by the Work Package Leader.

Each identified risk refers only to a single class type; nevertheless, the same cause may be at the origin of different risks (within the frame of the above classification).

In addition, the INTER-IoT risk management classifies the risks into the following categories:

- **Technology risks**: Risks derived from the software and hardware technologies, which are being used for developing the system.
- **Usability risks**: Risks that result from the tools, presentation, and use of features that may render the whole system less usable than envisaged or anticipated.
- **Organisation risks**: Risks associated with the people and partner's organisations comprising the project team.
- **Business risks**: Risks related to the market awareness about the project results, competition product acceptance and IPR handling.

The above categories may be updated in the future according to project needs.

The risk identification process generates a risk catalogue that is being updated throughout all the project lifecycle. In the INTER-IoT project, we have used a Google Sheet as an agile tool

for keeping the risk catalogue up to date, being available for all work package leaders. The aspect of this tool is shown in the figure below:

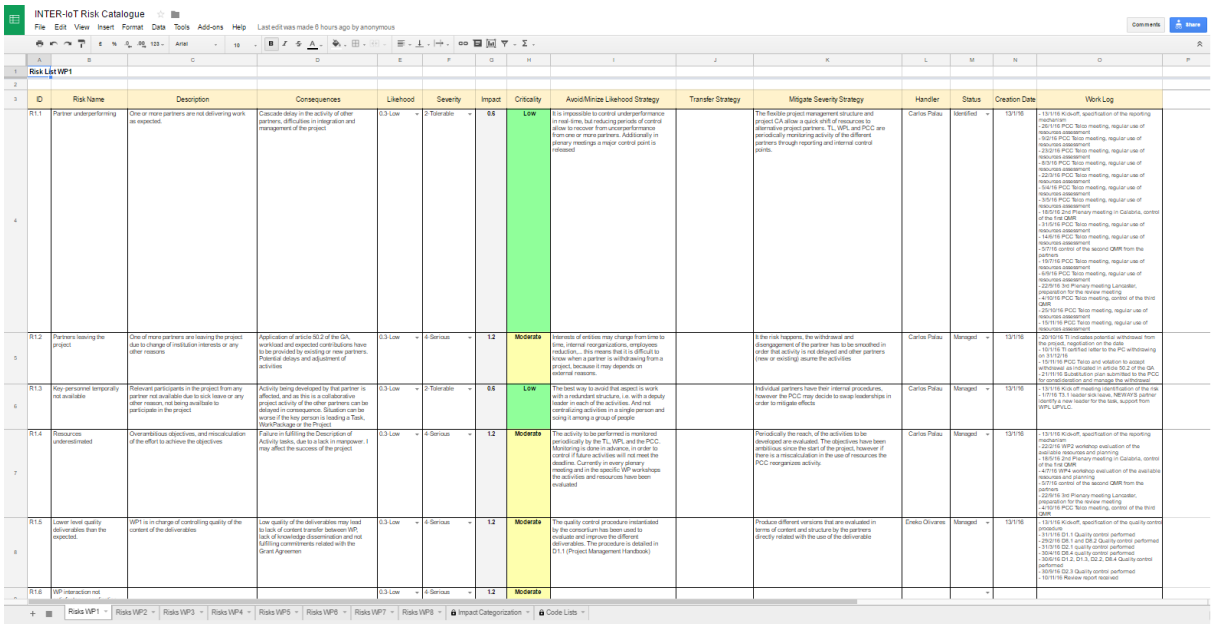

Figure 2: Screenshot INTER-IoT Risk Management shared document

Each Work Package has its own sheet, being each Work Package leader responsible for managing the risks related to its Work Package. For each risk, a set of attributes are being used:

- ID (Risk coding will make reference to the WP it is associated with (e.g. first risk identified for WP1 will be coded as R1.1).
- Risk Name
- Description
- Consequences
- Likelihood
- Severity
- Impact
- Criticality
- Avoid/Minimize Likelihood Strategy
- Transfer Strategy
- Mitigate Severity Strategy
- Handler
- Status
- Creation Date
- Work Log

In the Risk Identification Process, the following risk attributes are registered:

Table 1: Attributes registered in the Risk Identification Process

ID	Risk ID: RP.N, being P the WP number, e.g. R1.1 is the risk 1 of WP1.
Risk Name	Short name of the risk.
Description	Full description of the risk, in terms of the situation that produces the risk, rather than the consequences.
Consequences	Description of the consequences that may happen if the risk would finally occur.
Handler	Responsible for handling the risk and implementing the appropriate strategies described for the risk.
Status	Pending (nothing done but identification and description), Managed (strategies being implemented), Closed (Risk won't occur).
Creation Date	Date when the risk was recorded.
Work Log	Comments about actions done about the risk.

2.3 Risk Estimation

After the risks are identified, they are assessed in terms of their likelihood, which is the subjective probability of their occurrence; and the risk severity, which is the expected impact the project will suffer if the risk happens. Each risk is classified by a risk level based on its likelihood and severity (with risks with higher likelihood and/or higher severity being on a higher level). For each risk level the INTER-IoT partners will undertake appropriate actions.

From the risk severity and likelihood we have determined two heuristic functions and we have calculated the impact and the criticality what has been used in order to be able to prioritize the risks.

Very low level risks are placed on a watch list or adding a contingency reserve, as they don’t deserve more attention because they don’t affect the project too much. These risks don’t require proactive management action (and are considered again only if their likelihood increases).

All the other risks need to be further considered and mitigation activities need to be planned. For these risks a structured description is formed with the risk description and its impact. The information recorded or updated at this process about each risk is the following:

Table 2: Attributes updated in the Risk Estimation Process

Description	Full description of the risk, in terms of the situation that produces the risk, rather than the consequences
Consequences	Description of the consequences that may happen if the risk would finally occurs
Likelihood	Probability of the risk to occur.
Severity	Level of impact that the project will suffer if the risk finally occur.

Impact	Calculated value on the basis of Likelihood and Severity.
Criticality	Impact categorization.
Handler	Responsible for handling the risk and implementing the appropriate strategies described for the risk
Status	Pending (nothing done but identification and description), Managed (strategies being implemented), Closed (Risk won't occur)
Work Log	Comments about actions done about the risk

The description of the likelihood, severity and impact is shown below.

2.3.1 Risk Likelihood

Risk likelihood is classified in one of the following possible values, attending to the probability of the risk to occur:

- **Very low** (occurrence probability 10%): The probability of the risk is very low or its occurrence is late in relation to the project lifetime.
- **Low** (occurrence probability 30%): The probability of the risk is low and there is a small opportunity to occur.
- **Moderate** (occurrence probability 50%): The risk will occur with a good probability.
- **High** (occurrence probability between 70%): The probability of the risk is high.
- **Very high** (occurrence probability 90%): The probability of the risk is very high or almost certain.

2.3.2 Risk Severity[2]

Risks are classified with respect to the level of impact that the project will suffer if the risk finally occur. Their seriousness is classified into the following categories:

- **Insignificant**: Impact of the risk for the project is very low and does not affect any of its objectives.
- **Tolerable**: Impact of the risk for the project is low and effects specific modules of the project without affecting its global objectives.
- **Moderate**: Impact of the risk for the project is medium, however the effects in different modules can have a high impact in the objectives of the project.
- **Serious**: The risk impacts the main contractual requirements of the project but without impact on or redefinition of the critical path.
- **Devastating**: The risk impacts the main objectives of the project on the critical path.

[2] After the technical review and advise from the technical reviewers an assessment of the risk severity has increased the levels from four to five introducing a new severity level “Moderate”

2.3.3 Risk Level

The risk level has been calculated using the following matrix, in order to provide the impact and the risk level. The impact is calculated as a product between the likelihood and the severity (catalogued from 1: insignificant to 5: devastating), and the impact is translated into the risk level. According to the Figure 2 each risk can be classified into one of the following levels (for each of the five risks levels different actions must be taken by the project partners):

- **Risk Level 1** (very low level): These level risks are included in the risk report and reviewed by the Project Coordinator or Work Package Leader concerned, to check possible variation of its estimations. These risks remain in the report to be reviewed for any change in their level. Impact lower than 0,3.
- **Risk Level 2** (low level): A “risk handler” is assigned to the risk to monitor the risk evolution. The “risk handler” reports to the Project Coordinator or Work Package Leader concerned. Actions are evaluated in order to reduce the risk. Impact between 0,3 and 1.
- **Risk Level 3** (moderate level): Same actions as for Level 2. In addition, definitions of specific mitigation plans are created. The Project Coordinator or Work Package Leader concerned with the risk defines these plans and identifies also possible trigger events to start them. The risk handler monitors the risks and these trigger events. Impact between 1 and 2.
- **Risk Level 4** (high level): Same actions as for Level 3. In addition, the Project Coordinator and Work Package Leader concerned with the risk informs the Project Coordination Committee. The Project Coordination Committee is involved in the design of the mitigation plans and directly assigns the “risk handler”. The defined mitigation plans start immediately. Impact between 2 and 3.
- **Risk Level 5** (critical level): Same actions as level 4. Due to the seriousness of these level risks, catastrophic for the project, the Project Coordination Committee plans an extraordinary meeting in a week in order to decide the status of the project and how the project will continue. Impact higher than 3.

The level of each risk is determined using the matrix in Table 3 which has as rows the risk likelihood and as columns the risk severity for the project.

Table 3: Impact/Value Matrix

Likelihood / Severity	1	2	3	4	5
10%	0.1	0.2	0.3	0.4	0.5
30%	0.3	0.6	0.9	1.2	1.5
50%	0.5	1	1.5	2	2.5
70%	0.7	1.4	2.1	2.8	3.5
90%	0.9	1.8	2.7	3.6	4.5

Using the cell values, we have classified the risk impact in the following groups; the impact matrix is depicted in figure 2:

- Very Low: 0.1 – 0.3
- Low: 0.4 - 1

- Moderate: 1.1 – 2
- High: 2.1 - 3
- Critical: >3

Likelihood / Severity	Insignificant	Tolerable	Moderate	Serious	Devastating
Very Low	Very Low	Very Low	Very Low	Low	Low
Low	Very Low	Low	Low	Moderate	Moderate
Moderate	Low	Low	Moderate	Moderate	High
High	Low	Moderate	High	High	Critical
Very High	Low	Moderate	High	Critical	Critical

Figure 3: Risk Levels – Impact/Value Matrix

2.4 Risk Mitigation

Mitigation activities/strategies can be generally either characterised as prevention type activities/strategies or as correction type activities/strategies:

- The term *prevention type* refers to the mitigation activities/strategies, which have as a target the elimination of a possible risk before it occurs. This will also have as a result the elimination of the negative impact for the project.
- The term *correction type* refers to mitigation activities and strategies, which aim at the reduction of the negative results of a risk after it has occurred.

Several risk response strategies are available depending on the risk. The strategies for managing negative risks in the INTER-IoT project are the following::

- **Avoidance strategies** (prevention type): Avoidance strategies are targeting at avoiding the risk or reducing the likelihood that the risk will occur.
- **Transfer strategies** (prevention type): Transferring some or all of the negative impact of the risk to a third party if possible. Transferring a risk simply gives another party responsibility for its management, it does not eliminate the risk It may be empty in most situations in the project, as it's not easy to transfer risk responsibility..
- **Mitigate strategies** (correction type): Mitigation is the strategy for reducing the effects or impact of a risk if it occurs. Severity mitigation might target linkages that determine the severity. It also may contain the contingency strategies that are targeting at finding a back-up solution if the worst happen.

As the impact and consequently the risk level is the product of two factors (likelihood and severity), the strategies have to affect the two axis.

Unmanageable risks, that is, risks for which the Project Coordinator or concerned Work Package Leader is not able to deal with in a satisfactory way, shall be highlighted and a proper justification on the lack of mitigation actions should be provided.

Mitigation activity shall be followed-up by the Project Coordinator or Work Package Leader concerned, who supervises its accomplishment and verifies the effectiveness of the performed actions.

Risk Mitigation process is performed iteratively by the risk handler, who reports to the Work Package leader or Project Coordinator about changes in the strategies for mitigating risks as described above. This process updates the following risk attributes:

Table 4: Attributes updated in the Risk Mitigation Process

Avoid/Minize Likelihood Strategy	Description of the strategy for avoiding the risk or minimizing the likelihood that it will occur.
Transfer Strategy	Description of the strategy for transferring the risk to a third party if possible. It may be empty.
Mitigate Severity Strategy	Description of the strategy for mitigating the effects of a risk if it occurs
Handler	Responsible for handling the risk and implementing the appropriate strategies described for the risk
Status	Pending (nothing done but identification and description), Managed (strategies being implemented), Closed (Risk won't occur)
Work Log	Comments about actions done about the risk

2.5 Risk Monitoring

Each identified risk, other than Level 1 risks, shall have a handler. A risk handler is responsible for monitoring the risk and reporting about it. The Project Coordinator, Technology Director or Work Package Leader concerned, shall identify the handlers for all the risks that have been identified within Level 2 and Level 3.

The Project Coordination Committee shall identify the handlers for all the risks that have been identified within Level 4 and Level 5. In addition, for Level 5 risks, the Project General Assembly plans an extraordinary meeting in order to decide the status of the project and how the project will continue.

Each risk handler reports periodically to the Project Coordinator, Technology Director, Scientific Director or Work Package Leader concerned about the risks he/she is in charge of. The Project Coordination Committee and the Project General Assembly discuss during their meetings the risks of Level 4 and Level 5 respectively.

Risk management will be continuously handled by the partners. Every periodic telco will have a dedicated section in the agenda devoted to risk management, and at every plenary meeting there will be a session in order to manage and control risk management. Special emphasis is addressed at risks with higher impact. Additionally each risk handler may assess the risk and may take actions addressed to avoid/minimize likelihood and mitigate severity when an individual input related with the risk happens.

2.6 Risk definition and information table

The following table contains the same information present in the shared document used for management flexibility. The representation in table format is used to show the information in a more comprehensive way.

Table 5: Risk information table

Risk subcategory			
<technology, usability, organisation, business>			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
Rx.y	<Risk Name>	Detailed description of the risk	Description of the consequences of the risk to become true, and not mitigating it.
Likelihood	**Severity**	**Impact**	**Criticality**
<Very Low, Low, Moderate, High, Very High>	<Insignificant, Tolerable, Moderate, Serious, Devastating>	<Likelihood x Severity>	<Following figure 2>
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Describe how to avoid/minimize likelihood of the risk in order to decrease it in order to reduce the impact		Describe how to affect the severity of the risk in order to decrease it in order to reduce the impact	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
<Identified person who handles the risk>	<Identified, Managed, Closed>	<Risk Creation Date>	<description of the transfer strategy>
Work Log			
Identification and date of associated events, which the handler of the risk tracks the relevant events associated with the risk, e.g. risk changes status from identified to managed or from managed to closed, or the description and handler of the risk changes.			

3 IDENTIFIED RISKS FOR THE PROJECT

This section provides information tables of the risks that the Inter-IoT consortium has identified until the date of the delivery of this document. The risks have been classified per WP in order to provide a more dynamic risk management. The objective of organising the risks in this way allows the management of project specific related risks.

The risks have been labelled using the categories described in section 2.2.. Risk management is performed in three iterative steps: (i) at task level; (ii) work package level; and (iii) at project level.

Each time the Inter-IoT consortium identifies a new risk, the corresponding risk information table is added to an online document and a snapshot of this document, will be presented in the corresponding deliverables.

The list of risks presented in this document have been updated according to the project needs and the possible threats that the Inter-IoT consortium will identify during the whole Inter-IoT project lifetime. And additionally after the technical review meeting the risks have been revisited in order to make them more project-specific.

The following subsections represent the risk classified per WP in order to group them in a more comprehensive way. The day by day management is being performed by means of shared document accessible by every member of the consortium in which the Project Coordinator, Software Architect, Work Package Leaders, Task Leaders and specifically Risk Handlers update the different risks and consequently the worklog as actions are taken. Periodically as indicated in the risk management procedure, the PCC in plenary meetings, periodical telcos or specifically target events (e.g. workshops or telcos related with a specific activity) risks are assessed as a whole.

3.1 WP1 Related Risks

Table 6: Underperforming partner

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.1	Underperforming partner	One or more partners are not delivering work as expected	Cascade delay in the activity of other partners, difficulties in integration and management of the project

Likelihood	**Severity**	**Impact**	**Criticality**
Low	Tolerable	0.6	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
It is impossible to control underperformance in real-time, but reducing periods of control allow to recover from underperformance from one or more partners. Additionally in plenary meetings a major control point is released	The flexible project management structure and project CA allow a quick shift of resources to alternative project partners. TL, WPL and PCC are periodically monitoring activity of the different partners through reporting and internal control points.

Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau	Managed	13/1/2016	N/A

Work Log
- 13/1/16 Kick-off, specification of the reporting mechanism - 9/2/16 PCC Telco meeting, regular use of resources assessment - 8/3/16 PCC Telco meeting, regular use of resources assessment - 5/4/16 PCC Telco meeting, regular use of resources assessment - 3/5/16 PCC Telco meeting, regular use of resources assessment - 18/5/16 2nd Plenary meeting in Calabria, control of the first QMR, change of the risk from Identified to Managed in order to control imbalances in the use of resources - 14/6/16 PCC Telco meeting, regular use of resources assessment - 5/7/16 control of the second QMR from the partners - 19/7/16 PCC Telco meeting, regular use of resources assessment - 22/9/16 3rd Plenary meeting Lancaster, preparation for the review meeting - 4/10/16 PCC Telco meeting, control of the third QMR - 25/10/16 PCC Telco meeting, regular use of resources assessment - 30/10/16 Notification of TI withdrawal assessment of the impact on resources - 19/11/16 PCC Telco meeting, regular use of resources assessment - 13/12/16 PCC Telco meeting, regular use of resources assessment - 17/01/17 PCC Telco meeting, regular use of resources assessment. Evaluation of the termination report of TI in order to assess pending tasks and activities

Table 7: Partners leaving the project

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.2	Partners leaving the project	One of more partners are leaving the project due to change of institution interests or any other reasons	Application of article 50.2 of the GA, workload and expected contributions have to be provided by existing or new partners. Potential delays and adjustment of activities

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Interests of entities may change from time to time, internal reorganizations, employees reduction,... this means that it is difficult to know when a partner is withdrawing from a project, because it may depends on external reasons	It the risk happens, the withdrawal and disengagement of the partner has to be smoothed in order that activity is not delayed and other partners (new or existing) assume the activities

Handler	Current Status	Creation Date	Transfer Strategy
Carlos Palau	Managed	13/1/2016	N/A

Work Log
- 20/10/16 TI indicates potential withdrawal from the project, negotiation on the date. Risk changed from Identified to Managed. Implementation of the mitigation strategy to reduce severity. TI agreed to withdraw on 31/12/16 in order to finish the pending tasks in WP2. In order to mitigate impact on WP3, WP3 and WP5, a contingency plan was placed with some partners supporting the activity of TI. - 10/11/16 TI certified letter to the PC withdrawing on 31/12/16 - 15/11/16 PCC Telco and voting to accept withdrawal as indicated in article 50.2 of the GA - 21/11/16 Substitution plan submitted to the PCC for consideration and manage the withdrawal - 21/12/16 Request for amendment submitted, negotiation with EC and TI. - 27/01/17 Termination report submitted to EC, the risk cannot considered closed but the Severity has been reduced

Table 8: Key-personnel temporally not available

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.3	Key-personnel temporally not available	Relevant participants in the project from any partner not available due to sick leave or any other reason, not being availbale to participate in the project	Activity being developed by that partner is affected, and as this is a collaborative project activity of the other partners can be delayed in consequence. Situation can be worse if the key person is leading a Task, WorkPackage or the Project

Likelihood	**Severity**	**Impact**	**Criticality**
Low	Tolerable	0.6	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
The best way to avoid that aspect is work with a redundant structure, i.e. with a deputy leader in each of the activities. And not centralizing activities in a single person and doing it among a group of people	Individual partners have their internal procedures, however the PCC may decide to swap leaderships in order to mitigate effects

Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau	Managed	13/1/2016	N/A

Work Log
- 13/1/16 Kick-off, specification of the reporting mechanism - 22/2/16 WP2 workshop evaluation of the available resources and planning. Risk is updated from identified to managed. - 18/5/16 2nd Plenary meeting in Calabria, control of the first QMR - 4/7/16 WP4 workshop evaluation of the available resources and planning - 5/7/16 control of the second QMR from the partners - 22/9/16 3rd Plenary meeting Lancaster, preparation for the review meeting - 4/10/16 PCC Telco meeting, control of the third QMR

Table 9: Resources underestimated

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.4	Resources underestimated	Overambitious objectives, and miscalculation of the effort to achieve the objectives	Failure in fulfilling the Description of Activity tasks, due to a lack in manpower. I may affect the success of the project

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
The activity to be performed is monitored periodically by the TL, WPL and the PCC. Monitoring is done in advance, in order to control if future activities will not meet the deadline. Currently in every plenary meeting and in the specific WP workshops the activities and resources have been evaluated	Periodically the reach, of the activities to be developed are evaluated. The objectives have been ambitious since the start of the project, however if there is a miscalculation in the use of resources the PCC reorganizes activity.

Handler	Current Status	Creation Date	Transfer Strategy
Carlos Palau	Managed	13/1/2016	N/A

Work Log
- 13/1/16 Kick-off, specification of the reporting mechanism - 22/2/16 WP2 workshop evaluation of the available resources and planning. Risk updated from identified to managed - 18/5/16 2nd Plenary meeting in Calabria, control of the first QMR - 4/7/16 WP4 workshop evaluation of the available resources and planning - 5/7/16 control of the second QMR from the partners - 22/9/16 3rd Plenary meeting Lancaster, preparation for the review meeting - 4/10/16 PCC Telco meeting, control of the third QMR - 22/11/16 WP3/WP4 cluster, redistribution of the activity and efforts in different tasks of the WP as it was detected an imbalance between T3.1 and T3.2 and between T3.3 and T3.4.

Table 10: Lower level quality deliverables than the expected

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.5	Lower level quality deliverables than the expected	WP1 is in charge of controlling quality of the content of the deliverables	Low quality of the deliverables may lead to lack of content transfer between WP, lack of knowledge dissemination and not fulfilling commitments related with the Grant Agreement

Likelihood	**Severity**	**Impact**	**Criticality**
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
The quality control procedure instantiated by the consortium has been used to evaluate and improve the different deliverables. The procedure is detailed in D1.1 (Project Management Handbook)	Produce different versions that are evaluated in terms of content and structure by the partners directly related with the use of the deliverable

Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau	Managed	13/1/2016	N/A

Work Log
- 13/1/16 Kick-off, specification of the quality control procedure - 31/1/16 D1.1 Quality control performed - 29/2/16 D8.1 and D8.2 Quality control performed - 31/3/16 D2.1 quality control performed - 30/4/16 D8.4 quality control performed - 30/6/16 D1.2, D1.3, D2.2, D8.4 Quality control performed - 30/9/16 D2.3 Quality control performed - 10/11/16 Review report received. Risk updated from Identified to Managed. Task Forces creation in order to improve deliverables and reduce the severity of the measure. Handling of the risks transferred to WP leaders, in order to control specifically the associated risk. - 15/11/16 Mitigation measure taken for D4.1 in order to have the adequate quality. Risk transferred to WP4 leader.

Table 11: WP interaction not satisfactory, coordination not efficient.

Risk Nº	Risk Name	Risk Description	Consequences
R1.6	WP interaction not satisfactory, coordination not efficient.	There are different links between WP in INTER-IoT. The most critical are related between WP2 and WP3-5 and between WP3-5 and WP6. Additionally inter technical WP (WP3-5) is required.	The outcomes from WP2, specially the requirements and the scenarios are needed for the technical WP, if they are not adequate technical WP will not be able to start and produce adequate products for the pilots in WP6. At the same time WP3 results are needed by WP4 and WP3 and WP4 are both linked with WP5 and the methodology. All these communication paths have to be open and clear.

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Hold periodical meetings between WP leaders, a part of the plenary meetings. Share documents and intermediate reports and have continuous communication. Hire a senior Software Architect in order to homogenise the development of the components.	The flexible management strategy used in the project allow to detect malfunctions and react placing more effort in a specific task if a problem of communication has existed and some component has not developed or does not fit the required specification for integration. Modification of the schedule of different tasks in order to improve communication

Handler	Current Status	Creation Date	Transfer Strategy
Carlos Palau/Miguel A. Llorente	Managed	13/1/16	N/A

Work Log

- 22/2/16 WP2 workshop evaluation of the available resources and planning. Risk updated from identified to managed. Decision to amend the DoA and advance the start of WP3 to May 2016 (M5) to reduce likelihood of the risk and improve communication with WP2 and later with WP4.
- 24/6/16 meeting between WP2/WP3/WP4 and relevant task leaders in Valencia in the framework of the IoT-EPI meeting to fix development details between WP.
- 22/9/16 Plenary meeting in Lancaster (UK) workshop between WP2/WP3/WP4/WP5 leaders to homogenise development details and reduces communication failures between WP
- 1/11/16 Appointment of Miguel A. Llorente (PRO) as Software Architect of the project in order to follow recommendation from the technical reviewers and improve communication between WP
- 21/11/16 joint development workshop in Valencia for WP3 and WP4.

- 1/12/16 Traversal task force creation in order to homogenise the link between the new version of D2.3 with D3.1 and D4.1. The resubmission of the deliverable was seen as an opportunity to improve communication.

Table 12: Gathered open call proposals do not provide adequate contributors

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.7	Open Call does not attract a critical mass of contributors	INTER-IoT open call requires that a good number and quality of contributors is received by the consortium. The risk exists that due to the high number of open calls launched by H2020 projects, and the publicity means selected not many proposals are received by the consortium	The first consequence is that one goal of the project is not achieved, that is the gathering and creation of an ecosystem around INTER-IoT. The second consequence is that the INTER-DOMAIN use case could not be populated and the third is that the part of the budget of the project could not be executed.

Likelihood	Severity	Impact	Criticality
Moderate	Devastating	2,5	High

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
The strategy to minimize the likelihood is to provide as much publicity as possible and promote the open call in different forums and contacts from the partners. Use of the IoT-EPI network and other alternative communication channels. Provide the best information as possible in terms of benefits and clarification of the requested contributions.	The severity cannot be mitigated, as there is only one open call and no budget can be left for as second open call. Not having a high number of proposals may harm the quality of the objectives to be achieved.

Handler	Current Status	Creation Date	Transfer Strategy
Carlos Palau	Closed	13/1/16	N/A

Work Log

- 22/6/16 IoT-EPI meeting in Valencia, the open call is pre-announced in a Task Force meeting. The status of the risk changes from identified to Managed
- 22/9/16 Plenary meeting in Lancaster (UK) strategy of promotion of the open call agreed between partners
- 13/10/16 Launching of the open call, it coincided with the IoT-EPI event in Vienna, different publicity mechanisms implemented
- 13/11/16 Evaluation of the risk and new wave of publicity through the previous channels and new identified channels.
- 13/12/16 Evaluation of the risk and new wave of publicity through the previous channels and new identified channels, including a webcasting to proposers
- 10/1/17 Evaluation of the risk, and extension of one week in the submission procedure
- 20/1/17 Close of the open call submission procedure and close of the risk with 63 proposals received.

Table 13: Open Call outcomes do not provide adequate results

Risk subcategory			
Organisations			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.8	Open Call outcomes do not provide adequate results in order to meet the associated objectives defined in DoA.	Although a high critical mass of proposals is received, the quality has to be evaluated in order to fulfil the project requirements.	If the received contributions do not have the needed quality and technical contributions the goal pretended by the open call will not be achieved.

Likelihood	Severity	Impact	Criticality
Moderate	Serious	2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Explanation of the needs in a comprehensive format to potential contributors during the elaboration phase. Selection of expert reviewers in order to select the best proposals for the project.	Intervention of the consortium during the different phases of the open call until the third parties start working with the consortium. The PCC will reduce the severity mainly through the negotiation phase with the selected proposals in order to fine tune their contributions to the goals of INTER-IoT

Handler	Current Status	Creation Date	Transfer Strategy
Carlos Palau	Managed	13/1/16	N/A

Work Log

- 22/6/16 IoT-EPI meeting in Valencia, the open call is pre-announced in a Task Force meeting. The status of the risk changes from identified to Managed
- 22/9/16 Plenary meeting in Lancaster (UK) strategy of promotion of the open call agreed between partners
- 13/10/16 Launching of the open call, it coincided with the IoT-EPI event in Vienna, different publicity mechanisms implemented.
- 30/10/16 Launching of the call for reviewers.
- 13/11/16 Evaluation of the risk and new wave of publicity through the previous channels and new identified channels, including quality components
- 13/12/16 Evaluation of the risk and new wave of publicity through the previous channels and new identified channels, including a webcasting to proposers
- 20/1/17 Close of the open call submission procedure.
- 27/1/17 Selection of the reviewers based on their expertise and avoiding CoI in order to reduce likelihood and severity of the risk

Table 14: Change of the project requirements due to evolution of relevant technology and market landscape

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.9	Change of the project requirements due to evolution of relevant technology and market landscape	The market landscape is changed due to an evolution of the different technologies and influence in the market of technology alliances and standardization organisations.	The project may require an extra effort to adapt to this changes, and include or change some technology decisions made during the execution of the project. The consequence will be to adaptation of some requirements
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Moderate	0.9	Low
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
The selection of the technology and platforms to be integrated in the project have to be consolidated and select the platforms that are most used in the market, but considering the new emergent ones. The consortium will create a market watch in order to monitor in contact with other project within IoT-EPI the market trends.		The development of the different components in INTER-LAYER, INTER-FW and INTER-METH will be as open and flexible as possible in order to be able to adapt to the inclusion of new components.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau	Managed	13/1/16	N/A
Work Log			
- 22/2/16 WP2 workshop, analysis of the risk and change of the status from identified to managed. Creation of the TF to monitor evolution of the market. - 22/6/16 IoT-EPI meeting in Valencia, re-evaluation of the risk and analysis of the technology tendencies - 12/10/16 IoT-EPI meeting in Vienna, presentation of the IoT platforms landscape - 21/11/16 joint development workshop in Valencia, evaluation of the risk			

Table 15: Legal and regulatory constraints are not taken into account in pilots design

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.10	Legal. Regulatory and ethical constraints are not taken into account when designing INTER-IoT or risk the execution of the pilots.	Legal, regulatory and ethical component is a key factor when humans are involved in a project. In the case of INTER-IoT, the risk of not considering these aspects could harm exploitation. Especially in the use case of m-health.	Directly linked with the exploitation of the results in the deployment of the pilots. If legal, regulatory and ethical components are not considered the pilot will have significant drawbacks and the exploitation of the resulting products will not be feasible.

Likelihood	**Severity**	**Impact**	**Criticality**
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Consider the different legal and regulatory constraints in the countries of the deploying pilots (i.e. Spain and Italy) and also at European Level. Extending the analysis to the countries of the partners as a first step. Create an Ethical Advisory Board, including and external Ethical Advisor that support this activity and provide inputs to the consortium.	Validate the developed products periodically with the different legal, regulatory and ethical recommendations in order that an adaptation to a new one reducing the severity of the risk. The mitigation measure is critical in INTER-HEALTH use case.

Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau	Managed	13/1/16	N/A

Work Log
- 13/1/16 Kick-off, specification of ethical, legal and regulatory constraints of the project. - 22/2/16 ASLTO5 checked with the ethical committee of the Italian Health Ministry - 18/5/16 2nd Plenary meeting in Calabria, control of Ethical risks - 22/9/16 3rd Plenary meeting Lancaster, control and evaluation of the risk - 10/11/16 reception of the technical evaluation report, control of the ethical aspects - 31/12/16 completion of the D2.5 that contains the legal and regulatory constraints till this moment - 13/1/17 reception of the ethical report, and evaluation of the risk by the consortium

Table 16: Software Integration

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R1.11	Software Integration	Development of software components by different partners in the consortium may require to manage integration. There is a risk that the integration process requires extra effort.	The main consequence will be lack of effectivity in the development process and not meeting the deadline. Software integration is a process that in the project is present in the different WP, the technical ones producing the generic products and the pilots in which the products will be integrated with the IoT platforms present in the premises of the stakeholders.
Likelihood	**Severity**	**Impact**	**Criticality**
Moderate	Serious	2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Define clear development procedures in order that every partner meets them, at project, workpackage and task level. Nominate a Software Architect that provides clear directives and policies to achieve good integration. Periodically monitor advances of the development in the different components of the project. Develop adequate		Assess the degree of integration quality periodically and create specific task forces if needed. The degree of severity may vary from task to WP and from WP to the whole project. Periodical testing of the software integration as the project evolve. Adequate evaluation of the software interfaces.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau/Miguel A. Llorente	Managed	20/10/16	N/A
Work Log			
- 20/10/16 creation of the risk and management of the risk with the adequate handlers (project coordinator and software architect). Mitigation measures established to improve communication within tasks and between WPs. - 10/11/16 Fixation of weekly telcos and introduction of the use of slack and trello for task assignment in WP3 at task level. And periodical discussions between task leaders and WP leader - 10/11/16 Fixation of weekly telcos and introduction of the use of slack and trello for task assignment in WP4 at task level. And periodical discussions between task leaders and WP leader - 18/11/16 Meeting between Project Coordinator, Software Architect, WP3 leader, WP4 leader in order to improve software integration			

- 22/11/16 Integration workshop related with WP3 and WP4. Guidance to avoid problems in software integration created. - 31/12/16 Release of D3.1, reassessment of the risk. The deliverable includes the definition of the required components to achieve seamless integration of WP3 developed components, and the relationship with WP4 in terms of integration - 15/1/17 Release of D4.1, reassessment of the risk. The deliverable includes the definition of the meta-architecture for platform interoperability and the meta-data model, both in direct link with WP3.

3.2 WP2 Related Risks

Table 17: Legal and regulatory constraints are not taken into account

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R2.1	Legal and regulatory constraints are not taken into account	Legal and regulatory constraints are not taken into account when designing INTER-IoT or risk the execution of the pilots.	Solutions do not comfort to existing laws and have to be modified or are useless for the selected use cases (transport and mHealth).

Likelihood	Severity	Impact	Criticality
Low	Tolerable	0.6	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Introduce legal and regulatory assessment in the early phases of the project (D2.5) and take into account the Policy Report published by AIOTI.	In the case any regulatory or legal constraint appears in a scenario during the pilot deployment, provide a simulated approach where this regulatory or legal constraint is not applicable.

Handler	Current Status	Creation Date	Transfer Strategy
Miguel Llop	Closed	15/6/2016	N/A

Work Log
- 13/1/16 Kick-off, specification of the reporting mechanism. - 22/2/16 WP2 workshop evaluation of the available resources and planning. Risk updated from identified to managed. - 27/10/16 Finish a thorough review of relevant legislation - 31/12/16 Risk closed when D2.5 was submitted.

Table 18: Incomplete requirements

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R2.2	Incomplete requirements	Identified requirements for INTER-IoT are not complete, nor relevant, too complex or unfeasible to achieve.	Technical WP cannot start the design and development process because the requirements do not provide the required information.
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Tolerable	0.6	Low
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Evaluate and re-formulate those requirements which are out of the scope, unfeasible or too complex to attend in INTER-IoT. Remove those requirements which are not related with the objectives of the project.		Perform an analysis of the existing requirements by the task and work package and rewrite them being more concrete and adjusting to the development of the products.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Miguel Llop	Managed	31/1/2016	N/A
Work Log			
- 30/09/16 The task is finished without risk - 22/2/16 WP2 workshop evaluation of the available resources and planning. Risk updated from identified to managed - 10/11/16 Task Force created to fulfil the recommendation of the reviewers and reduce the severity of not prioritised requirements. - 04/12/16 Completion of the requirements review - 31/01/17 D2.3 has been submitted, and the risk remains open and managed as the requirements risk will exist through the whole project.			

Table 19: Scenarios are not feasible

Risk subcategory			
Usability			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R2.3	Scenarios are not feasible	Scenarios are not real or not feasible to be demonstrated in the pilots.	The scenarios do not fulfil the needs of the project, not being significant for the testing of the solutions.
Likelihood	**Severity**	**Impact**	**Criticality**
Very Low	Insignificant	0.1	Very Low
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Propose several scenarios to ensure that at least there will be enough scenarios demonstrated in the pilot deployment to validate all the functional, non-functional, qualitative and quantitative indicators established in the project.		Identify and discard those scenarios that are unfeasible duly justifying the reason and focus on the feasible scenarios for the pilot deployment and validation.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Miguel Llop	Closed	01/2/2016	N/A
Work Log			
- 22/2/16 WP2 workshop evaluation of the available resources and planning. Risk updated from identified to managed - 1/7/16 Modification of the risk description and mitigation strategy after the IoT-EPI meeting in Valencia - 20/11/16 After the Viena technical review the scenarios were redefined, in order to reduce the likelihood of the risk - 31/12/16 T2.4 associated with the risk is finished and the risk closed. The risk will be reopen when WP6 integrates the different components for the pilots.			

Table 20: Stakeholder does not participate in the pilot

Risk subcategory			
Usability/Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R2.4	Stakeholder does not participate in the pilot	Stakeholders identified for participating in the pilot deployments do not engage in the demonstration.	Scenarios, use cases and main interoperability procedures cannot be tested as fixed at the start of the project.

Likelihood	**Severity**	**Impact**	**Criticality**
Moderate	Devastating	2.5	High

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Keep the key stakeholders that will participate in the pilots informed and take into account their needs.	Seek other equivalent stakeholders to participate in the pilot, obtain their agreement and prepare them for conducting the pilot.

Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau/Miguel Llop	Managed	1/2/2016	N/A

Work Log
- 14/2/16 Risk updated from Identified to Managed, during the execution of T2.1, due to a reduced implication of external stakeholders - 15/04/16 Meetings with different stakeholders to inform and involve them and reduce the severity. - 1/7/16 Meetings with stakeholders to inform and involve them and reduce the severity - 11/11/16 Meetings with stakeholders to inform and involve them and reduce the severity, after the Vienna meeting. Compromise of transportation and e-health stakeholders to participate in the pilots - 1/12/16 Agreement to join the IoT-EPI challenge with 120 stakeholders interested in the pilots 1/1/17- Start of IoT1 – LSP ACTIVAGE and ICT14 Total Transport BigData LSP, with several stakeholders that will be involved in the pilots. Conversations to start

Table 21: Obsolescence due to changes in the market or user views

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R2.5	Obsolescence due to changes in the market or user views	The market environment or the user views change making the results obsolete.	The solutions will have to be adapted to the new products and standards in the market and may introduce delays.

Likelihood	Severity	Impact	Criticality
Low	Tolerable	0.6	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Establish contact with the most relevant alliances (e.g. AIOTI); standardization organisations (e.g. ETSI or IEEE) and have a permanent market-watch in order to detect changes in the IoT landscape.	The robust effort on market analysis in WP2 and the development of an appropriate exploitation plan in WP7 including a business analysis will make sure that user needs and wishes as well as market trends are constantly taken into account.

Handler	Current Status	Creation Date	Transfer Strategy
Pablo Giménez	Managed	15/1/2016	N/A

Work Log
- 28/10/16 The platform originally designed for the port has been changed to WSO2, it affects T3.1. Risk status updated from Identified to managed - 15/11/16 With the withdrawal of TI eCare platform no longer available. Mitigation measure to look for another equivalent platform. Contacts with UniversAAL developers. Risk Criticality increased to High due to a modification of the Likelihood - 21/12/16 Amendment submitted to EC eCare Platform substituted by UniversAAL. Severity of the risk reduced

Table 22: Different business interests

Risk subcategory			
Business			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R2.6	Different business interests	Different or concurrent business interests of partners endanger the collaboration and development of the project.	Unsuccessful exploitation of project results failing in achieving a relevant impact.
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Serious	1.2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Alignment of business interests and exploitation plans during WP2 and WP8.		Mediation and agreement among partners on business conflicting issues that appear and affect the execution of the project. Application of the CA when needed.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Miguel Llop	Closed	10/2/2016	N/A
Work Log			
- 13/05/16 Each partner define their own business model - 25/05/16 Define joint business model for the 3 products (INTER-LAYER, INTER-FW and INTER-METH) - 30/06/16 The task is finished without risk, it was identified, never managed. There were no business conflicting issues			

3.3 WP3 Related Risks

Table 23: Standards Obsolescence

Risk subcategory			
Technical			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.1	Standards Obsolescence	Due to long project duration the standards selected for the implementation of the INTER-IoT middleware integration at the early stages may become obsolete.	Obsolete standards might not be suitable anymore for the project. New standards have to be selected, extra effort is needed to adapt the interoperability procedures

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
It will be imperative that the selection process takes into account not only the current importance of a standard, but also the mid-term dynamics among them. During the requirements phase a strong analysis and link with AIOTI and other bodies will place INTER-IoT in context of the IoT landscape, and during the execution of the project an iterative and continuous process will detect the new standards and those losing favour from the community.	Include the new standard after an internal debate to consider it, taking into account that INTER-IoT INTER- LAYER product has as a basic requirement extendibility and the easy inclusion of new standards.

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares	Managed	1/3/2016	N/A

Work Log

- 18-19/05/16 Plenary Meeting Calabria. Risk detected during the proposal stage, already included in the Grant Agreement.
- 20/06/16 IOT EPI. Informal technical meeting
- 19/07/16 Telco meeting. SoA for analizing the technologies and standards available to be used in the project.
- 06/09/16 Telco meeting. Selection of the best suitable technologies and standard after the research.
- 11-13/10/16 Plenary/Review Meeting in Vienna
- 25/10/16 Telco meeting. Preparation of the technical workshop to start developing following these standards.
- 21-22/11/16 WP3 workshop. Development plan discussion and task reassignment.
- 29/11/16 Telco meeting. Risk progression control.
- 13/12/16 Telco meeting. Risk progression control.

Table 24: Finalization of Open Software support

Risk subcategory			
Technical			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.2	Finalization of Open Software support.	If an Open Source Software implementation is selected for the base implementation of the INTER-IoT middleware integration, there is a risk associated with the solution's community and its continuity, in case that the support for OSS implementation ends prematurely.	If the community abandons an OSS project selected for Inter-IOT, its commercial utilization would be jeopardized, and thus that of the INTER-IoT middleware.

Likelihood	Severity	Impact	Criticality
Low	Tolerable	0.6	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Looking into the community size and health, as well as the project's history should provide enough information to evaluate the potential of such problems. A continuous activity monitoring of the main contributors of the project and their activity in other similar projects may be enough to detect implementation decline and rise of a new one.	Selecting a new open source implementation associated with the same protocol; adapting a new one to meet the needs of providing support to the OSS implementation from INTER-IoT partners.

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares	Managed	1/6/2016	N/A

Work Log

- 18-19/05/16 Plenary Meeting Calabria. Risk detected during the proposal stage, already included in the Grant Agreement.
- 20/06/16 IOT EPI. Informal technical meeting
- 19/07/16 Telco meeting. Research about Open Source technologies and standards available to be used in the project.
- 06/09/16 Telco meeting. Selection of the best suitable Open Source technologies, with a huge community to support these technologies.
- 11-13/10/16 Plenary/Review Meeting in Vienna. Review of the technologies.
- 25/10/16 Telco meeting. Preparation of the technical workshop to start development with these Open Source technologies.
- 21-22/11/16 WP3 workshop. Development plan discussion and task reassignment.
- 29/11/16 Telco meeting. Risk progression control.
- 13/12/16 Telco meeting. Risk progression control.

Table 25: Bad interoperability design due to poor analysis of other platforms

Risk subcategory			
Technical			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.3	Bad interoperability design due to poor analysis of other platforms.	Insufficient analysis of existing IoT platforms, leading to a poor design.	INTER-IoT extendibility is reduced, specifically regarding interoperability and integration features

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Make a proper initial identification of successful IoT platforms and existing initiatives and related IoT standards to make a complete definition and analysis of the methods for layer interoperability and integration. Early evaluation of reference IoT platforms with expected contribution from the Advisory Board.	Identify the exact interoperability failures and create new high priority tasks in order to solve them. Deep review of the last stable state of the target IoT platforms.

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares/ Miguel A. Llorente	Managed	15/1/2016	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. Risk detected during the proposal stage, already included in the Grant Agreement. First task assignments.
- 20/06/16 IOT EPI. Informal technical meeting
- 19/07/16 Telco meeting. Research about platforms, technologies and tools. 1st draft design of architecture and components.
- 06/09/16 Telco meeting. Discussion about platforms characteristics and features, possible improvements of the 1st architecture draft and inclusion of new modules.
- 20-21/09/16 September Plenary Meeting Lancaster. 2nd draft design of architecture and components following the analysis of the platforms carried put in the first stage.
- 11-13/10/16 Plenary/Review Meeting in Vienna. Review of the architecture
- 25/10/16 Telco meeting. Preparation of the technical workshop to start development with the final architecture design. Components and sequence diagrams definition for basic functionalities.
- 21-22/11/16 WP3 workshop. Development and task reassignment. Last changes on the final architecture design.
- 29/11/16 Telco meeting. Tasks and performance progression control
- 13/12/16 Telco meeting. Tasks and performance progression control

Table 26: Poor performance of INTER-LAYER

Risk subcategory			
Technical			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.4	Poor performance of INTER-LAYER.	Low performance of INTER-LAYER regarding scalability, reliability, security, privacy and trust.	INTER-LAYER not having adequate performance in terms of scalability may create bottlenecks. At the same time lack or low performance of reliability, security, privacy and trust may avoid adoption of INTER-LAYER between platforms managed by different stakeholders.

Likelihood	Severity	Impact	Criticality
Moderate	Devastating	2.5	High

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Special care will be taken to first identify the most crucial requirements, and to monitor them during the entire process of the implementation of INTER-LAYER. Write and review the testing plan before the code. Iterative development and testing process in order to detect bad performance at an early stage.	Common development procedures in the different tasks of the WP Develop new strategies in order to improve performance and reduce software complexity. Feedback from the software architect in order to homogenise the different developments

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares Miguel A. Llorente	Managed	1/5/2016	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. Risk detected during the proposal stage, already included in the Grant Agreement. First task assignments.
- 19/07/16 Telco meeting. Research about platforms, technologies and tools. 1st draft design of architecture and components.
- 20-21/09/16 September Plenary Meeting Lancaster. 2nd draft design of architecture and components.
- 11-13/10/16 Plenary/Review Meeting in Vienna. Review of the INTER-LAYER architecture
- 25/10/16 Telco meeting. Preparation of the technical workshop
- 21-22/11/16 WP3 workshop. Development and task reassignment. Last changes on the final INTER- LAYER architectural design.
- 29/11/16 Telco meeting. Development progression control.
- 13/12/16 Telco meeting. Development progression control.
- 17/01/17 Telco meeting. Development progression control.

Table 27: High complexity creating proxy software for additional IoT platforms.

Risk subcategory			
Technical			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.5	High complexity creating proxy software for additional IoT platforms.	There might be potential problems to create support for new integrations or supporting new IoT platforms once the project is finished. This will reduce the applicability of the project results.	Once implemented, the INTER-IoT will not be able to adapt to new IoT platforms and standards.

Likelihood	Severity	Impact	Criticality
Moderate	Serious	2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Study and select a proper development methodology in order to create modular and adaptable software components. Create clear and understandable documentation of the software components.	Rewrite the project structure/codebase is possible and feasible. Once the INTER-LAYER components are in an intermediate or late stage of development rework the API docs, tutorials and guides in order to document better the software components.

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares Miguel A. Llorente	Managed	1/5/2016	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. Risk detected during the proposal stage, already included in the Grant Agreement. First task assignments.
- 19/07/16 Telco meeting. Research about platforms, technologies and tools. 1st draft design of architecture and components.
- 20-21/09/16 September Plenary Meeting Lancaster. 2nd draft design of architecture and components.
- 04/10/16 Telco meeting. Research and design progression control
- 11-13/10/16 Plenary/Review Meeting in Vienna. Review of the architecture
- 25/10/16 Telco meeting. Preparation of the technical workshop
- 21-22/11/16 WP3 workshop. Development and task reassignment. Last changes on the final architectural design.
- 29/11/16 Telco meeting. Development progression control.
- 13/12/16 Telco meeting. Development progression control.
- 17/01/17 Telco meeting. Development progression control.

Table 28: Integration failure between the different components of INTER-LAYER

Risk subcategory			
Technical			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.6	Integration failure between the different components of INTER-LAYER	The different software modules fail the integration tests of the whole system. This can occur if developers (especially when not working together) tend to drift apart in implementation.	The whole system or part of it will not properly work.

Likelihood	Severity	Impact	Criticality
Moderate	Serious	2	High

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Software Architect and Work Package Leader have to closely monitor and track the progress of development and keep track that the interfaces match.	Revise the implementation of the failing components and recode the interfaces in order to match with the external components.

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares Miguel A. Llorente	Managed	1/5/2016	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. Risk detected during the proposal stage, already included in the Grant Agreement. First task assignments.
- 19/07/16 Telco meeting. Research about platforms, technologies and tools. 1st draft design of architecture and components.
- 20-21/09/16 September Plenary Meeting Lancaster. 2nd draft design of architecture and components.
- 11-13/10/16 Plenary/Review Meeting in Vienna. Review of the INTER-LAYER architecture
- 25/10/16 Telco meeting. Preparation of the technical workshop
- 21-22/11/16 WP3 workshop. Development and task reassignment. Last changes on the final INTER- LAYER architectural design.
- 29/11/16 Telco meeting. Development progression control.
- 13/12/16 Telco meeting. Development progression control.
- 17/01/17 Telco meeting. Development progression control.

Table 29: Underperformance of partners

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.7	Underperformance of partners in WP3.	There is a possibility that a partner cannot meet deadlines, or underperforms. So, the task or piece of software that he is in charge will not be properly finished.	A part (or critical part) is missing or fails the unitary tests and integration tests with the rest of the components, causing severe delays to the project.

Likelihood	Severity	Impact	Criticality
Moderate	Serious	2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
WP Leader, Task Leaders with the help of the Software Architect must monitor and track the tasks assignments and deadlines. Also, perform periodical unitary and integration tests to ensure that all the components pass them.	Once detected which task/s or component/s is missing or failing identify the impact to the rest of the project. Reassign the task/s and/or component/s, speed up the development and rethink the work-plan to meet the project deadlines.

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares	Managed	1/5/2016	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. First task assignments. Project management plan presentation.
- 14/06/16 Telco meeting. Tasks and performance progression control.
- 19/07/16 Telco meeting. Tasks and performance progression control
- 21/09/16 Plenary meeting in Lancaster. Development plan consensus.
- 25/10/16 Telco meeting. Tasks and performance progression control
- 21-22/11/16 WP3 workshop. Development plan discussion and task reassignment.
- 13/12/16 Telco meeting. Tasks and performance progression control
- 17/01/17 Telco meeting. Tasks and performance progression control

Table 30: Breach of deadlines

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.8	Breach of deadlines of WP3 (due to underperformance R3.7) or due to underestimation of software implementation time.	The deadlines cannot be met by several cases (underperformance R3.7) or due underestimation of the time/people that has to be dedicated to a specific development task. If not enough resources (time/people) are designated to a software development task, this could not be accomplished.	The specific software piece may not be ready for the first integration test causing the project to delay.

Likelihood	**Severity**	**Impact**	**Criticality**
Moderate	Serious	2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
If have been an underestimation of resources, the WP3 Leader has to identify in the early stages of the development phase and solve it, dedicating more resources or speeding-up the task with an improved organization and time expenditure, or even prioritize critical software pieces over trivial ones.	WP3 Leader and Task leaders have to study the impact and speed-up or prioritize the critical software components.

Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Eneko Olivares	Managed	24/1/2017	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. First task assignments.
- 20/06/16 IOT EPI. Informal technical meeting
- 19/07/16 Telco meeting. Research about platforms, technologies and tools. 1st draft design of architecture and components.
- 06/09/16 Telco meeting. Tasks and performance progression control
- 20-21/09/16 September Plenary Meeting Lancaster. Development plan consensus. 2nd draft design of architecture and components.
- 11-13/10/16 Plenary/Review Meeting in Vienna. Review of the technologies.
- 25/10/16 Telco meeting. Preparation of the technical workshop to start development with the final design.
- 21-22/11/16 WP3 workshop. Development plan discussion and task reassignment.
- 29/11/16 Telco meeting. Tasks and performance progression control
- 13/12/16 Telco meeting. Tasks and performance progression control

Table 31: Performance failure of the development environment tools

Risk subcategory			
Technical			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.9	Performance failure of the development environment tools. (Including; code repositories, building tools, backup system, etc)	The tools deployed for development, continuous integration and code versioning (Jenkins, Nexus, Git, etc) may suffer a failure in its operation.	The code already generated may be corrupted or lost.

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
WP3 Leader and Software Architect have to track the correct operation of the tools and quickly identify if there is any malfunction. Comply with the backup strategy plan requirements and create regular backups of the source code and configuration of the tools.	Restore the most recent backup and in the case that there is any source code loss, since the incremental backups are performed daily, search for local copies of the affected source code.

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares	Managed	24/1/2017	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. First task assignments.
- 19/07/16 Telco meeting. Research about platforms, technologies and tools.
- 06/09/16 Telco meeting. Revision of tools and performance progression control
- 20-21/09/16 September Plenary Meeting Lancaster.
- 11-13/10/16 Plenary/Review Meeting in Vienna. Review of the technologies.
- 25/10/16 Telco meeting Set-up of the development environment tools (Jenkins, Nexus, Git, etc), set-up of backup's code system and preparation of the workshop.
- 21-22/11/16 WP3 workshop. Creation of tutorials for use of development tools and development workshop.
- 29/11/16 Telco meeting. Revision of tools and performance progression control.
- 13/12/16 Telco meeting. Revision of tools and performance progression control.

Table 32: Lack of communication and coordination between developers of a software module.

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.10	Lack of communication and coordination between developers of a software module.	Two or more different developers in charge of the same piece of software can misunderstand their duties.	The piece of software may be miss functional or not be ready for the first integration test.

Likelihood	Severity	Impact	Criticality
Low	Tolerable	0.6	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
The WP3 leaders and Task Leaders should be in charge of organizing the adequate meetings and telcos for communication and use the available organization tools (as ISL, Trello, Horde Calendar, etc.) in order to define correctly the duties assigned to each developer.	If the organization plan is not clear, neither the attributions, a change in the organization system must be carried out, including the rethinking of the use of communication and organization tools. Use of new communication tools like Slack or Trello

Handler	Current Status	Creation Date	Transfer Strategy
Eneko Olivares	Managed	24/1/2017	N/A

Work Log

- 19/05/16 Plenary meeting in Calabria. First task assignments. Project management plan presentation. Set-up of ISL communication tools for periodically telcos.
- 19/07/16 Telco meeting. Tasks and performance progression control
- 06/09/16 Telco meeting. Task progression control. Selection of best tools for communication, task assignments and collaborative development (Slack, Trello, Git Issues, etc)
- 20-21/09/16 September Plenary Meeting Lancaster.
- 04/10/16 Telco meeting. Tasks and performance progression control.
- 11-13/10/16 Plenary/Review Meeting in Vienna.
- 25/10/16 Telco meeting. Revision of collaborative tools and its effectiveness.
- 21-22/11/16 WP3 workshop. Development plan discussion and task reassignment.
- 29/11/16 Telco meeting. Tasks and performance progression control.
- 13/12/16 Telco meeting. Tasks and performance progression control
- 17/01/17 Telco meeting. Tasks and performance progression control

Table 33: Underestimation of the budget dedicated for this WP

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R3.11	Underestimation of the budget dedicated for WP3	The agreed budget to carry out the tasks included in this WP is not enough. That is, inability to pay developers, lack of budget for meetings, for the purchase of new HW or SW elements, etc.	Some software pieces will be missing or incomplete. The project will not be able to meet the requirements if any software or hardware piece is missing.
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Serious	1.2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
The project coordinator and the WP3 Leader should carry out an initial complete budget study to finalize all tasks in WP3, with a budget margin for exceptional cases.		If the budget study was not sufficiently precise or the margin is not large enough to palliate the exceptional costs, a redistribution of the budget in the whole project can be performed to minimize the impact of this risk.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau	Managed	24/1/2017	N/A
Work Log			
- 19/05/16 Plenary meeting in Calabria. First task assignments. Project management plan presentation. Estimation of the exact budget for material and licences needed for the project. - 19/07/16 Telco meeting. Study of the private tools with license needed to pay for the project development, and the physical material (servers, switches, peripherals, etc) - 20-21/09/16 September Plenary Meeting Lancaster. Review of the budget and needed material. - 04/10/16 Telco meeting. Budget progression control. - 11-13/10/16 Plenary/Review Meeting in Vienna. - 25/10/16 Telco meeting. Budget progression control. - 13/12/16 Telco meeting. Budget progression control.			

3.4 WP4 Related Risks

Table 34: Focus on a small set of IoT platforms

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R4.1	Focus on a small set of IoT platforms	Design guidelines are focused on specific IoT platforms while there are hundreds of them with different features	INTER-IoT would lose the generic approach of interoperability of IoT platforms, being compatible only with the selected IoT platform range

Likelihood	Severity	Impact	Criticality
High	Tolerable	1.4	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
It's impossible to offer 100% universal interoperability, but we can use the partners' expertise during the design phase of the different components to take into account possible further differences that can be easy to be implemented	Perform a thorough analysis of the IoT platforms so that the widest spread platforms are covered, not only the current platforms, but also the future ones and especially those relevant from the European point of view. Use an extensible approach for the future support of new platforms, so that its support can be easy to implement

Handler	Current Status	Creation Date	Transfer Strategy
Miguel A. Llorente	Managed	15/6/2016	N/A

Work Log
- 22/9/16 Methodology for analysing and generating the client for any IoT platform developed by A. Romeu (PRO) - 29/9/16 Selected IoT platforms are: FIWARE, OpenIoT, OneM2M, UniversAAL, Azure IoT

Table 35: Least common IoT platform feature set

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R4.2	Least common IoT platform feature set	The wider number of IoT platforms supported, the least common features we may find	A wide IoT platform analysis looking for generic features can cause that only common features are handled. For instance, one IoT platform may offer announcements of new devices, while others may not, or one platform can offer CEP services and another one can have it not available.
Likelihood	**Severity**	**Impact**	**Criticality**
High	Moderated	2.1	High
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Select a subset of reference IoT platforms important for the project		Focus not only on the least common features, but on the least feature set we decide, adding if necessary new capabilities in the bridges (e.g. measurement filtering) or by supporting different capabilities for the different platforms, having it available for INTER-FW clients	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Miguel Montesinos	Managed	15/6/2016	N/A
Work Log			
- 16/11/16 Preparation of technical workshop taking into account platform capabilities for interfaces			

Table 36: Reference Architecture does not match real IIoT architecture

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R4.3	Reference Architecture does not match real IIoT architecture	The reference architecture designed in T4.1 may not reflect the real architecture designed in the overall INTER-IoT project and its inner component architecture	D4.1 may be useful as theory exercise buy useless for INTER-IoT development

Likelihood	Severity	Impact	Criticality
High	Moderated	2.1	High

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Establish continuous communication between task leader (Alex) and the Sw Architect to match ongoing architecture design of WP3 with T4.1	Readapt the reference architecture to match with the real architecture of INTER-LAYER and INTER-FW

Handler	Current Status	Creation Date	Transfer Strategy
Alex Bassi	Closed	15/11/2016	N/A

Work Log
- 16/11/16 First telco set-up for 16th-nov-16 - 17/1/17 Conversations were made, and Sw Architect aligned D3.1 and D4.1

Table 37: D4.1 may be late

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R4.4	D4.1 may be late	D4.1 is not advancing at the pace it should, remaining a hard work as of mid November-16	D4.1 may be delivered out of date or it may not contain the necessary information with enough detail and analysis

Likelihood	Severity	Impact	Criticality
High	Serious	2.8	High

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Weekly review of the status of D4.1 coordinated by Alex Bassi and with all contributors' participation	Further iteration of the deliverable and working in parallel T4.3 with this iteration

Handler	Current Status	Creation Date	Transfer Strategy
Alex Bassi	Closed	15/11/2016	N/A

Work Log
- 18/11/16 Work is progressing. Risk is being managed - 16/1/17 D4.1 was finally delayed 2 weeks

Table 38: Too many configuration helper tools

Risk subcategory			
Usability			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R4.5	Too many configuration helper tools	According to the design and development of INTER-LAYER it seems INTER-IoT may have too many configuration to be specified during run-time by INTER-IoT users. INTER-FW should provide helper tools to ease the deployment and usage of INTER-IoT configuration needs, so the number of tools may be big	Impossibility of creating all the expected tools, which in turn may lead to challenges in using INTER-IoT
Likelihood	**Severity**	**Impact**	**Criticality**
Moderate	Serious	2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Try to reduce the complexity of the work an INTER-IoT user is supposed to do at the design and implementation time in INTER-LAYER		Good technical documentation of INTER-FW with examples	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Miguel Montesinos	Managed	22/11/2016	N/A
Work Log			
- 22/11/16 Already managed during technical workshop at Valencia 21-22/11/16			

Table 39: Security management might be not only exclusive to INTER_FW

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R4.6	Security management might be not only exclusive to INTER_FW	So far, security aspects have been delegated to the INTER-FW, but it can be not valid, as there could be security risks at lower level	Security holes or risks might appear in INTER-LAYER if an external user directly accesses it by-passing INTER-FW

Likelihood	Severity	Impact	Criticality
Moderate	Serious	2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Analyze the impact on security at lower levels under INTER-FW, and if after the assessment it is perceived security aspects will have to be shared all along the different layers of INTER-IoT	Design a security approach to avoid direct usage of INTER-LAYER without the specific security compliances

Handler	Current Status	Creation Date	Transfer Strategy
Miguel A. Llorente	Managed	17/1/2017	N/A

Work Log
- 17/1/17 Design to be done at INTER-FW design (T4.3)

3.5 WP5 Related Risks

Table 40: Delayed or Insufficient WP outcomes for INTER-METH

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R5.1	Delayed or Insufficient WP outcomes for INTER-METH	WP2, WP3, WP4 and T5.1 provide delayed or incomplete outcomes that can delay the development or even mine the effectiveness of INTER-METH	A delay in providing developments for WP5, will led to a delay in producing INTER-METH CASE tool. In this event, the time to support test end-user groups in evaluating the developed methodology and tools would be drastically reduced affecting the overall validation of the product.
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Serious	1.2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Continuous monitoring and communication between WP leaders and even Task leaders in order to reduce malfunctions.		INTER-METH is based on an iterative process organized in iterated phases that systematically incorporates and use the outcome of WP2, WP3, WP4 and T5.1, until they are considered suitable. If some delay or potential incompleteness is detected, adjustment measures will be taken to solve the issue in terms of adding more manpower or providing developing solutions.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Giancarlo Fortino	Managed	28/7/2016	N/A
Work Log			
- 22/9/16 Risk status change from identified to managed during the workshop help in the plenary meeting in Lancaster (UK) - 24/11/16 Risk updated after Valencia workshop - 24/1/17 Risk assessed during WP5 telco			

Table 41: INTER-METH poor Usability and lack of interest

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R5.2	INTER-METH poor Usability and lack of interest	INTER-METH is unattractive, harder to use and the integration process results long, costly and complicated.	A non-attractive and usable methodology and associated CASE tool may lead to a reduced impact and scarce interest because users do not want to work with it or does not help interoperability between platforms.

Likelihood	**Severity**	**Impact**	**Criticality**
Very Low	Serious	0.4	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Run specific usability tests with end-user groups with previous experience on design methodologies, and adapt the HMI and concepts to the requirements specified by them	The consortium has already planned to provide both an appropriate documentation to support different typologies of users/stakeholders and the INTER-METH CASE tools (Task 5.3). The latter has precisely the aim of making the integration of IoT platforms rapid, simple and robust by supporting the automated application of the INTER-METH methodology in all the development phases. Moreover, the development of a user-friendly graphical interface of the CASE tool, will surely reduce the risk of poor usability.

Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Giancarlo Fortino	Managed	28/7/2016	N/A

Work Log
- 22/9/16 Risk status change from identified to managed during the workshop help in the plenary meeting in Lancaster (UK) - 24/11/16 Risk updated after Valencia workshop - 24/1/17 Risk assessed during WP5 telco

3.6 WP6 Related Risks

Table 42: Mismatch in architecture

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R6.1	Mismatch in architecture	A mismatch in architecture has the consequence that system modules do not connect.	Delay in the integration, since software must be adjusted.
Likelihood	**Severity**	**Impact**	**Criticality**
Moderate	Serious	2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Test parts of the system in advance		Software Architect must be very keen and sharp on interfaces. No deviations on the agreed interfaces are allowed, also the software architect must ensure that all interfaces are fully defined and specified.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Roel Vossen/Miguel A. Llorente	Identified	22/2/16	N/A
Work Log			
- 22/2/16 WP2 workshop identification of the risk, from the analysis of the requirements - 9/7/16 WP4 workshop related with the architecture, input from WP6 required - 22/9/16 3rd Plenary meeting Lancaster, risk update after the analysis of the use cases - 22/11/16 WP3/WP4 workshop assessment of the risk through the definition of the interfaces			

Table 43: Systems at implementation site are not compliant to new architecture

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R6.2	Systems at implementation site are not compliant to new architecture	Systems at the harbour may be different or not (fully) accessible for the new software architecture	Integration cannot take place, no integration possible in the systems
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Serious	1.2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
A new platform/subsystem can be placed between the original systems to implement the architecture. The original system will be treated as a sensor/actuator		Prepare the integration and map the current systems. Preparation can be done by having some platforms to be placed in-between	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Roel Vossen	Managed	19/5/16	N/A
Work Log			
- 19/5/16 Plenary meeting in Calabria, presentation of the stakeholders' architectures to be used in the pilot. Identification of the risks - 9/7/16 WP4 workshop related with the architecture, input from WP6 required - 22/9/16 3rd Plenary meeting Lancaster, risk update after the analysis of the use cases - 22/11/16 WP3/WP4 workshop assessment of the risk through the definition of the interfaces - 21/12/16 risk assessment after withdrawal of TI			

Table 44: IoT platform doesn't meet the promised functionalities

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R6.3	IoT platform doesn't meet the promised functionalities	Identified and selected IoT platforms for the pilot does not meet the specifications described in the documentation and has to be changed.	The pilot cannot be developed and it takes more time and effort to finish the prototype.

Likelihood	Severity	Impact	Criticality
Low	Devastating	1.5	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Perform a thorough analysis of each of the specifications of the selected IoT platform. Design the framework so that it is relatively easy to change one platform to another.	Analyse what may be an appropriate alternative platform that has been analysed in the state of the art and develop the necessary bridges.

Handler	Current Status	Creation Date	Transfer Strategy
Carlos Palau	Managed	19/05/16	N/A

Work Log
19/5/16 Plenary meeting in Calabria, presentation of the stakeholders' architectures to be used in the pilot. Identification of the risks - 9/7/16 WP4 workshop related with the architecture, input from WP6 required - 22/9/16 3rd Plenary meeting Lancaster, risk update after the analysis of the use cases - 12/10/16 Discussion with stakeholders in the IoT-EPI event to reduce likelihood and severity of the risk - 22/11/16 WP3/WP4 workshop assessment of the risk through the definition of the interfaces - 21/12/16 risk assessment after withdrawal of TI - 31/12/16 D2.4 submitted containing the scenarios and use cases, that will be analysed to be used in WP6

3.7 WP7 Related Risks

Table 45: Complexity of the Evaluation Plan

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.1	Complexity of the Evaluation Plan	The evaluation plan contains too much detail to perform the subsequent WP7 tasks.	More work will be required to effectively perform subsequent WP7 tasks.
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Tolerable	0.6	Low
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Effective task management encouraging communication among project partners and participation in T7.1.		Redefine the Evaluation Plan in order to reduce complexity. Create a Task Force, including the stakeholders in order to determinate the complexity of the evaluation activities. Evaluation Plan is a deliverable that has to be reviewed considering content but also applicability.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Eric Carlson	Identified	12/07/2016	N/A
Work Log			
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment - 10/11/16 Risk assessment after technical review report reception			

Table 46: Lack of detail in the Evaluation Plan

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.2	Lack of detail in the Evaluation Plan	The evaluation plan contains too little detail to perform the subsequent WP7 tasks.	No good outcome of the WP7 would have been achieved. More work will be required to effectively perform subsequent WP7 tasks.

Likelihood	Severity	Impact	Criticality
Very Low	Tolerable	0.2	Very Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Effective task management encouraging communication among project partners and participation in T7.1.	Redefine the Evaluation Plan in order to provide the required details. Create a Task Force, including the stakeholders in order to determinate the needs of the evaluation activities. Evaluation Plan is a deliverable that has to be reviewed considering content but also applicability.

Handler	Current Status	Creation Date	Transfer Strategy
Eric Carlson	Identified	12/07/2016	N/A

Work Log
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment - 10/11/16 Risk assessment after technical review report reception

Table 47: Evaluation and assessment out of scope

Risk subcategory			
Technology			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.3	Evaluation and assessment out of scope	The technical evaluation and assessment does not adequately cover the scope of the project.	Some aspects of the project are not covered in the evaluation and assessment phase. Uncertainty about the quality of the project would appear.
Likelihood	**Severity**	**Impact**	**Criticality**
Very Low	Serious	0.4	Low
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Initial buy in on T7.1 to fully understand the evaluation plan and insure that all aspects of the project are covered		Clearly determine the scope of the evaluation procedures and required results, eliminating those that may provide relevant performance and interoperability results that are not defined under the GA.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Eric Carlson	Identified	12/07/2016	N/A
Work Log			
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment - 10/11/16 Risk assessment after technical review report reception			

Table 48: Extra trials needed

Risk subcategory			
Organisation			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.4	Extra trials needed	Additional trials are needed to further evaluate the platform	Additional time will be needed to effectively evaluate these trials.

Likelihood	Severity	Impact	Criticality
Moderate	Tolerable	1	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
The trials to be performed will be set before the onset of M25 to allow adequate time for preparation.	The consortium will endeavour to include all necessary trials to fully evaluate the platform, but will prioritize the trials that offer the most project relevant feedback.

Handler	Current Status	Creation Date	Transfer Strategy
Eric Carlson	Identified	22/09/16	N/A

Work Log
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment - 10/11/16 Risk assessment after technical review report reception

Table 49: Questionnaires useless

Risk subcategory			
Usability			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.5	Questionnaires useless	Questionnaires designed to assess process evaluation do not adequately identify drivers and barriers to INTER-IoT adoption.	Questionnaire results do not accurately reflect INTER-IoT process impact.

Likelihood	Severity	Impact	Criticality
Very Low	Tolerable	0.2	Very Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Inclusion of all project partners in the review of T7.4 questionnaires.	Reengaging with end users and project partners to review and refine the questionnaire, adding targeted questions to address barriers and drivers missed during the initial phase.

Handler	Current Status	Creation Date	Transfer Strategy
Eric Carlson	Identified	22/09/16	N/A

Work Log
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment - 10/11/16 Risk assessment after technical review report reception

Table 50: Simplicity of Interoperability Methodology

Risk subcategory			
Usability			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.6	Simplicity of Interoperability Methodology	The developed interoperability methodology is too simplified and is not easily applicable for interoperability validation	Impossible to complete overall interoperability validation

Likelihood	Severity	Impact	Criticality
Low	Tolerable	0.6	Low

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Inclusion of all project partners in the development and review of interoperability methodology	Clearly determine and define the scope of the validation methodology

Handler	Current Status	Creation Date	Transfer Strategy
Eric Carlson	Identified	22/09/16	N/A

Work Log
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment. Participation in the discussion between WP3/4/5 and WP7 - 10/11/16 Risk assessment after technical review report reception

Table 51: Complexity of Interoperability Methodology

Risk subcategory			
Usability			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.7	Complexity of Interoperability Methodology	The developed interoperability methodology is too complex and interoperability validation cannot be tested properly	Impossible to complete overall interoperability validation

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Inclusion of all project partners in the development and review of interoperability methodology	Clearly determine and define the scope of the validation methodology

Handler	Current Status	Creation Date	Transfer Strategy
Eric Carlson	Identified	22/09/16	N/A

Work Log
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment. Participation in the discussion between WP3/4/5 and WP7 - 10/11/16 Risk assessment after technical review report reception

Table 52: The results from INTER-IoT are not easily transferred to other IoT domains

Risk subcategory			
Usability			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.8	The results from INTER-IoT are not easily transferred to other IoT domains	The barriers for transferring the developed results are too high	Impossible to complete the transfer of ItnerIoT results
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Tolerable	0.6	Low
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Inclusion of all project partners in the development and review of process evaluation		Clearly determine and define the scope of the process evaluation	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Eric Carlson	Identified	22/09/16	N/A
Work Log			
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment. - 12/10/16 IoT-EPI participation in the discussion of the TF. Risk Assessment - 10/11/16 Risk assessment after technical review report reception			

Table 53: The results from impact evaluation and process evaluation are not consistent

Risk subcategory			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R7.9	The results from impact evaluation and process evaluation are not consistent	The developed evaluation processes do not work together. They will not allow to produce a comprehensive picture of obtained benefits	Impossible to complete overall evaluation
Likelihood	**Severity**	**Impact**	**Criticality**
Low	Serious	1.2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Inclusion of all project partners in the development and review of process evaluation		Clearly determine and define the scope of the evaluation process	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Eric Carlson	Identified	18/10/2016	N/A
Work Log			
- 22/9/16 Plenary meeting in Lancaster (UK). Risk assessment. - 10/11/16 Risk assessment after technical review report reception			

3.8 WP8 Related Risks

Table 54: Failed Exploitation

Risk subcategory			
Business			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R8.1	Failed Exploitation	Failed or Insufficient exploitation results by partners	Effort spent in the project not useful for Business when the project ends

Likelihood	Severity	Impact	Criticality
Low	Serious	1.2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Alignment of business interests and exploitation plans during WP2 and WP8	The Exploitation Plan will identify an exhaustive list of reasonable exploitation opportunities for INTER-IoT results, some of them exploitable on an individual partner basis, but also in the consortium as a whole or by a reduced group of partners.

Handler	Current Status	Creation Date	Transfer Strategy
Eric Carlson	Managed	13/1/16	N/A

Work Log
- 13/1/16 Kick-off, description of the exploitation process - 22/2/16 WP2 workshop evaluation risk status updated from identified to managed - 30/4/16 Submission of D8.3, assessment of the link with D2.2 - 18/5/16 2nd Plenary meeting in Calabria, control of the first QMR including impact assessment - 5/7/16 control of the second QMR from the partners - 22/9/16 3rd Plenary meeting Lancaster, preparation for the review meeting - 4/10/16 PCC Telco meeting, control of the third QMR - 11/10/16 Reception of the Technical Review Report, analysis of the concerns associated with exploitation - 17/1/17 agreement on an exploitation workshop in February 2017

Table 55: Impact generated by the project not significant

Risk subcategory			
Business			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R8.2	Impact generated by the project not significant	The project results are largely ignored by our stakeholders, undermining the following exploitation and mid-to-long term sustainability of the project	Effort spent in the project not useful

Likelihood	Severity	Impact	Criticality
Moderate	Serious	2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Work with Communication and Marketing professionals. Fluent exchange of information between stakeholders and the consortium. Validate venues for scientific publication.	Monitoring regularly metrics and consulting marketing and communication experts. Additionally track scientific contributions from the partners in order to achieve high impact, and re-visit venues to consider high relevance

Handler	Current Status	Creation Date	Transfer Strategy
Alessandro Bassi	Managed	13/1/16	N/A

Work Log
- 13/1/16 Kick-off, description of the exploitation process - 22/2/16 WP2 workshop evaluation risk status updated from identified to managed - 30/4/16 Submission of D8.3, assessment of the link with D2.2 - 18/5/16 2nd Plenary meeting in Calabria, control of the first QMR including impact assessment - 5/7/16 control of the second QMR from the partners - 22/9/16 3rd Plenary meeting Lancaster, preparation for the review meeting - 4/10/16 PCC Telco meeting, control of the third QMR - 11/10/16 Reception of the Technical Review Report, analysis of the concerns associated with impact: including industrial dissemination and communication - 17/1/17 agreement on an exploitation workshop in February 2017

Table 56: Open Source Strategy not adequate

Risk subcategory			
Business			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R8.3	Open Source Strategy not adequate	The project fails to create or join an open source community and contribute to it with the corresponding project results.	Effort spent in the project regarding open source software distribution is not useful and the project fails to meet one of the indicated objectives: creation of new business models.

Likelihood	Severity	Impact	Criticality
Moderate	Serious	2	Moderate

Contingency plan	
Avoid/Minimize Likelihood Strategy	**Mitigate Severity Strategy**
Work together with IoT-EPI in order to improve community building models. Grab support from the Open Call partners entering in the project. Merge efforts with existing open source initiatives.	Analyse periodically the open source strategy and check the efforts dedicated to it. Creation of a TF to periodically assess the license policy to be used

Handler	Current Status	Creation Date	Transfer Strategy
Carlos Palau/Amelia del Rey	Managed	20/10/16	N/A

Work Log

- 20/10/16 Creation of the risk after the technical review meeting
- 25/10/16 Participation in ECLIPSECON Europe with other IoT-EPI projects
- 11/10/16 Reception of the Technical Review Report, analysis of the concerns associated with open source software. TF creation to work in the open source strategy
- 15/10/16 Creation of the Open Source Task Force to analyse open source licenses of the products integrated in INTER-IoT and assess the best license to be used in INTER-IoT products. Task Force composed by (Carlos Palau (UPV), Miguel A. Llorente (PRO), Amelia del Rey (PRO) and Flavio Fouart (X-LAB).
- 21/12/16 Agreement to join Eclipse initiative related with IoT platforms interoperability for Smart Cities
- 17/1/17 agreement on an exploitation workshop in February 2017

Table 57: Industrial Dissemination not adequate

Risk subcategory			
Business			
Risk Nº	**Risk Name**	**Risk Description**	**Consequences**
R8.4	Industrial Dissemination not adequate	The project fails to create adequate impact in the events associated with the stakeholders interested in INTER-IoT products	Stakeholders are not aware of the products developed and the project fails to create impact in one of the axis of the exploitation policy. The industrial dissemination policy is not adequate.
Likelihood	**Severity**	**Impact**	**Criticality**
Moderate	Moderate	1.2	Moderate
Contingency plan			
Avoid/Minimize Likelihood Strategy		**Mitigate Severity Strategy**	
Work together with IoT-EPI in order to identify venues adequate for industrial dissemination. Identify from the stakeholders of the project the most adequate venues. Identify from the stakeholder group identified in WP2 the most adequate venues		Periodically monitor the relevant events/trade fairs of interest for the generic products (INTER-LAYER, INTER-FW and INTER-METH) and for the specific products. Monitor the success of the actions taken in the area of industrial dissemination.	
Handler	**Current Status**	**Creation Date**	**Transfer Strategy**
Carlos Palau	Managed	20/10/16	N/A
Work Log			
- 20/10/16 Creation of the risk after the technical review meeting - 15/11/16 Release of the exploitation questionnaires to the stakeholders - 1/12/16 Agreement to participate in the IoT-EPI stakeholders meeting - 17/1/17 agreement on an exploitation workshop in February 2017			

4 Conclusions

The Risk Management Document reflects the attention that the Inter-IoT Consortium intends to provide to potential threats and risks for the Inter-IoT Project. The intention beyond the list of risks is to make all partners involved in the project aware of the importance of meeting project goals and objectives.

The Risk Management procedures constitute an important part of the project management. The current version of the Risk Management Plan/Report is updated according to the outputs generated in the Inter-IoT Consortium meetings and will be followed up during the entire period of the project. It has helped to reduce the probability of some risks to occur, and it also has detected potential risks that finally happened, helping to mitigate their impact when they occurred.

No risk identified by the consortium has a critical impact. The likelihood of most risks is low/moderate, which facilitates their management. Although some of the risks have a serious to devastating severity. The corresponding mechanisms to avoid or minimize likelihood and mitigate the severity have allowed the consortium to deal with some of the risks, e.g. withdrawal of Telecom Italia and software integration risks.

Next version of the risk document will include the evolution of the risks management worklogs, and the introduction of more risks that will be detected through the execution of the project.