

Risk Management and event handling Module

D7.9

April 2022

Deliverable

PROJECT ACRONYM	GRANT AGREEMENT #	PROJECT TITLE
TWINERGY	957736	Intelligent interconnection of prosumers in positive energy communities with twins of things for digital energy markets

DELIVERABLE REFERENCE NUMBER AND TITLE

D7.9 Risk Management and event handling Module

Revision: v1.0

AUTHORS

Luigi Sechi	Stylios Karatzas
STAM	UoP



Funded by the Horizon 2020 programme of the European Union
Grant Agreement No 957736

DISSEMINATION LEVEL

- ✓ P Public^[SEP]
- C Confidential, only for members of the consortium and the Commission Services

Version History

REVISION	DATE	AUTHOR	ORG...	DESCRIPTION
V0.1	11.02.2022	Luigi Sechi Stylios Karatzas	STAM UoP	T.o.C
V0.2	16.03.2022	Luigi Sechi	STAM	1 st draft to review
V0.6	20.03.2022	Luigi Sechi	STAM	2 nd draft to review
V0.7	28.03.2022	Stylios Karatzas	UoP	STPA methodology
V0.8	29.04.2022	Luigi Sechi Stylios Karatzas	STAM UoP	Final draft submitted to PC
V1.0	30.04.2022	Luigi Sechi Stylios Karatzas	STAM UoP	Draft submitted to EC by the PC

Statement of Originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Legal Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced authors shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Union. Neither the CINEA nor the European Commission is responsible for any use that may be made of the information contained therein.

© 2022 by TwinERGY Consortium

Executive summary

This present document is the D7.9 “Risk Management and event handling Module” of the TwinERGY project, funded by the European Commission’s Innovation and Networks Executive Agency (CINEA) under its Horizon 2020 Research and Innovation programme (H2020). The main objective of this deliverable is to provide a Module handbook for the Risk management module developed in T7.9 “Risk Management and event handling Module”.

Deliverable D7.9 reports on the development and implementation of two models, RAMPART and STPA, in risk management. Both models are used supplementary in this deliverable’s framework in order to exploit the potential of energy demand flexibility. The main objective of this document is to produce a comprehensive a qualitative and quantitative risk management application dedicated to the residential buildings. Firstly, with the use of STPA, system level threats have been identified and divided into hazards and losses, while countermeasures (control actions) were produced corresponding to each threat. In the next sections of this deliverable, the different components of the tool, the User Interface, the commands available to the user and the information that can be visualized are also being described.

Given the fact that the pilot’s installations activities remain ongoing, additional enhancements and testing activities are needed to be introduced. Since feedback is continuously changing in TwinERGY pilot demonstrations, the next steps for further development of the algorithm will focus on a more dynamical way to add and update the data acquired.

Index

1. Introduction	9
1.1. Scope of the document	9
1.2. Structure of the deliverable	9
1.3. Abbreviation list	10
2. Module requirements and functionalities.....	12
3. Qualitative Risk Analysis	14
3.1. Risk analysis with the use of STPA.....	14
3.2. STPA processes in TwinERGY	15
3.2.1. Data acquisition and qualitative processing.....	15
3.2.2. Hazards and Losses - Identification and Analysis	16
4. Quantitative Risk Analysis.....	24
4.1. Importance of the topology	24
4.2. Cascading effect, propagation of effects to multiple assets	26
4.3. Inputs & Initial Data	27
4.4. Scenario generation	28
4.5. Scenario simulation	28
4.6. Likelihood Calculation	31
4.7. Impact Calculation	32
4.7.1. Computation of physical damages.....	33
4.7.2. Estimation of out of service.....	33
4.8. Risk computation	34
4.9. Algorithm implementation.....	34
5. Set up of the Risk analysis	35
5.1. Configuration and Asset's topological structure	35
5.2. Threats and Impacts	37
5.3. Risk Computation	38
5.4. Countermeasures application	41

6. Users experience and results	43
6.1. Risk Analysis GUI.....	43
7. Conclusions and next steps.....	45
Annexes.....	46
Annex A. Data collection from pilots and partners' expertise	46
Sheet 1 – System involved	46
Sheet 2– Threats.....	46
Sheet 3 – Countermeasure installed	49
References.....	50

List of Figures

Figure 1. Steps in STPA Methodology	14
Figure 2. Control Structure Model.....	15
Figure 3. Tree Model.....	25
Figure 4. Risk Management Algorithm.....	26
Figure 5. Process implementation	27
Figure 6. Possible Outcomes	30
Figure 7. Mapping for the propagation	31
Figure 8. Topological Entities	35
Figure 9. Topology of simple townhouse	36
Figure 10. Partners' feedback collected	38
Figure 11. Flow chart of the Algorithm logic based on the Power Loss Threat.....	40
Figure 12. Scenario selection risk GUI.....	43
Figure 13. Risk Analysis results in the GUI.....	44
Figure 14. System involved selection	47

List of Tables

Table 1: Abbreviation list.....	11
Table 2. Risk module requirement.....	12
Table 3. Risk module requirement.....	12
Table 4. Risk module requirement.....	12
Table 5. EVS table, possible causes & suggested countermeasures.....	16
Table 6. CPS table, possible causes & suggested countermeasures.....	17
Table 7. PVS table, possible causes & suggested countermeasures.....	19
Table 8. SMS table, possible causes & suggested countermeasures.....	20
Table 9. BS table, possible causes & suggested countermeasures.....	21
Table 10. HVS table, possible causes & suggested countermeasures	22
Table 11. LS table, possible causes & suggested countermeasures	23
Table 12. Threats description template - PV System example	47
Table 13. Main Systems - Threats description template	48
Table 14. Countermeasures installed template.....	49

1. Introduction

1.1. Scope of the document

Following the DoA, this deliverable reports on the development of the tool for the risk management within TwinERGY platform. In this deliverable, the release of the tool and the algorithms used for it are described in detail.

Tenants, building managers and up to the energy providers and the DSO need tools capable of analysing and predicting the effects of the threats, both physical and cyber related to the infrastructures, and need to estimate in quantitative and monetary terms how those threats can affect their activity. These kinds of tools are fundamentals for such organisations in order to support decision makers and to better plan future activities. The tool developed for the risk management in the TwinERGY project has to deal with an array of threats and risks, stored inside the module database. Currently, it has been populated thanks to the contributions of the pilots' representatives and of the technical support partners of the TwinERGY project. The next step is to increase the database dynamically. To this end, this deliverable is:

- Compiling the risks/ threats identified in different assets/elements which are part of the TwinERGY Pilot's ecosystem, along with their potential countermeasures
- Synthesizing the different methods in the creation of a cohesive risk analysis tool
- Proposing a risk analysis framework with a clear mapping of threats and countermeasures for each pilot site, along with a calculation engine for the risk assessment process
- Documenting the integration and implementation activities that need to be performed at a system level in order to prevent/mitigate risks
- Being integrated with other tools to highlight mutual benefits of ensuring interoperability

1.2. Structure of the deliverable

This deliverable is structured starting with an Executive Summary of the document and is composed of the following chapters:

- Chapter 2: Compiling the risks/ threats identified in different assets/elements which are part of the TwinERGY Pilot's ecosystem, along with their suggested countermeasures
- Chapter 3: Overview of the Module main requirements and the related functionalities of the Risk tool

- Chapter 4: Overview of the logic behind the risk analysis
- Chapter 5: Describes the set up in back end of the risk analysis
- Chapter 6: Describes the interface of the tool, how the end user can interact with it and the results displayed.
- Chapter 7: Presents the conclusions and the next steps features of the tool
- Chapter 8: Annexes

1.3. Abbreviation list

Table 1: Abbreviation list

Acronym	Full Name
Acronym	Full Name
DoA	Description of Action
DT	Digital Twin
API	Application Programming Interfaces
DSO	Distribution System Operators
A	Area
TH	Threat
EO	Estimated Occupancy
EVA	Economic Value of an area
POA	Probability of anomaly
S	Scenario
M	Threat magnitude
EF	Efficiency of the countermeasure
EL	Economic loss
ELIS	Economic loss interruption of service

PD	Physical Damage
GUI	Graphical Users Interface
EVS	Electric Vehicle System
CPS	Charging Point System
EPS	Electrical Panel System
PVS	Photovoltaic System
SMS	Smart Meter System
BS	Battery System
HVS	HVAC System
LS	Lightning System

2. Module requirements and functionalities

In the following tables, the main functionalities and requirement of the Risk Module are reported.

Table 2. Risk module requirement

Req.-ID	<i>Risk_1</i>
Short name	Creation of libraries of the pilot environment to create and model the building to be analysed with the tool
Key objective	<ul style="list-style-type: none"> • Definition of features of the infrastructure
Description /Comments /Constraints	Libraries to model areas, assets and the related attributes are necessary. Moreover, they are needed to define security countermeasure of the infrastructure.
Priority rank	<i>Essential</i>

Table 3. Risk module requirement

Req.-ID	<i>Risk_2</i>
Short name	Population of the database of threats and countermeasure installed in the building to be analysed with the tool (Further identification of system threats (hazards) with the STPA methodology-enhancement of existing dataset)
Key objective	<ul style="list-style-type: none"> • Definition of features of the main threats
Description /Comments /Constraints	Libraries to model areas, assets and the related attributes are necessary. Moreover, they are needed to define security countermeasure of the infrastructure.
Priority rank	<i>Essential</i>

Table 4. Risk module requirement

Req.-ID	<i>Risk_3</i>
Short name	Computation of Risk
Key objectives	<ul style="list-style-type: none"> • Perform Risk assessment • Evaluate damages to appliances and services

	<ul style="list-style-type: none"> ● Assess likelihood and impact of threats
<p>Description /Comments /Constraints</p>	<p>Computation of risks in a quantitative way. The process of risk assessment should be easy and done automatically as far as possible. Risk and other relevant metrics should be visualized to the user in an intuitive way through indicators and charts. Moreover, cascading effects should be modelled within the analysis to consider this relevant phenomenon. The risk computation should gather as outputs several indicators, among them a Security Risk Assessment Index will be implemented to provide the user with an overall score about its own infrastructure.</p>
<p>Priority rank</p>	<p><i>Essential</i></p>

3. Qualitative Risk Analysis

This section deals with the use of STPA methodology for the risk analysis of the systems of interest within TwinERGY project. Firstly, a justification of the selection of the methodology is introduced, while later, the integration plan is introduced.

3.1. Risk analysis with the use of STPA

In this Chapter, following the identification of the main functionalities and requirements of the risk modules, we used Systems-Theoretic Processes Analysis (STPA) as a theoretic risk identification method. Considering that one of the leading challenges in safe system development is the identification of all potential failure modes along with the unsafe interactions among system components, we used STPA to ensure TwinERGY systems' safe function under all conditions.

The concept of risks used in STPA methodology differs from the one used in the risk analysis developed in the next chapters of this deliverable. Specifically, in STPA methodology we recognize system risks/threats as either losses or hazards, based on the impact that the occurring event has on the system that is being analyzed. Thus, for the sake of completeness and consistency, the main concepts of STPA are stated below:

System level Accidents

Accident (Loss) is an undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

System level Hazards

Hazard – A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).

STPA methodology consists of four main steps, those being:

- Step 1: System design by using system engineering foundation: Define the purpose of analysis, system boundaries, losses of concern and system hazards
- Step 2: Modelling the Control structure
- Step 3: Identification of Unsafe control actions
- Step 4: Identification of accident causal scenarios



Figure 1. Steps in STPA Methodology

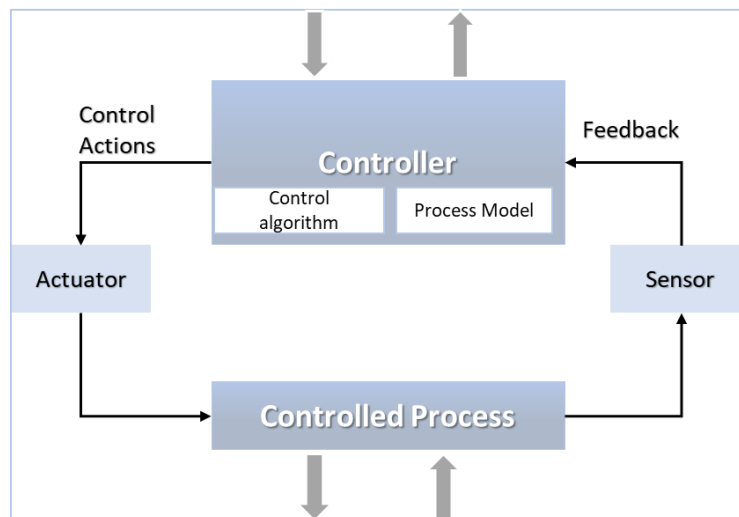


Figure 2. Control Structure Model

In the content of this deliverable, the first two steps of STPA are used to help in the process of threat detection within the TwinERGY system, while steps 2 and 4 were altered into a more simplified version in order to provide the countermeasures needed for the risk analysis conducted in the next sections.

STPA outputs shall be used in many different ways in the content of TwinERGY project in the next phases, among which the above are identified:

- Drive the system architecture
- Create executable requirements
- Identify design recommendations
- Identify mitigations and safeguards needed, and
- Drive new design decisions, since STPA is used during the project development

To conclude, STPA (System-Theoretic Process Analysis) [1] is used to define accidents and hazards as well as identify unsafe control actions within a system, while it mainly focuses on unsafe controlling interactions between system components. In STPA the main assumption is that accidents can be caused by unsafe interactions of system components, as well as component failures. What this methodology provides in terms of the requirements of this deliverable, is a powerful hazard identification method that proactively analyses potential causes of accidents related to system components.

3.2. STPA processes in TwinERGY

3.2.1. Data acquisition and qualitative processing

To acquire the data related to the TwinERGY project risk module, a Risk Template for each pilot site was initially created. The purpose of this template was to compile a list of threats

as detected in each pilot case. In order to create a comprehensive list of all threats, each pilot leader was asked to choose the systems (see Chapter 5) related to their pilot case and fill in the document with the threats and impacts corresponding to each one of them. The lists of threats with their frequency and magnitude (severity), along with the countermeasures installed, have been collected based on TwinERGY partners' feedback and the literature. Our partners provided their contributions through the template appendant in Annex A.

For the purpose of STPA analysis, our partners were further requested to provide possible causes and countermeasures of the threats detected in each system. Conjointly, the systems provided were eight as mentioned below:

1. Electric Vehicle System (EVS)
2. Charging Point System (CPS)
3. Electrical Panel System (EPS)
4. Photovoltaic System (PVS)
5. Smart Meter System (SMS)
6. Battery System (BS)
7. HVAC System (HVS)
8. Lighting System (LS)

Following, a list of threats was created based on each pilot system's level of analysis, the feedback provided by TwinERGY partners and the literature. In the following stages, the detected threats were characterized as Hazards or Losses, while possible causes were also detected. Finally, a list of controls (control actions) for the elimination of each risk was created.

The systems along with their detected threats, possible causes and countermeasures are listed in the next subsection of this deliverable.

3.2.2. Hazards and Losses - Identification and Analysis

In the tables below, each pilot system's threats are being provided. Each threat based on its severity and whether the impact is reversible or not, is being recognized as hazard or loss.

Table 5. EVS table, possible causes & suggested countermeasures

Electric Vehicle			
Identified threat	Characterisation (hazard/loss)	Possible causes	Countermeasures/List of controls to prevent/mitigate risks

Ordinary Maintenance	Hazard	Planned maintenance which due to unawareness or lack of experience can lead to unwanted hazardous events	Regular revisions to guarantee the correct operation of the vehicle
Unplanned Maintenance	Loss	Unexpected event can cause maloperation in the EV	-
Battery damage	Loss	Electrical, mechanical, chemical malfunctioning can damage the battery health	Follow up the scheduled calendar of the electric vehicle revisions to analyse the battery health
Repair	Hazard	Diverse incidents can cause the need for a reparation (e.g. due to environmental causes)	N/A
Fire	Loss	Defective electrical components can spark a fire	Follow up the scheduled calendar of the electric vehicle revisions to analyse the vehicle's status
Damage to the EV batteries	Loss	Attacks on the EV Battery management systems through compromised web services or malware	Patches for some of the vulnerabilities found in the EV ecosystems
Loss of load/Voltage-drop	Hazard	High percentage of EV penetration (uncontrolled EV charging especially during peak load)	Controlled Charging with V2G (vehicle-to-grid) scheme, Shifting the EV charging to night times

Table 6. CPS table, possible causes & suggested countermeasures

Charging Point			
Identified threat	Characterisation (hazard/loss)	Possible causes	Countermeasures/List of controls to prevent/mitigate risks
Ordinary Maintenance	Hazard	Regular revisions to guarantee the correct operation of the charging point	-
Unplanned Maintenance	Hazard	Unexpected event can cause disoperation in the EV	-
Vandalism, theft	Loss	Vandalic acts that can damage or make	Increase the monitoring of the Charging points

Cyber Attack	Hazard	disappear the charging infrastructure	
		The high interconnectivity can be seen as a gap to the rise of cyber vulnerabilities (malicious attacks, system outages, bugs and other glitches)	Upgrade constantly all the software involved in the Charging Point Operation Process
Server Failure	Hazard	The server in control to the charging points can face problems such as intermittent lack of internet connection	Upgrade constantly all the software involved in the Charging Point Operation Process
Fire hazard	Hazard/Loss	The charger is not working satisfactorily; Flammable or combustible material stored within the designated charging area	Security or other responsible staff on site who may be called to take action in an emergency

Table 7. PVS table, possible causes & suggested countermeasures

PV System			
Identified threat	Characterisation (hazard/loss)	Possible causes	Countermeasures/List of controls to prevent/mitigate risks
Fault/ electricity produced	No Loss	Malfunction, problem with the wiring	N/A
PV system offline (solar inverter offline)	Loss/Hazard depending on the cause	A communication issue in the daytime, an inverter issue or it can be a Wi-Fi issue, low production of electricity, overvoltage	Inspect all wires, connections, fuses and battery performance
Low production-panels producing less electricity than before (2%)	Hazard (can cause PV system going offline)	Uncleaned panels, poor electrical connections, Cracked or broken glass on panels	Panels cleaning in every 6 months, ordinary maintenance planned
Overvoltage	Hazard (can cause PV system going offline)	Poor electrical connections	Voltage control by Power Conditioning Systems (PCS)
Damage or shortened lifetime	Loss	Overvoltage	Voltage control by Power Conditioning Systems (PCS)
Overconsumption/Undervoltage	Hazard	Malfunction	Panels cleaning in 6 monthly ordinary maintenance planned
Constricted normal performance of electric equipment	Loss	Undervoltage	Voltage control by Power Conditioning Systems (PCS)

Bad performance	Loss	Weather conditions, sediment built up from weather residue, Cracked or broken glass on panels	Panels cleaning in 6 monthly ordinary maintenance planned
Discomfort (fault codes or error messages)	Hazard	System failure	-
Ordinary Maintenance	Hazard	Servicing, cleaning	Transparent back glass (TBC)
Unplanned Maintenance	Hazard	Malfunction	TBC

Table 8. SMS table, possible causes & suggested countermeasures

Smart Meter			
Identified threat	Characterisation (hazard/loss)	Possible causes	Countermeasures/List of controls to prevent/mitigate risks
Ordinary Maintenance	Hazard	Software updates and maintenance	Requirement for asynchronous messaging. Exception handling for missing data.
Unplanned Maintenance	Hazard	Software troubleshooting, OS crashes	Requirement for asynchronous messaging. Exception handling for missing data.
Time synchronisation error	Hazard	NTP connection failure	Alert notification
Device failure	Loss	Hardware/firmware failure	Alert notification
Inaccuracy in metrics	Hazard	System failure	Recording of the data and comparison of the readings. Alert notifications originating from historical data and possibilities
Application error	Loss	Loss of internet connection	Alert notification

Ordinary Maintenance Hazard Software updates and maintenance Requirement for asynchronous messaging. Exception handling for missing data.

Table 9. BS table, possible causes & suggested countermeasures

Battery			
Identified threat	Characterisation (hazard/loss)	Possible causes	Countermeasures/List of controls to prevent/mitigate risks
Ordinary Maintenance	Hazard	Software updates and maintenance	Requirement for asynchronous messaging. Exception handling for missing data.
Unplanned Maintenance	Hazard	Software troubleshooting. OS crashes	Requirement for asynchronous messaging. Exception handling for missing data.
Time synchronisation error	Hazard	NTP connection failure	Alert notification
Device failure	Loss	Hardware/firmware failure	Alert notification
Fire hazard	Hazard/Loss	Circuit breakers; Missing covers	Frequent electrical inspections
Application error	Hazard	Loss of internet connection	Alert notification

Table 10. HVS table, possible causes & suggested countermeasures

HVAC			
Identified threat	Characterisation (hazard/loss)	Possible causes	Countermeasures/List of controls to prevent/mitigate risks
Fault	Loss	Problem in device due to chronic use/ Old device	Suggestion for preventive service once a year
Standing water	Hazard	Low degree of tolerance for precipitation	Adequate drainage around the HVAC
Dirt builds up in the compressor	Hazard	Low frequency of inspections and cleaning	
Overconsumption/ Higher bills	Loss	Heater involved, inadequate maintenance	Suggestions via the application created during the TwinERGY Project for consumption lowering and cleaning
Bad performance	Loss	Problem in device due to chronic use/Heater, fluid lacking	N/A
Discomfort	Loss	Poor regulation of temperature; Poor humidity control; Poor filtration / source air	Alerts/Notifications, Frequent equipment inspections
Poor regulation of temperature; Poor humidity control; Poor filtration / source air	Hazard	Poor ventilation; Bad systems settings; Inefficient filters	A dedicated outdoor air system (DOAS) coupled with a radiant cooling system
Unplanned Maintenance	Hazard	Problem in device due to chronic use	-
Ordinary Maintenance	Hazard	Filters substitution	Alert notification

Table 11. LS table, possible causes & suggested countermeasures

Lighting System			
Identified threat	Characterisation (hazard/loss)	Possible causes	Countermeasures/List of controls to prevent/mitigate risks
Overconsumption	Hazard	Old device; No maintenance	Suggestions via the application created during the TwinERGY Project for consumption lowering and cleaning
Fault	Loss	Old Wiring, Heat Damage, Water Damage, poor quality lamps	Maintenance and timely replacement
Ordinary Maintenance	Hazard	-	-
Unplanned Maintenance	Hazard	Problem in device due to chronic use	-

Due to the lack of numerical data upon the frequency of each threat's occurrence, not all of the threats could be analysed quantitatively. However, this section provides a clear mapping of threats and countermeasures that could be used in the countermeasure application (see Chapter 6.4.), paving the way for a detailed Risk Analysis adjusted to the need of the pilot sites.

4. Quantitative Risk Analysis

This section seeks to explain how the user can use the tool to analyse the risk and to explain in detail what happens in the risk algorithm, including different steps and formulas [2]. Obviously, the quality of the results provided by the tool is strongly depended on the quality of the data entered as input.

The algorithm used to compute the risk in the Risk module is capable of handling several types of data as input. The data that the algorithm requires are:

- The topology and features of residential infrastructures.
- The model of the building with their areas and respective assets
- The number of people present in the building at given timeframes
- The countermeasure deployed to the various element presents in the model
- The services provided by the element presents in the model
- The specification of the threats
- The specifications of the impacts and consequences

These data are used by the algorithm to firstly, generate possible scenarios and then to compute the likelihood, the impact and associated risk of the scenario.

The model used by the algorithm implemented in this tool is based on a tree structure [3], [4]. It has been chosen to adopt this type of structure because in such way it is possible to track how every event contributes to the overall risk in a simple way. It is similar to the approach used in the Fault Tree Analysis, which is a standard technique used normally in risk assessment and accident analysis [5], [6].

4.1. Importance of the topology

The tree model structure used in the module (Figure 4), like the Fault Tree Analysis, adopts a top-down approach in which the triggering event is a threat against a certain target present in the network which generates several, even diverse, impacts. The mentioned propagation of impact is strongly dependent on the topology of the structure considered, since the impacts are generated and propagated depending on the connection among the elements in the network. The impacts generated are mitigated by the countermeasures present in the network which have the capability to mitigate or eliminate the effects of those impact and contribute to the generation of various outcomes.

One of the main differences compared to classical fault tree is the possibility to represent the building as a graph. Indeed, the tree approach is used to represent a scenario

occurring because of a threat, but within the same network it is possible to have several scenarios (and indeed several trees).

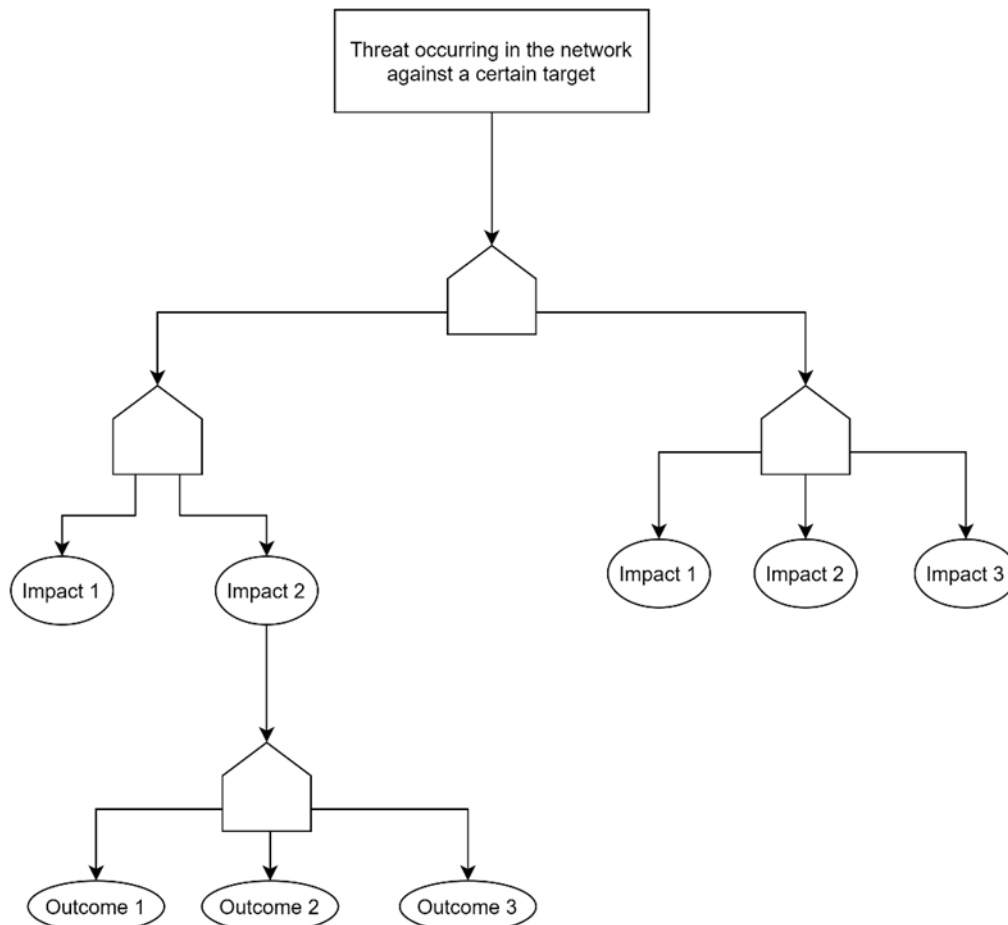


Figure 3. Tree Model

The algorithm created for this tool (Figure 5) can be subdivided in four steps:

1. **Scenario Generation:** depending on the parameters inserted by the user (network topology, assets, countermeasures, threats, targets, etc.) the scenario is generated.
2. **Scenario Simulation:** the previously generated scenario is simulated, taking into account the applied countermeasures and the cascading effect (which is responsible for the propagation of the threats and generations of the related impacts), and the various outcomes are generated.
3. **Likelihood Calculation:** after the outcomes are generated the corresponding likelihood is computed, starting with the computation of the probabilities related to the triggering event.
4. **Impact Calculation:** the effect of each outcome is computed in monetary terms, taking into account its related physical damages, out of service and revenue losses, but even fatalities and injuries can be considered.

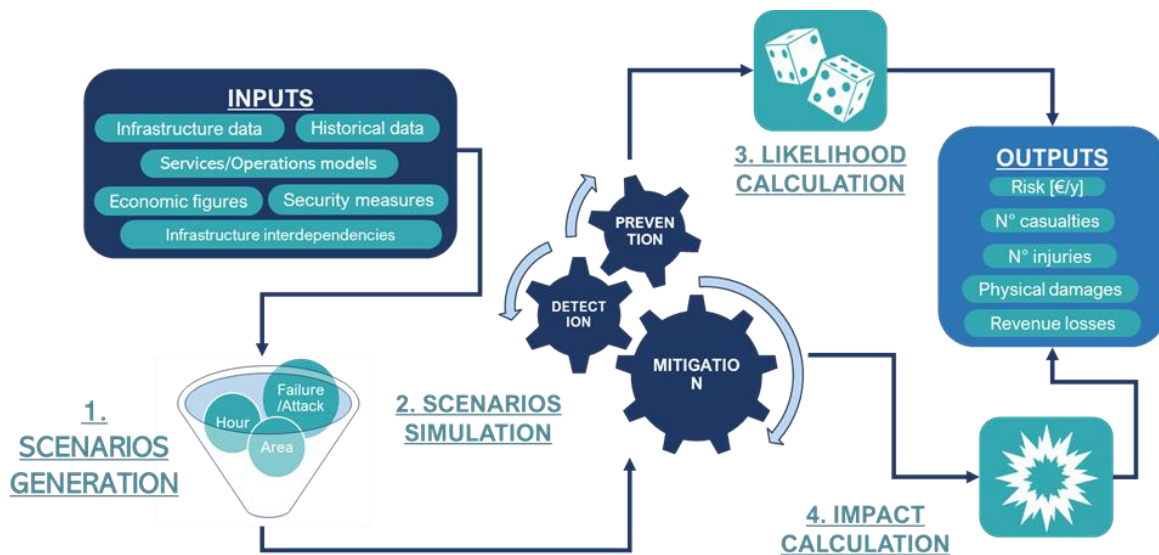


Figure 4. Risk Management Algorithm

4.2. Cascading effect, propagation of effects to multiple assets

As previously stated, the algorithm used in the risk module is based on a tree model structure, this specific structure facilitates the propagation of impacts in the modelled network. As said above, this is fundamental for the cascading effect since when something affects a parent node in the tree model the same will affect the corresponding child nodes. Another important aspect related to this model is that threats are intended to be propagated from the parent node to the children but not vice versa, respecting the hierarchy of the model of the infrastructure presented below. The rationale of this rule is avoiding incurring an infinite loop. However, since disruption of an asset is causing effects also on services, it is considered within the analysis that a damage to a small asset (e.g., the electrical panel) can cause degradation of the performances offered by the whole building.

The tree model operates a fundamental role in the computation of the risk in the algorithm (Figure 6). The computation of the risk begins with generation of the first impact on an element of the network. The computation is done for each possible magnitude of the impact, and depending on several parameters, such as the presence and effectiveness of the countermeasures, several outcomes could be generated. The impact on a specific element of the network could be Prevented, Defused, Mitigated, or Not mitigated and diverse outcomes could arise. Finally, the outcomes are propagated to the child nodes and the process is repeated.

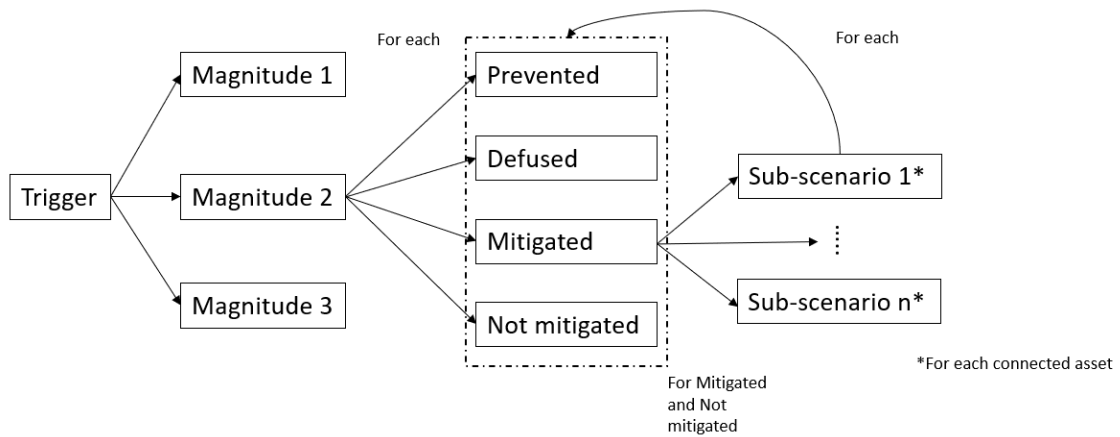


Figure 5. Process implementation

4.3. Inputs & Initial Data

In order to properly work the algorithm for the computation of the risk requires several parameters [7], [8]. The value that required to be collected in the Database [9] of the tool are:

- List of the areas present in the building $A_i = [a_1, a_2, \dots, a_i]$
- Time slots that need to be considered $T_i = [t_1, t_2, \dots, t_j]$
- List of all the possible threats $TH_i = [th_1, th_2, \dots, th_k]$
- Estimated occupancy of an area in a specific timeslot $EO_{ij}(A_i, T_j) \geq 0$
- The economic value of each area $EVA_i(A_i)$

Other starting parameters and initial computation that are present in the database of the tool are:

- The tree levels of magnitude $M_z = [m_1, m_2, m_3]$, which represents the intensity of a threat
- The probability of a specific anomaly $0 < POA_{tot} < 1$
- The probability of a certain threat

$$P(TH_k) = [P(th_1), P(th_2), \dots, P(th_k)]; \sum_{z=1}^k P(TH_k) = 1$$

- The probability of a certain threat with a certain magnitude

$$P(TH_k, M_z) = [P(TH_1, M_1), P(TH_2, M_2), P(TH_k, M_k)]; \sum_{z=1}^k P(TH_k, M_z) = 1$$

The total value of an area $TVA_{ij} = VSL * EO_{ij} + EVA$

4.4. Scenario generation

As previously mentioned, the starting step of the algorithm is the generation of a feasible scenario [6] [10]. A scenario in this case is characterised by three elements: threat, target, and time of occurrence. (1)

$$\text{Scenario}(\text{Threat}, \text{Target}, \text{Time of occurrence})\#(1)$$

Threat and target are fundamental in the identification of a scenario in order to understand the corresponding impacts and their relative propagation on the network elements, the time of occurrence is needed in order to define all the parameters that depends on the time, like for example the occupancy. The scenario is then subdivided in sub-scenarios (2), which, as said before, depend on the type of magnitude and the type of outcome.

$$\text{Sub - scenario}(\text{Threat}, \text{Magnitude}, \text{Target}, \text{Time of occurrence})\#(2)$$

The value of the magnitude is strongly related to the threats and to the users' perception of it. In this tool three levels are used: Low, Medium, and High. This means that for each scenario, three sub-scenarios are arranged based on the likelihood of the same threat considered with less or more intensity.

The equation that is used to compute the probability of a specific scenario is:

$$P(S_{ijkz}) = POA_{tot} * P(TH_k) * P(TH_k, M_z) * IM(A_i, T_j)\#(3)$$

4.5. Scenario simulation

Once an impact hit an element of the infrastructure, it is possible that the other elements which are linked to the targeted one in the model structure will be also affected by the impact and could even generate a consequent impact. (3)

$$\text{Impact}(\text{Sub - scenario}, \text{Secondary Target})\#(4)$$

This process is not immediate, there is the need to start taking into account the effects that the countermeasures have on the impacts. Since the countermeasures are directly applied to the element of the network that can be targeted by threats, they can even block the propagation of the impact and reduce the damages.

The application of the countermeasures can generate four diverse outcomes (Figure 7) :

- **Prevented:** when the impact is prevented, there are no impacts on the element targeted and the propagation stops.

The total efficiency of an area which is in Prevention is:

$$EP_{tot}^{sec}(A_i) = 1 - [(1 - P_1^{sec}) * (1 - P_2^{sec}) * ... * (1 - P_m^{sec})]\#(5)$$

The probability of outcome in this case is:

$$P_{SS1}(S_{ijkz}) = P(S_{ijkz}) * EP_{tot}^{sec}(A_i)\#(6)$$

- **Defused:** an impact is defused when the countermeasures are effective in not letting it generate any damage.

The total efficiency of an area in Defusion is:

$$EF_{tot}^{sec}(A_i) = 1 - [(1 - F_1^{sec}) * (1 - F_2^{sec}) * \dots * (1 - F_m^{sec})] \#(7)$$

The probability of outcome in this situation is:

$$P_{SS2}(S_{ijkz}) = P(S_{ijkz}) * (1 - EP_{tot}^{sec}(A_i)) * (ED_{tot}^{sec}(A_i)) * EF_{tot}^{sec}(A_i) \#(8)$$

- **Mitigated:** in this situation the impact happens but its effects are mitigated thanks to the countermeasures applied.

The total efficiency of an area with the impacts Mitigated is:

$$EM_{tot}^{sec}(A_i) = 1 - [(1 - M_1^{sec}) * (1 - M_2^{sec}) * \dots * (1 - M_m^{sec})] \#(9)$$

The probability of outcome in this case depends on the level of Magnitude, with low magnitude the equation is:

$$P_{SS3}(S_{ijk1}) = P(S_{ijk1}) * (1 - EP_{tot}^{sec}(A_i)) * [(1 - ED_{tot}^{sec}(A_i)) + (ED_{tot}^{sec}(A_i) * (1 - EF_{tot}^{sec}(A_i)))] * EM_{tot}^{sec}(A_i) \#(10)$$

The probability of outcome with medium magnitude is:

$$P_{SS5}(S_{ijk2}) = P(S_{ijk2}) * (1 - EP_{tot}^{sec}(A_i)) * [(1 - ED_{tot}^{sec}(A_i)) + (ED_{tot}^{sec}(A_i) * (1 - EF_{tot}^{sec}(A_i)))] * EM_{tot}^{sec}(A_i) \#(11)$$

The probability of outcome with high magnitude is:

$$P_{SS7}(S_{ijk3}) = P(S_{ijk3}) * (1 - EP_{tot}^{sec}(A_i)) * [(1 - ED_{tot}^{sec}(A_i)) + (ED_{tot}^{sec}(A_i) * (1 - EF_{tot}^{sec}(A_i)))] * EM_{tot}^{sec}(A_i) \#(12)$$

- **Not Mitigated:** when an impact is not mitigated it means that the countermeasures applied have no effect or that there are no countermeasures applied to the targeted element.

In this case the total efficiency cannot be computed, just the probability of outcome can be calculated. For the low magnitude the equation is:

$$P_{SS4}(S_{ijk1}) = P(S_{ijk1}) * (1 - EP_{tot}^{sec}(A_i)) * [(1 - ED_{tot}^{sec}(A_i)) + (ED_{tot}^{sec}(A_i) * (1 - EF_{tot}^{sec}(A_i)))] * (1 - EM_{tot}^{sec}(A_i)) \#(13)$$

For the medium magnitude:

$$P_{SS6}(S_{ijk2}) = P(S_{ijk2}) * (1 - EP_{tot}^{sec}(A_i)) * [(1 - ED_{tot}^{sec}(A_i)) + (ED_{tot}^{sec}(A_i) * (1 - EF_{tot}^{sec}(A_i)))] * (1 - EM_{tot}^{sec}(A_i)) \#(14)$$

For the high magnitude the equation is:

$$P_{SS8}(S_{ijk3}) = P(S_{ijk3}) * (1 - EP_{tot}^{sec}(A_i)) * [(1 - ED_{tot}^{sec}(A_i)) + (ED_{tot}^{sec}(A_i) * (1 - EF_{tot}^{sec}(A_i)))] * (1 - EM_{tot}^{sec}(A_i)) \#(15)$$

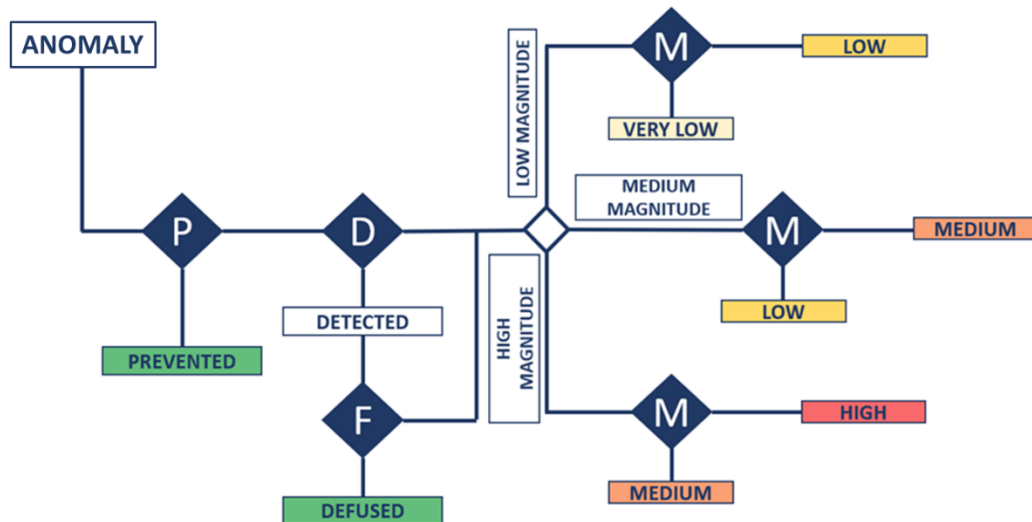


Figure 6. Possible Outcomes

The sum of the likelihood of all the outcomes for a possible scenario is equal to one since they cover all the possibilities for a given threat.

In order to estimate the outcomes, each countermeasure is defined by several parameters that define the efficiency of the countermeasures and the reduction of likelihood and damages. These parameters are scores in prevention, detection, defusion and mitigation.

Since one of the main features is the cascading effect, the outcomes Mitigated and Not Mitigated can propagate to the connected element of the model infrastructure generating new impacts.

In order to propagate the impact and generate consequent impacts, a specific mapping is required for the Risk algorithm (Figure 8).

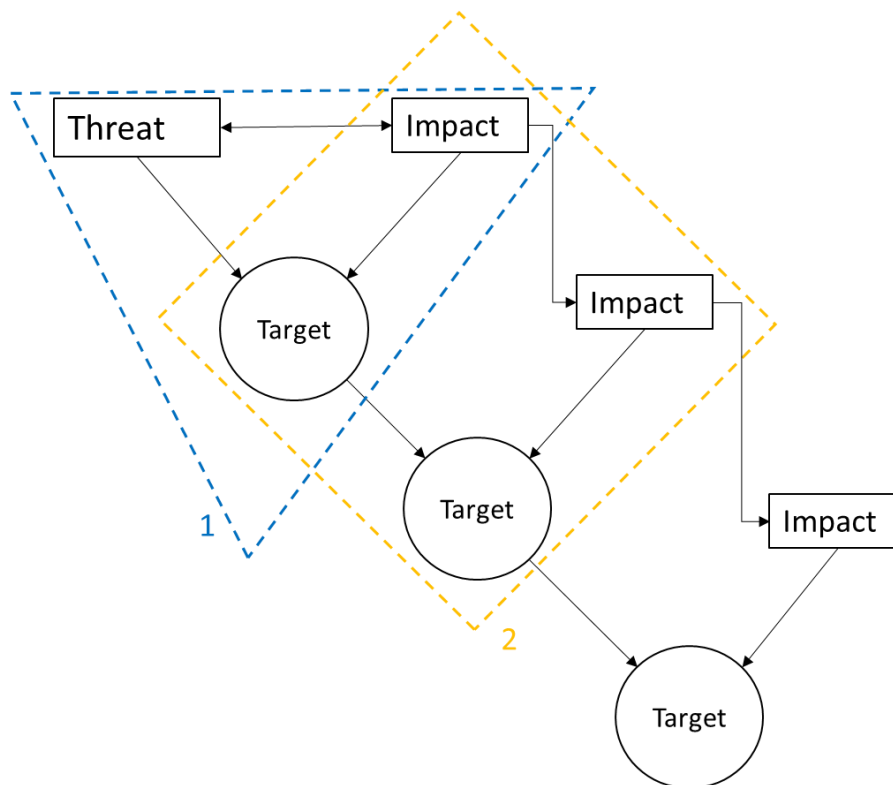


Figure 7. Mapping for the propagation

In the figure above it can be seen that the mapping can be divided in two parts. In the first section of the mapping (the blue triangle in the figure), the threat is mapped to a target, and both are mapped to an impact. This is due to the fact that only some targets can be targeted by some threats, and depending on the target and the threat, a specific impact is generated. The second section of the mapping (the orange square) links the starting generated impact to the subsequent one, and the new target to the old one. Depending, on the starting target and impact, new element of the network can become new target and they can even generate new and different impacts.

4.6. Likelihood Calculation

As previously stated, for each of the outcomes generated the algorithm computes the likelihood of occurrence.

This kind of computation starts with the *POA*, which is present in the software. It is a value which is estimated from the literature and from the contributions of the pilots' representants and of their technical support partners; based on their experience and on historical record data, these are values collected in the database of the platform [10].

It is important to highlight that, diverse threats have diverse probabilities, so the *POA* is computed using the following equation:

$$POA(TH_k, M_z) = [P(TH_k, M_1)P(TH_k, M_2)P(TH_k, M_3)] = \sum_{z=1}^3 P(TH_k, M_z) \#(16)$$

The meaning of this formula is that the percentage for specific threat is subdivided among the three level of magnitude.

The result of such equation is not the finale value of the *POA*, to compute the finale value a few steps are required:

1. The likelihood is subdivided among the elements of the building. The values are split considering that some elements are more critical than others in the supply of services or because they have higher cost, or they are more relevant in ensuring the security.
2. The likelihood is also divided according to the time frame that is being considered, since some threats have more probability of happening when there are more people present.
3. The likelihood can be reduced by the overall protection score that is relative to the target considered.
4. The likelihood is reduced of a predefined percentage each time an impact generates a new threat, since the cascading effect is not deterministic.

The final value of the likelihood is a frequency assigned to each outcome generated by the simulation of the scenario.

4.7. Impact Calculation

The computation of the impact is conducted at the same time of the estimation of the likelihood. For every outcome generated the tool computes:

- Percentage of physical damage of the target
- Average number of users affected
- Average hour of interruption of services
- Expected economic losses due to physical damage
- Expected economic losses due to interruption of service

Also in this case, the estimation of the impact is strongly dependent on the type of threat, target, impact, and magnitude.

The final value of the impact calculation is the estimation of total economic losses, which is computed using the equation below.

$$EL_{tot} = +EL_{physical_damage} + ELIS_{tot} \#(17)$$

4.7.1. Computation of physical damages

Concerning the physical damages, it is estimated as a percentage that symbolizes how much the integrity and functionality of an element has been affected.

To compute the economic losses at first there is the need to compute the physical damage function, which strongly depends on the type of anomaly and level of magnitude. But it important to highlight that there are two different types of physical damage functions, which depend on the type of outcome: Mitigated (18) or Not Mitigated. (19)

$$PD_{mitigated}(TH_k, M_z) \#(18)$$

$$PD_{not_mitigated}(TH_k, M_z) \#(19)$$

$$PD(th_k, m_k) = PD_{base} \#(20)$$

Finally, the equation used to estimate the economic losses related to physical damages is:

$$EL_{physical_damges} = PD(th_k, m_k) * EVA_i(A_i) \#(21)$$

4.7.2. Estimation of out of service

Another important aspect for the correct estimation of the economic losses is the estimation of the out of service. In this estimation there is the need to take into account the value of the element of the building considered, and the maintenance cost that could be required for the restoration of the functionalities.

It has been chosen to consider those parameters because the time required to repair an asset is proportional to its cost, and also the choice of replacing or fixing an asset is strongly related to the corresponding costs.

Taking all of this in consideration, the formula used to compute the time of out of service is:

$$Toos(Value, Damage, Type) = \{T_{fix}, \quad C_{fix} < C_{rep} T_{rep}, \quad C_{rep} \geq C_{fix} \#(36)$$

Where T_{fix} (37) is the estimation of the time required to fix the asset, T_{rep} (38) is the time required to replace the asset, C_{fix} (39) is the cost of repairing the asset, and C_{rep} (40) is the cost of replacing the asset.

$$T_{fix}(Damage, Type) = Type_{RepairRate} * Damage + 0.5 \#(37)$$

$$T_{rep}(Value) = 6 * 10^{-16} * Value^3 + 8 * 10^{-10} * Value^2 + 0.0004 * Value + 1 \#(38)$$

$$C_{fix}(Damage, Type) = Type_{RepairCost} * People_{Needed}(Damage) * T_{fix}(Damage, Type) \#(39)$$

$$C_{rep}(Value) = Value \#(40)$$

$$People_{Needed}(Damage) = -1 * 10^{-10} * Damage^2 + 0.0002 * Damage + 1 \#(41)$$

Where $Type_{RepairCost}$ and $Type_{RepairRate}$ are respectively the salary of one day of work for the people required to repair an asset and the time required to repair one euro of damage on the considered asset.

So, the estimation of the economic losses for the out of service depend on either if it chosen to repair the asset or to substitute it.

$$ELIS_{tot} = \{C_{fix}, \quad C_{fix} < Threshold \quad C_{rep}, \quad C_{rep} < Threshold \#(42)$$

The value of the threshold is predetermined for each type of asset present in the network and saved on the database.

4.8. Risk computation

After conducting all the previous steps, it is possible to compute the overall risk score, which is computed for each possible outcome of the scenario. The formula usually used to estimate the risk score:

$$Risk = Likelihood \times Expected \text{ damages} \#(43)$$

This equation in SecuRail becomes:

$$RiskLevel_i = P_{SSi} * EL_{tot} \#(44)$$

The risk score is expressed in monetary terms (€/year) since the likelihood is expressed in number of expected events per year and the expected damages in euros. The risk score of a scenario is considering the threat set as the trigger of the scenario (e.g., Overconsumption), as well as all the consequent impacts caused by the initial threat.

4.9. Algorithm implementation

The functionalities of the algorithm are implemented in the backend of the Risk tool. The backend can be seen subdivided in two parts, one responsible for the computation of the risk and one responsible to manage all the specific elements related to the residential buildings.

The Risk backend is responsible for modelling and keeping track of the relation between threats and their response. In this part of the backend are modelled the countermeasures, threats, targets, services, and other elements fundamental for the computation of the risk [12], [13].

Concerning the Building backend, it is the part responsible for managing everything specific to the residential environment. Here all the elements of the infrastructures: sections, areas and assets are managed.

5. Set up of the Risk analysis

In the following chapter the application of the algorithm is depicted in a typical building configuration. In the real application in the pilots, the building configuration is going to be taken as input from the Digital Twin (DT).

The threats for the risk module and the respective countermeasures have been collected with the use of STPA methodology and our TwinERGY partners' feedback, while data regarding the threats' frequency and magnitude (severity) has resulted from literature and the TwinERGY partners' feedback where possible.

Due to the infancy of the pilot demonstrations, the frequency and magnitude (severity) of some of the threats detected with the STPA could not be provided or predicted. For this reason, for the risk analysis tool only the ones resulting from partners feedback were kept for the computation method. Our TwinERGY partners' contributions are explicated through the template in Annex A.

5.1. Configuration and Asset's topological structure

In Figure 6 are shown the main entities (Asset, Area and Devices) of the assets tree model structure inside the risk algorithm.

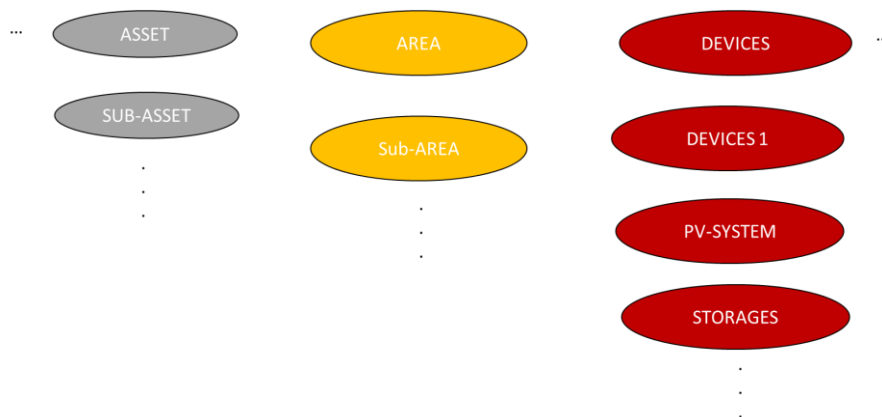


Figure 8. Topological Entities

The correlation among the entities creates the structure hierarchy and the structure is highly scalable.

In order to configure the risk module within the TwinERGY project for the module release and the tests purposes, it has been created an ad-hoc model that describes the graph structure of an asset of type "Building - Townhouse". This kind of models (to be precise, slight generalizations of those) are the ones needed in the majority of project's use cases.

The figure below summarizes the topology of a simple townhouse used for the first tests. To configure the risk module within the TwinERGY project for test purposes, we have created an ad-hoc model that describes the graph structure of a single asset of type "Independent Building". This kind of models are the ones needed in the majority of the use cases.

The figure below summarizes the topology of a simple townhouse used for the first tests.

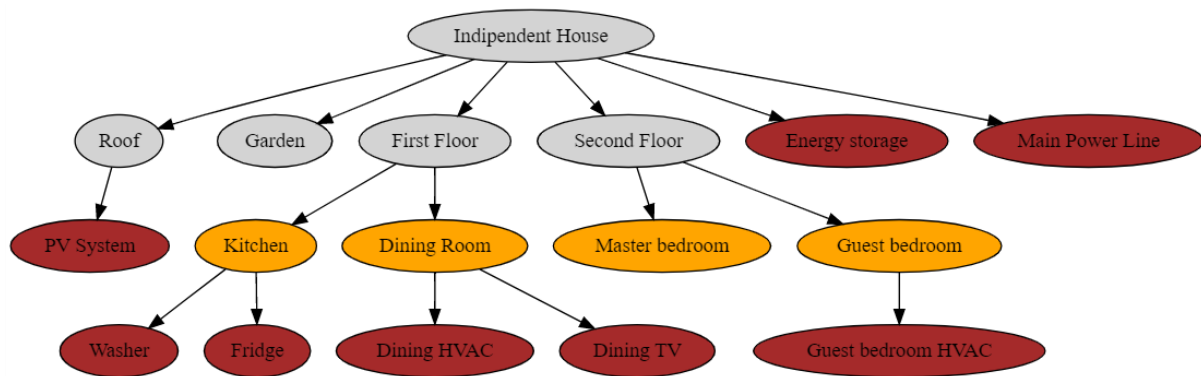


Figure 9. Topology of simple townhouse

From now on it is refer to:

- Parent – as the higher-level entities
- Child – as the entity related to the parent ones

The parenting relation means that an event to a parent node could also influence the children node.

Its structure is as follows:

- the root node is a Asset named "Independent House" has six children:
 - Roof, whose target type is "Area"
 - Garden, whose target type is "Area"
 - First Floor, whose target type is "Area"
 - Second Floor, whose target type is "Area"
 - Energy Storage, whose target type is " Photovoltaic System "
 - Main Power Line, whose target type is "Device"
- the first floor has, in turn, two children:
 - Kitchen, whose target type is "Sub-Area"
 - Dining Room, whose target type is "Sub-Area"
- the second floor has two children:
 - Master bedroom, whose target type is "Sub-Area"

- Guest bedroom, whose target type is "Sub-Area"
- the roof has one child:
 - PV System, whose target type is "Photovoltaic System"
- the kitchen has two children which represent two appliances:
 - Washer, whose target type is "Electronic Device"
 - Fridge, whose target type is "Electronic Device"
- the dining room has also two children:
 - Dining HVAC, whose target type is "Electronic Device"
 - Dining TV, whose target type is " Electronic Device"
- finally, the guest bedroom has a single child:
 - Guest Bedroom HVAC, whose target type is " Electronic Device"

The target type of any target defines which threats' impacts a target can undergo. e.g., A target of type "Electronic Device" may suffer of a permanent failure or of a temporary malfunction. Both are called impacts of a specific threat that may occur on the target, e.g., the threat "Device Obsolescence". Threats and their impacts are better described further in this page.

5.2. Threats and Impacts

In order to correctly configure the Risk module, two basic concepts need to be introduced:

1. **Threat** - action/event that may cause danger, damage, or any other unexpected behaviour; any threat has at least one impact
2. **Impact** - the effects/consequences of a threat on a given target type

Ex. On the target type "Electronic Device" the threat "Device Obsolescence" may give rise to the impact "Temporary Malfunction".

Ex. On the target type "Photovoltaic System" the threat "PV System Malfunction" may produce the impact "Low Production".

We started extracting the number of threats and impacts for TwinERGY scope by looking at the data contained in the Risk Template shared by the partners.

In Table 4 the data collected from the risk templates are shown, while the threats probability which was obtained by our project partners is also displayed.

First draft of detected threats within Twinergy project

Impacts	Severity (1 to 10)	Threats	Probability
Power supply interruption	3	Power loss	0,049315068
Overconsumption	5	Energy Demand Overload, Malfunction, Heater involved, Old device, No maintenance	0,136986301
Overvoltage	5	Energy Demand Overload	0,04109589
Undervoltage	3	Malfunction	0,035616438
Overcurrent	3	Malfunction	0,001369863
Overpower	3	Malfunction	0,001369863
Unplanned Maintenance	8	Malfunction due to improper use of appliances	0,071232877
Ordinary Maintenance	3	Servicing, Cleaning, Malfunction, filters substitution	0,032876712
Time synchronisation error	6	NTP connection failure	0,002739726
Device failure	10	Hardware/firmware failure	0,000547945
Application error	9	Loss of internet connection	0,016438356
Bad performance	8	Heater, fluid lacking, Weather conditions, sediment built up from weather residu	0,093150685
Discomfort	9	--	0,139726027
Fault	10	Malfunction/Old device	0,024657534
Battery damage	6	Electrical, mechanical, chemical malfunctioning can damage the battery health	0,002739726
Repair	5	Diverse incidents can cause the need for a reparation	0,002739726
Vandalism/theft	10	Vandalic acts that can damage or make dissappear the charging infrastructure	0,001369863
Cyber Attack	10	The high interconnectivity can be seen as a gap to the rise of cyber vulnerabilities (malicious attacks, system outages, bugs and other glitches)	0,001369863
Server Failure	6	The server in control to the charging points can face problems such as intermitent lack of internet connexion	0,002739726
Low production	6	uncleaned panels	0,093150685

Figure 10. Partners' feedback collected

Other threats and impacts will arise in the future during the project, and they can be included in the TwinERGY Risk module data model. Also threats and events depending on Demand Response actions will be included following the progress of the project.

5.3. Risk Computation

To assess the approach to the risk computation within TwinERGY, it is considered in the following three use cases.

Given the "Independent Building" model described above.

1. It is considered the threat "PV System Fault" on the target type "Photovoltaic System". The impact of this threat on the target type "Photovoltaic System" is "Low Production". There is only one target of type "Photovoltaic System" in the "Independent Building" model. Furthermore, the impact "Low Production" may have secondary impacts related to it, namely "Power Supply Interruption" and

"Discomfort". These secondary impacts are taken into account in the risk computation.

2. It is considered the threat "Device Obsolescence" on the target "Dining room HVAC"; this target has type "Electronic Device". The impact of this threat on the target type " Electronic Device" is "Temporary Malfunction". The impact "Temporary Malfunction" may have a "Discomfort" impact as secondary impact.
3. It is considered the threat "Power Loss" on the root target "Independent House"; whereas the threat "Power Supply Interruption" has impact "Power Loss". Since the root target has many children, the impact "Power Loss" propagates to any other area in the model, like kitchen, dining room and the bedrooms. Moreover, the impact "Power Loss" has a secondary "Temporary Malfunction" impact on any target type "Area Electronic Device" that affects all appliances in the model, e.g. Dining HVAC, Fridge, Washer, etc.

The following flow chart roughly explains which steps the risk algorithm performs within the use case of Threat "Power Supply Interruption" occurring on the asset "Independent building".

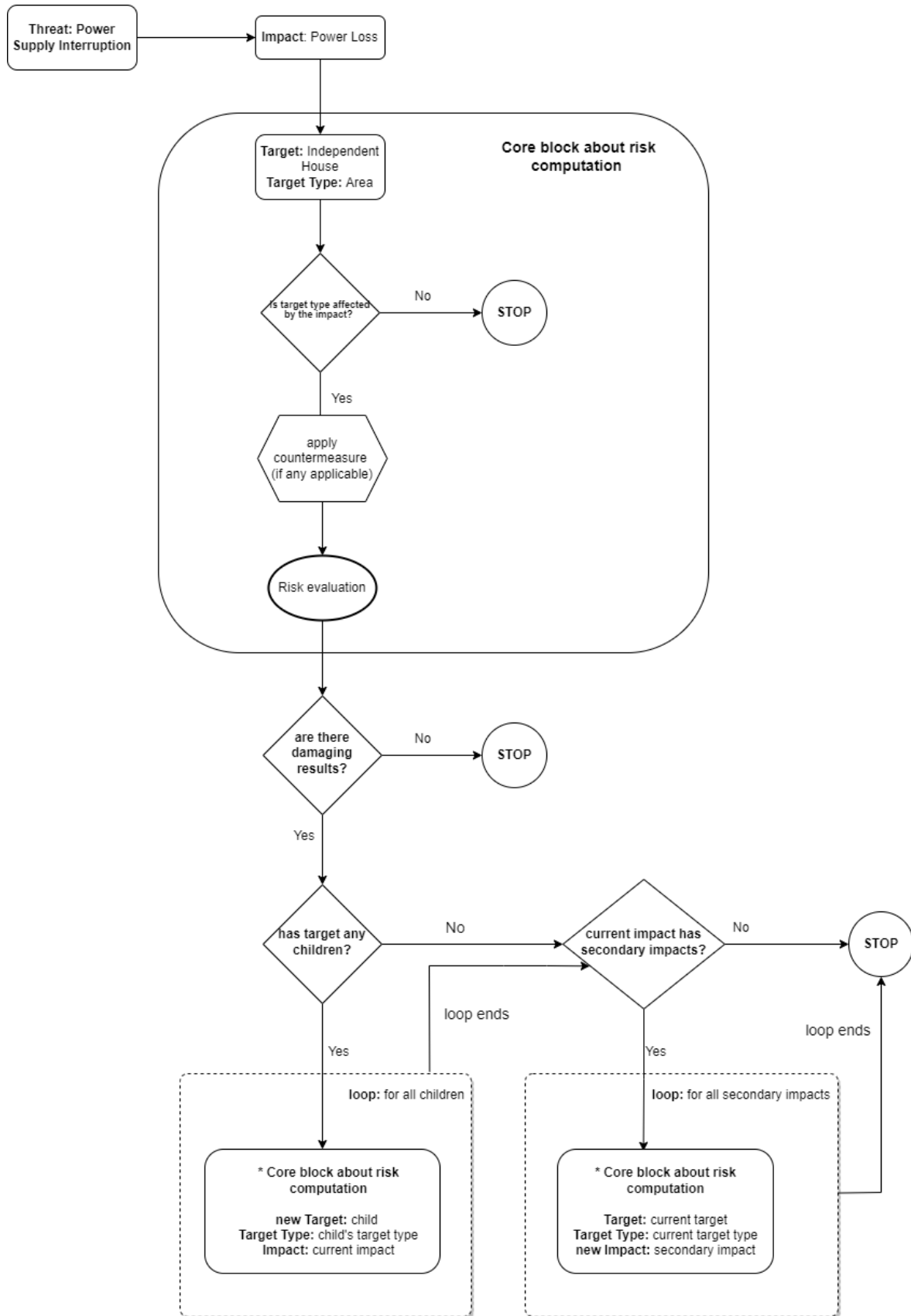


Figure 11. Flow chart of the Algorithm logic based on the Power Loss Threat

Flow chart explanation:

1. For a threat onto a target, it checks first if the target's impact affects the target type
2. If so, it applies the countermeasures (if any) and evaluates the risk on that target
3. Secondly, it checks whether the target has any child
4. If so, it verifies if the child's target type is affected by the impact
5. If so, it applies the countermeasures (if any) and evaluates the risk on the child target
6. The operation in 4. - 5. are performed for all children
7. The points 1. - 6. implies that the graph structure of the asset is explored following a depth first search logic
8. When any child is reached, the algorithm verifies also if the current impact has any secondary impact that may affect the target type of the current child
9. If so, it applies the countermeasures for all secondary impacts and evaluates the risk

5.4. Countermeasures application

On any target type one can apply countermeasures that could prevent or at least mitigate the impact [10]. A countermeasure can affect a given impact by

1. **preventing** the impact; the prevention rate of the countermeasure is the probability of the countermeasure to prevent the impact
2. **detecting** the impact; the detection rate is the probability to detect the impact
3. **defusing** the impact; the defusion rate represents the probability to defuse the impact
4. **mitigating** the impact; the mitigation rate represents the probability to mitigate the impact

The countermeasures will influence the threats probability as a reduction coefficient [14].

- The effect rates of any countermeasure for its four properties, e.g., mitigation rate, prevention rate, etc.
 - The correlated effect rate is expressed in terms of percentage:
 - Prevention rate - x%
 - Detection rate - x%
 - Defusing rate - x%
 - Mitigation rate - x%
- Economic reference value for the asset operations

-
- Single value: e.g., 10.000 € for the target (Independent house) and its operations
 - For each impact, the percentage of damage in the asset

Given a target with some countermeasures applied and a threat occurring on this target the risk algorithm checks if any countermeasure installed is effective against the impact of the threat. If so, it computes the "effect rate" of the countermeasure on that impact with respect to all four countermeasure properties. Finally, corresponding to each countermeasure's property it evaluates again the risk of the current threat onto the current target by taking into account the countermeasure's efficiency of that property.

6. Users experience and results

6.1. Risk Analysis GUI

The risk module is integrated as a microservice in the Graphic Users Interface of the TwinERGY Platform. From there, the users can select a specific threat from a list of preconfigured threats, and the target intended as the system involved in his building. After inserting of the aforementioned values, the risk analysis can be executed by clicking on the yellow run button on the card positioned on the top of the page. The user experience is presented by the web page represented in Figure 12.

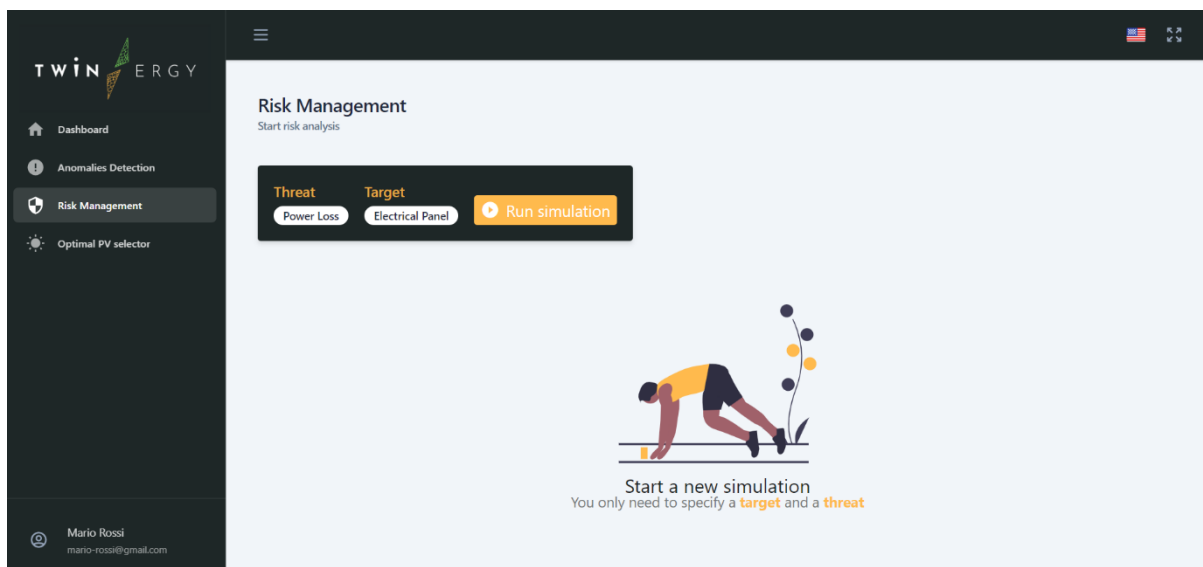


Figure 12. Scenario selection risk GUI

The results of the analysis are provided in the dashboard as shown in Figure 13. The results are provided is through a dashboard which presents the results in an aggregated way in order to be easily understandable by the user. The values which are reported on this page are:

On the left

- The number of cascade appliances involved by the threat
- The value of the risk in €/year
- The countermeasure installed against the threat

On the right

- The detailed card of the devices involved
- The value of the probability (likelihood) corresponding to the diverse threats

- The devices scenario presented with its corresponding impacts in €
- An indication of the most common action to avoid the specific threat

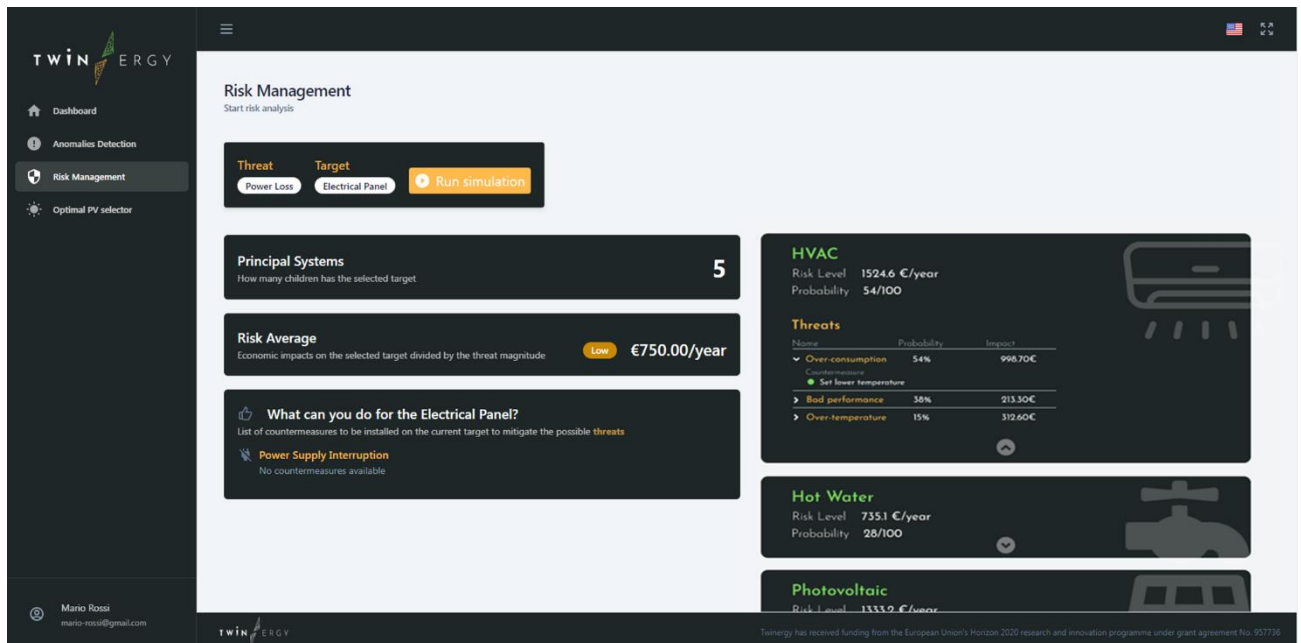


Figure 13. Risk Analysis results in the GUI

The module is deployed online at <https://twenergy.stamtech.dev/risks>.

7. Conclusions and next steps

This document has described the functional aspects of the Risk Management module. Specifically, the logic of the algorithm underlying the risk analysis engine is reported to make the risk assessment process transparent to the stakeholders involved. The interfaces and commands of the web application has been explained in order to give an overview of what the end-user, i.e., the tenants and/or the building manager, can do through the tool and what results can be gathered.

The most important step for the consistency of the risk analysis results relays on the quantity and quality of the data provided in input. Now, these data relays on the literature and on the expertise of the TwinERGY partners. The next steps for further development of the algorithm will focus on a more dynamical way to add and update these data. It would be possible by the users, by the maintenance technicians and/or thanks to the monitoring system and correlating the database with the outputs of anomalies detection algorithm, such as the one developed in the T7.4 Home & Tertiary real-time Energy Monitoring Module. These objectives are going to be pursued during the progress of the TwinERGY project and later on.

The module is deployed online at <https://twinergy.stamtech.dev/risks>.

Currently no authentication is required. It will follow the integration phase.

Annexes

Annex A. Data collection from pilots and partners' expertise

Sheet 1 - System involved

Dear Partners, here you can add the more critical energy system in your UC/Pilots. To do that, you need to add/delete/modify the list of elements in "Main energy system involved". It is currently requested a focus on the systems referred to the building level with domestic usage.

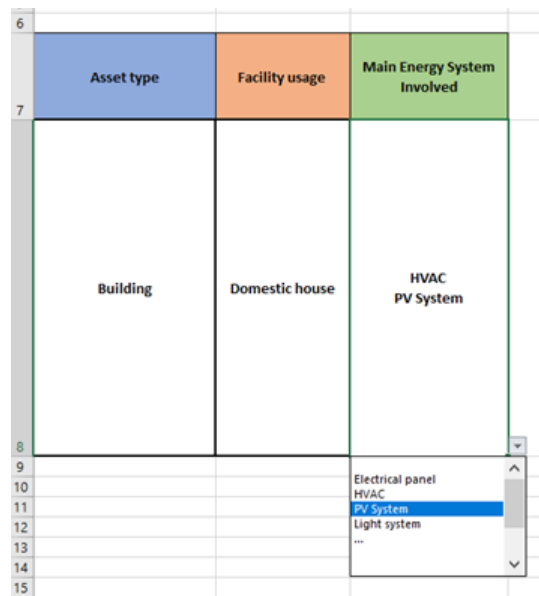
Feedbacks from experts		
Asset type	Facility usage	Main Energy System Involved
Building	Domestic house	Electrical panel
		HVAC
		PV System
		Light system
		...

We are interested especially to explore the systems at building level and in relation to the Domestic usage. Because of that, the "asset type" and the "Facility usage" in the table in the left are read-only.

In the column "Main energy system involved" you can add the most critical systems related to your UC. These elements will be related to the threats of your UC/Pilots, following your expertise and experience or from literature.

Sheet 2- Threats

Based on the *systems involved* listed in the Sheet 1, you can create a new table of threats selecting the energy system from the dropdown list as shown in Figure 13 for the PV System.



6			
7	Asset type	Facility usage	Main Energy System Involved
8	Building	Domestic house	HVAC PV System
9			
10			Electrical panel
11			HVAC
12			PV System
13			Light system
14			...
15			

Figure 14. System involved selection

As shown in in the Table 6 for the PV system, you need to provide the main threats/events that can occur on the system, with information about annual frequency, severity and the possible causes.

Table 12. Threats description template - PV System example

Threat - PV System	Number of days per year in which the event occurred	Severity (1 to 10)	Possible causes
PV system offline			
Low production			
Overvoltage			
Fault			
Ordinary Maintenance			
Unplanned Maintenance			
Other 1 (Specify)			
Other 2 (Specify)			
Other 3 (Specify)			
...			

As shown in Table 7 we have already selected some of the most interesting systems we want to gather the data for, and some of the most common threats events are populating the tables, but please add every systems/elements you do think are the more influent in your UC/pilots and complete and integrate the related table. Some of the typical threats, for common systems, have been already selected. It is required to fill in the data about the already selected threats (if they well fit your UC) and please add/modify them based on your expertise.

For the new systems, a custom table will appear. An example is shown at the end of Table 7 using as sample *Trial 1*.

Table 13. Main Systems - Threats description template

Threat - Electrical Panel	Number of days per year in which the event occurred	Severity (1 to 10)	Possible causes
Power supply interruption			
Overconsumption			
Overvoltage			
Undervoltage			
Overcurrent			
Overpower			
Ordinary Maintenance			
Unplanned Maintenance			
Other 1 (Specify)			
Other 2 (Specify)			
Other 3 (Specify)			
...			
Threat - HVAC	Number of days per year in which the event occurred	Severity (1 to 10)	Possible causes
Fault			
Overconsumption			
Bad performance			
Discomfort			
Ordinary Maintenance			
Unplanned Maintenance			
Other 1 (Specify)			
Other 2 (Specify)			
Other 3 (Specify)			
...			
Threat - Light System	Number of days per year in which the event occurred	Severity (1 to 10)	Possible causes

Overconsumption			Old device/No maintenance/...
Fault			
Ordinary Maintenance			
Unplanned Maintenance			
Other 1 (Specify)			
Other 2 (Specify)			
Other 3 (Specify)			
...			
Threat – Trial 1	Number of days per year in which the event occurred	Severity (1 to 10)	Possible causes
Ordinary Maintenance			
Unplanned Maintenance			
...			

Sheet 3 - Countermeasure installed

Here you can deploy the countermeasures peculiarities related to a specific pilot. It is asked to populate the table with countermeasures related to some threats you selected in the previous sheet (sheet 2).

Based on your expertise and experience in Table 8 you can provide the information about the countermeasures actives in a pilot and related to the threats. Please add/substitute/modify the specific values and feel free to detail them whenever is necessary.

Table 14. Countermeasures installed template

Threats	Common countermeasures installed	Pilot
PV fault	NA	Benetutti
PV Low Production	Panels cleaning in 6 monthly ordinary maintenance planned	Benetutti
HVAC Fault
HVAC Overconsumption
HVAC Bad performance
...		

References

- [1] Leveson, N. G., & Thomas, J. P. (2018). STPA handbook. Cambridge, MA, USA.
- [2] I. Iso, "Risk management-Principles and guidelines," *International Organization for Standardization, Geneva, Switzerland*, 2009.
- [3] I. Robinson, J. Webber, and E. Eifrem, *Graph databases: new opportunities for connected data.* " O'Reilly Media, Inc.," 2015.
- [4] 22. Lucidchart, "ntity-Relationship Diagram Symbols and Notation."
- [5] C. of Europe. C. for C. C. E. Committee. M. L. Division, *Common European framework of reference for languages: Learning, teaching, assessment.* Cambridge University Press, 2001.
- [6] M. Glinz, "A glossary of requirements engineering terminology," *Standard Glossary of the Certified Professional for Requirements Engineering (CPRE) Studies and Exam, Version*, vol. 1, p. 56, 2011.
- [7] ENISA, "Glossary - Risk Management." <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary> (accessed Jun. 21, 2021).
- [8] ENISA, "Glossary. Risk. [Online] ." <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary> (accessed Jun. 21, 2021).
- [9] N. K. Anh, "Database System Concepts." <https://cnx.org/contents/tXuHYGiY@1/Database-System-Concepts> (accessed Aug. 28, 2021).
- [10] S. Haugen and M. Rausand, "Introduction Hazardous event Accident scenario Probability Consequences Severity Risk Safety Accident Risk Assessment 2. The Words of Risk Analysis." [Online]. Available: <http://www.ntnu.edu/ross/>
- [11] Chartered Accountants, "Risk Management. Monitor & Review." https://survey.charteredaccountantsanz.com/risk_management/small-firms/monitor.aspx (accessed Dec. 10, 2021).
- [12] G. Simsion and G. Witt, *Data modeling essentials.* Elsevier, 2004.
- [13] P. Merson, "Data model as an architectural view," *CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST*, 2009.
- [14] S. Hiermaier, S. Hasenstein, and K. Faist, "Resilience engineering-how to handle the unexpected," in *7th REA Symposium*, 2017, p. 92.