Improving the robustness of urban electricity networks
IRENE

D4.2 – Open modelling framework

Document version: v7.0
Document status: Draft – Ready for Final Review – To be delivered at AB by 25th of January
Project Document Date: 23/01/2017
Workpackage Contributing to the Project Document: WP4
Dissemination level: confidential
Author(s):
Andrea Ceccarelli (UNIFI, Editor)
Tommaso Zoppi (UNIFI, Editor)
Andrea Bondavalli (UNIFI)
Alexandr Vasenev (UT)
Anhtuan Le (QMUL)
Eng Tseng Lau (QMUL)
Michael Chai (QMUL)
Yue Chen (QMUL)
Edward Lambert (Ethos)
Keith Chappell (Ethos)
Oliver Jung (AIT)
Sandford Bessler (AIT)
Daniel Hovie (AIT)
Internal Reviewer(s):
To Be Assigned

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This deliverable is the last report of Work Package (WP) 4 “Tool Development”. It describes the activities performed in Task 4.3 “Integration and Validation”.

The activities here reported investigate how to integrate all the models and algorithms developed within the WP4 and the rest of the IRENE projects in a unique *open modelling framework*. This framework brings together methodologies, policies and the toolset to evaluate and measure the resilience of the targeted smart grid.

More precisely, the Task 4.3, and consequently this deliverable, aims at

i) building an integrated methodology and framework that merges in a unique process all the different components, and
ii) validating the proper integration of all components.

This task collects inputs from other tasks in the same WP (Task 4.1, Task 4.2), and previous IRENE WPs (WP1-3).

The deliverable first summarizes the inputs to define a set of information and policies that the user of the framework (i.e., a stakeholder) must provide in order to use the different tools (these are mostly inputs of the different tools, and requirements for their usage). Then the deliverable overviews the tools that were developed in the whole project and that are going to be integrated in the framework.

Further, the deliverable describes the overall methodology and framework that integrate all the considered tools, resulting in i) an open modelling framework composed of tools and specification of inputs and outputs, ii) a methodology, which allows defining a workflow that combines the usage of tools, and iii) policies and additional information to support the final users of such framework, including the methodology to exercise it.

The usage of the open modelling framework is then regulated by the collaborative framework that traces the bounds of the interaction among different users of the framework (e.g., generic stake-holders, DNOs, city planners, regulators).

The rest of the deliverable reports on the validation of such integration process which results in the open modelling framework. The validation of the integration is performed by applying the workflow on a sample scenario based on the Smart Grid architecture that was built within IRENE WP3. This demonstrates how the framework can be used on a grid scenario, simulating the user inputs (e.g., providing a grid topology) and showing the whole process including the final outputs provided by the open modelling framework.

1 INTRODUCTION

This deliverable describes the open modelling framework that was developed within the IRENE project. This framework brings together methodologies, policies and the toolset to evaluate and measure the resilience of the targeted smart grid. The framework will be used to investigate threats in the smart grid and to put into practice the identified solutions. Based on identified outage scenarios, risk analysis and resilience ratings, provided by the developed framework, provide a way to support city planners in their decisions.

The framework include tools performing an extensive threat analysis that leads to the identification of possible root causes of outages, which are then simulated to estimate the capabilities of the grid to supply its components also when an outage happens. Further, models of the different settings and mitigation methods are integrated into the framework to enable users to evaluate the efficiency of fault and attack mitigation measures, the energy resilience outcomes, and the impact on different critical infrastructures.

In addition, this documents focuses on the effort of integrate all the models and algorithms, and get an understanding of their performance in terms of prediction accuracy. Then, an internal validation of the integration of all the components is performed.

1.1 MOTIVATION OF OUR WORK

IRENE aims at evaluating how a decentralized energy generation in urban areas can allocate energy to supply critical infrastructures, when long-term power outages occur. Its focus is on power outages caused by cyber-attacks and on how dependability of urban electricity grids and their ICT infrastructure can be improved to overcome and mitigate these attacks through both social and technical means. Summarizing, IRENE targets to:

- Define technical means of utilizing distributed energy generation, storage and demand flexibility to increase power availability for critical infrastructure.
- Identify security treats and their impacts on the critical infrastructure availability in smart grid.
- Clarify necessary procedures and incentives for multi-stakeholder interactions to allow increased power availability for critical infrastructure.
- Develop tools that help city planners and distribution system operators to rank infrastructure criticality level and guide the planning/deployment of smart grid functions needed to optimize power availability for critical infrastructure.

All these targets were reached through different activities that were conducted within the project. More in detail, i) security threats and their impact were investigated within WP2, ii) procedures and policies for interaction among stakeholders are described by the work performed in WP1, while iii) technical and architectural means of utilizing distributed energy generation were tackled in WP3. Tools development is a responsibility of WP4, of which this deliverable takes part. In WP2-3-4, supporting tools were devised and implemented, aiming to help city planners in their planning activities regarding the Smart Grid. However, these tools were developed to solve specific problems, thus calling for dedicated solutions, interfaces and use cases.

This document, namely the "Open Modelling Framework" deliverable, summarizes all the tools developed within IRENE and devises a strategy and a workflow to integrate them in a unique toolset. The final result is a framework and a methodology to execute it. This has a key relevance for the whole project since it transforms some different disconnected tools in a toolset where each tool is connected to the others. Moreover, this gives a final output that summarizes the results of the single tools, ultimately providing resilience metrics of the grid that are built taking into account all the technical contributions that partners created within IRENE.

1.2 TECHNICAL CONTEXT

The document focuses on two main contributions: i) the integration of the tools within the IRENE open modelling framework by providing a workflow for the consequent usage of such tools, and ii) the validation of such integration, using a shared case study in which we executed the tools according to the workflow we described previously.

1.2.1 Integration

The integration subtask aims at defining an integrated view on the IRENE open modelling framework. In fact, this means that the individual tools are integrated in a unique toolset that supports all the methods and analyses developed in all the WPs of the IRENE project.

The outcome is a framework and a methodology, presented through a workflow and a toolset, which are collaborative giving to the user (i.e., a city planner) a unique vision of the toolset with well-defined inputs and outputs.

1.2.2 Validation of the Integration

The workflow related to the usage of the open modelling framework is finally validated using a sample scenario that involves the well-known IEEE 14 node grid topology (see Section 5.1). Starting from this basic configuration, two scenarios were built. The first one represents a basic configuration of one of the nodes of such grid, while the other represents a possible evolution of the grid where city planners decided to add other renewable data sources. The tools in the toolset are used in the order defined by the workflow finally validating the whole toolset that is presented in Section 3.

1.3 OBJECTIVES AND OUTCOMES

Outcomes specifically tackling IRENE objectives. Project partners developed different tools to support each specific task of the project. Specifically, tools regarding threat identification, risk estimation and proposal of mitigations were developed within WP2 [1], [2] of this project. The architectural description of the smart grid is in in WP3 [5], together with demand-side management techniques that characterize this specific category of power grid called for dedicated tools to balance the distribution of energy also when outages affect the grid. Lastly, the modelling tool developed within WP4 [21] includes stochastic techniques and algorithms that allowed estimating the most critical areas and possible actions to increase the resilience of such grid.

All these tools were developed for specific purposes. However, in this document we present a workflow that proposes a way of using all the tools following a specific methodology. In this way, the user (i.e., a city planner) will be able to take advantage of all the findings of the project finally ob-

taining a resilience evaluation of the investigated grid which takes into account all the outputs and the elaborations performed by the tools which build the IRENE open modelling framework.

Research-related outcomes. Research related outcomes are mostly related to the purpose of the single tools, which offer new solutions to known problems by taking the current state-of-the-art material and extending its functionalities providing new ways to tackle problems related to optimization and security of smart grids. The integration of the tools and the definition of the framework will advance the state of the art as there are few collaborative instruments available for smart cities planner and stakeholders. Further, we provide a process that allows the user to analyse the investigated grid targeting security and load balancing aspects in a unique flow.

1.4 DOCUMENT STRUCTURE

The document is structured as follows. Section 2 summarizes all the inputs of the open modelling framework and defines unified lists in case of inputs shared among different constituent tools. Section 3 defines the tools that were developed within the IRENE project. For each tool, we report the responsible partner, inputs, outputs and a description of its functioning. In Section 4 we define the workflow that integrates all the single tools supporting the open modelling framework, that is finally validated in Section 5 by applying the workflow on two simple grid scenarios based on the IEEE 14 node grid topology.

2 FRAMEWORK INPUTS

In this section, we report the main inputs of the IRENE open modelling framework. The objective here is to clarify which inputs that are required to run all the tools within this framework. This will also allow understanding i) which inputs are shared among different tools, and ii) what is required to make the tools suitable for the identified inputs.

2.1 PORTFOLIO OF GRID CHANGES

The whole IRENE project aims at investigating a grid in which the configuration, the sensors or the actuators can change due to decisions of authorities as city planners or stakeholders. The evolution of the grid can be due to long-term planning, requiring knowledge of experienced city planners. In addition, punctual intervention can be identified to perform efficiency improvements or to fix problems. Therefore, updates can be planned and implemented due to:

- Long-term planning of evolutions, defined by city planners and possibly also in agreement with the relevant stakeholders. City planners as municipality may decide to invest significant amount of money to make the energy distribution more resilient and efficient. Further, city planners may decide to modify governance e.g., opening the energy market to new DNOs or promoting the prosumers (both producer and consumer) model;

- the inclusion of specific mitigation strategies to improve robustness and security in an existing part of the grid;

- the addition or removal of electric components to improve specific metrics related to the grid (e.g., a new direct power line between two buildings, new breaker, redundant hardware to improve fault tolerance).

These categories of changes, also summarized in Table 1, will be expanded in the following of this section. In particular, the columns of Table 1 indicate i) the name of the category of the grid change, ii) the temporal horizon that we take into account when planning these evolutions (long, mid and short term), iii) the technical knowledge needed by the city planners to provide this category of change (low, medium, high), and iv) examples of items belonging to the specific category.

We will explore the differences of the three categories above and the motivations that made them becoming inputs and outputs for the IRENE open modelling framework. We reported this classification to highlight the main kinds of grid changes we consider; obviously, partial overlaps between categories may exist (e.g., the application of a mitigation could be the addition of a new electric line, thus merging the second and the third category of our classification) but do not act as a burden to our approach.

Table 1: Categories of grid changes

Category	Planning Term	Technical Knowledge	Examples

Planned Evolutions	Long / Mid	Low (City Planner)	Decarbonisation, Optimization of costs, (see [4])
Implementation of Mitigation Strategies	Mid / Short	Medium (Security Expert)	Security Assessment and Authorization, Media Protection, Personnel Security (see Annex C of [1] for the complete list)
Specific Topology Update	Short	High (Power Grid and Energy Flow Expert)	Add a power line, adding a breaker, new communication infrastructure (see Table 2 for the complete list)

2.1.1 Planned Evolutions

IRENE is strongly oriented to an evolutionary environment in which several components, strategies or policies can be changed by stakeholders. Consequently, the possible evolutions of a smart grid need to be taken into account as main parameters of the whole open modelling framework.

Some high-level evolution steps and evolutionary features that city planners can take looking at the political context were defined in [4]. Other possible contributions will come from the workshop with stakeholders planned for WP5, where experts will elaborate on possible evolutions of smart grids depending on their knowledge.

2.1.2 Implementation of Mitigation strategies

When security experts look at the infrastructure, they may complain on the security measures that are realized to make the grid robust and tolerant to possible faults or attacks. In particular, within WP2 [1] we investigated a methodology for identifying threats due to cyber-attacks, and therefore we reported a list of mitigations derived by NISTIR security requirements [13] that can be taken into account to avoid or mitigate such identified threats.

The *implementation of mitigations* can result in a change of the topology of the grid e.g., adding a spare power line that can be used if the main one is targeted by attackers that want to damage the spreading of energy through the whole grid.

2.1.3 Specific Topology Updates

Specific Topology updates are changes that are not due to planned high-level evolutions or as the result of the mitigation strategies i.e., the other two inputs. Such *specific topology updates* can be identified depending on different needs. As example, we can imagine a company that requested a direct connection to a power substation, calling for the addition of a new cable that was not due to planned evolutions or implementations of mitigations. The list of considered topology updates is reported in Table 2.

Table 2: Considered Topology Updates

Topology Update	Description and Example
Add Generators	In general, local generators, previously mostly diesel operated ones are added to make critical buildings, e.g., hospital, police, fire station, or data warehouse more resilient to outages. The modification is combined with the installation of breakers to disconnect from the grid and isolate the protected building.
Add Circuit Breaker	Measure is part of adding generators or additional power injection line in order to disconnect the rest of the load (islanding the protected building, or area)
Add Power Line	A main power line disconnection (following a physical, cyber-attack or natural disaster) leads to an overload of the lines downstream. Therefore, redundant power injection to supply those loads is planned in combination with circuit breakers that would disconnect some loads.
Add Controllers	Building, campus or microgrid controllers, together with the communication infrastructure are used to realize smart control strategies
Add Communication Infrastructure	Evolution to smart grid, or microgrid means in general adding building, neighbourhood controllers and the required communication infrastructure, in order to realize automation, metering and control concepts.
Dynamic Reduction of Demand	A method of graceful degradation in case of failure, Demand-Side Management (DSM) works by disconnection of non-critical demand. However, it requires all the equipment mentioned above.

2.2 LIST OF COMPONENTS

The list of components is based on the lists identified in WP2 [1], [2]. Moreover, novel components were identified in the process of the project, to guarantee a specific and realistic architectural description [5], supported by available datasets. The additional components, reported in the table below, consist mainly of commercial building types that allow a more realistic modelling of urban consumption. The detailed characteristics of these buildings are described in [18].

Table 3: Novel Grid Components

Component			
Icon	**Name**	**Code**	**Description**

Component			
Icon	**Name**	**Code**	**Description**
	Secondary Power Substation	SS	Power Substation that has switching, protection and energy transforming utilities used to convert medium to low voltage (0.4 kV). It can connect the power grid to a specific micro-grid through the supervision of a micro-grid controller
	Outpatient Clinic	OC	Clinics for ambulant treatment, includes offices and has similar consumption types: heating, A/C, ventilation, lighting, equipment, etc.
	Supermarket	MKT	Food store has ventilation, lighting, space heating/cooling, ICT (cashier, billing system), and a lot of refrigeration consumption.
	Midrise Apartment Block	AB	3-floors building with 24 apartments, common area, office (US model), common heating/air conditioning.
	Restaurant	RS	Quick service restaurant: consumption includes heating, cooling, ventilation, equipment, lighting-

In particular, we added a distinction among a power substation that transforms high to mid voltage (Primary Power Substation - PS), and a *Secondary Power Substation* (SS), which is able to convert the mid-voltage to low voltages. All the other additions regard buildings, respectively i) an *Outpatient Clinic* (OC), ii) a *Block of Apartments* without smart functionalities (AB), and iii) *Supermarket* (MKT) and *Restaurant* (RS), which can be commonly found in any kind of city.

It is important to remark that these changes of the list of components do not compromise the structure of the list obtained in the WP2 [1], [2] of this project. All the added components, except the substation SS, are specific special buildings (see [1]) and therefore all the threats related to the newly added components were classified in the past deliverables under the "special building" category. Moreover, the description of the components was enriched with architectural details.

The full list of components, with such additional details, is reported in Annex A.

2.3 CONSUMPTION PROFILES

According to the origin of the consumption data, we distinguish between:

- Commercial buildings: the tools related to the architecture and modelling use the energy consumption models from the US Department of Energy (DoE) as reference. The dataset called "*Commercial and Residential Hourly Load Profiles for all TMY3 Locations in the United States*" is found under [19]. Since several consumption components such as cooling, heating, ventilation, ICT etc. are available, new critical and interruptible consumption pro-

files are created. Flexible loads are added according to the configuration and where possible (e.g. cooling) their output is calibrated to fit the profile.

- Residential buildings: the high-level tool uses data from *Elexon Ltd.* for normal household profile (categorized as *Profile Class 1* in the UK, with 24 hours of consumption data [20]).
- Remaining components: secondary power station, power plant, factory, stadium, primary power station, do not have or need associated energy consumption profiles.
- Aggregated data An important feature of this model is the possibility to aggregate the profiles forecast, which is accomplished through the active-aware-based *Ensemble Kalman Filter* (EnKF), first introduced in [15]. EnKF is generally a Monte-Carlo based recursive filter approach for generation of an ensemble of model representations. EnKF is applied in sequential data assimilation and even a few ensemble members have the ability to exhibit large-scale covariance behaviour of a system considered [16]. The EnKF evaluation results from WP3 demonstrate the capability and robustness of EnKF in forecast and matching the energy demand, either in real-time or based on prior knowledge and historical records. For this reason, EnKF allows the convergence of data assimilations, on condition that the ensemble size selected is sufficiently large.

2.4 THREAT LIST

The threat list and the attacker profiles are defined in [1], [2]: starting from the NIST [3] guidelines, we built the IRENE list of 38 threats related to cyber-security that is used both in T2.1 and in T2.2 to define the disaster scenarios [2]. Each threat belongs to a category that is used to classify them depending on their characteristics (e.g., attack conduction, gathering information, accidental and environmental).

2.5 OUTAGE SCENARIOS

The threats that can affect a given grid scenario can be mitigated applying the techniques as presented in Section 2.1.2. Anyway:

- Mitigations may not be able to completely prevent the occurrence of the threat or negate its effects;

- The effectiveness of the identified mitigations may require further investigation. In fact, at this point, the extent they are able to mitigate the adverse effects of a threat is not analysed or known.

For example, suppose that a city has a carbon power plant as unique source of energy. The occurrence of an unexpectedly large flood affecting the power plant may have cascading effects, possibly leading to large outages. This may require further analysis to understand how to deal with such possible threat.

Focusing specifically on outages, we consider having an *outage scenario*, or rather the consequences of the happening of a threat that negatively impact the grid resulting in one or more outages. The expected duration of this outage is related to the specific source threat and grid scenario we are dealing with.

Outage scenarios must be defined by stakeholders, namely Risk Assessment (RA) experts, once the grid scenario is defined. Outage scenarios constitute one of the main dimensions of analysis to evaluate the resilience of the smart grid in presence of such detrimental events.

3 IRENE TOOLS

This Section reports the IRENE tools that will be integrated in a unique workflow. These tools have been already described in D2.1 [1], D2.2 [2], D3.1 [5], and D4.1 [21]. We report a summary here for completeness. Further, for each tool we identify the interfaces (in terms of inputs and outputs) to create the basis for their integration in the toolset which constitutes the open modelling framework.

3.1 EVOLUTIONARY THREAT ANALYSIS

3.1.1 Responsible partner

Responsible partner for this tool is UNIFI.

3.1.2 Threats and Mitigations

The likelihood of success of a cyber-attack to Smart Grid control infrastructures will increase with the massive and incremental deployment of advanced automation and communication technologies relying on standardized protocols. The key issues about dependencies in critical infrastructures were addressed the first time in the United States by [3]. Here a *dependency* is defined as a connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other, e.g., a *Hospital* that depends on the energy provided by a *Carbon Power Plant*.

Within the community of experts in power system security the problems arising from system inter-dependency stressed the need to extend the power system transient analysis with new approaches able to deal with cascading contingency chains [7]. Since no standard methodology for conducting cyber risk analysis of energy control systems is available, in [1], [6] we proposed a methodology for *evolutionary threat analysis* that deals with smart grids. Once threats are identified, the methodology digs into a set of mitigations (see below) to provide a list of them that is suitable to mitigate the effects of the threats that may affect the grid scenario.

The problem of mitigating or mediating the propagation of threats is a topic that is strictly related with Smart Grid security mechanisms; the aim of these techniques is to prepare the grid to avoid or limit the impact/diffusion of a known threat. Some useful contributions are available at the state of the art with different purposes: as example, the authors in [11] show a specific list of mitigation techniques that can be used to respond against Denial of Service (DoS) attacks in power grids, splitting the techniques in network-based and physical-based. A more general approach is described in [12], where the focus is on the propagation of different types of cyber-physical threats: after providing threat taxonomy, the authors link the threat types with some high level guidelines aimed to limit the damage propagation.

3.1.3 The Tool

Figure 1: Overview of the Evolutionary Threat Analysis tool.

The threat analysis in [1] led to the implementation of an evolutionary threat analysis tool in WP4. In fact, the threat identification and analysis framework has been implemented into an integrated tool determining the variation of mitigation strategies and the scenario-based distribution analysis [6]. It makes use of the *Colibri-Java FCA API*[1] to analyse the distribution of threats. The tool takes as input the evolution steps defined in terms of evolutionary features and the mapping between threats and their corresponding required mitigation strategies [1], aiming at providing an actual list of mitigations depending on the current grid scenario, that is obtained by merging the evolution steps with the initial grid scenario.

The analysis is evolutionary, meaning that the actual list of mitigations is obtained starting from the previous result and considering the new evolution step that e.g., is defined by city planner. Each evolution step is composed of a set of evolutionary features (e.g., adding / removing a specific component) that can make the set of threats (and consequently mitigations) bigger or smaller. The tool takes the partial set of mitigations and modifies it considering the changes introduced by the new evolution step.

Inputs.

- Threat List, containing 38 threats to (cyber)security that may arise in smart grid scenarios;
- List of grid components, considering basic (e.g., connections, data cables), electric infra-structure (e.g., power substations), generators (e.g., carbon power plants, wind farms) or services to citizens (e.g., hospitals, offices) elements;
- Grid Changes, which as described in Section 2.1 could be planned evolutions or changes in the topology due to a malfunction or a temporary change to bypass energy using different paths;
- Possible Mitigations, which as described in Section 2.1.2 are a list of high-level techniques to avoid or mitigate an arising cyber-threat (e.g., implementing strict access control policies on a public access point component).

Outputs. Defined as a list of threats and mitigations for the current grid scenario, which is composed by the threats that can arise in such a context and the connected mitigations.

[1] https://code.google.com/archive/p/colibri-java

3.1.4 Further reference

For further information, please refer to:

- WP2 deliverable D2.1 [1]
- WP4 deliverable D4.1 [21]
- [6], which summarizes the description of the motivation and problem, as well as the entire solution.
- Further, analyses on tool usability are planned within WP5 together with partner University of Twente. A paper describing results currently available is submitted.

3.2 BAYESIANFAIR THREAT EVALUATION

3.2.1 Responsible partner

Responsible partner for this tool is QMUL.

3.2.2 Motivation and Description

BayesianFAIR is a module that allows numerical threat assessment based on the states of the four FAIR factors [25], including Contact, Action, Threat capability, and Control Strength. The numerical outputs given by *BayesianFAIR* can help to further rank threats in the same category (e.g. High or Very High), which is an extension from the FAIR framework [25]. This will be helpful to prioritise threats to assign the constraint security resources, especially in cases where many threats are considered in the network. Moreover, *BayesianFAIR* allows the fuzzy inputs, instead of the common fixed enters like Very High, High, Medium, Low, Very Low (VH, H, M, L, VL). For example, inputs can be 40%M - 60%H, compared to the original FAIR module that only accepts fixed states like M or H. Such improvement can provide a flexible solution in cases where there are conflicts in security experts' assessments. *BayesianFAIR* calculations also help to highlight the impact of a single factor on the overall assessment, and from that, help to point out the most influential factor[2] that a system operator should focus on to build effective mitigation plans[3].

3.2.3 The Tool

The *BayesianFAIR* tool provides the numerical output based on the states of the four FAIR factors. In real scenarios, for each threat, we assume that security experts are the ones who give input state for every factor. All the Bayesian parameters are obtained from the FAIR tables as guided in the FAIR model [25] and encoded to the tool. Although the parameters are fixed for this particular im-

[2] The most influential factor (of the four input factors) for a threat is the factor that will decrease this threat's severity the most, given the same improvement on the input's security level [2].

[3] A detailed case study to illustrate that point can be found in [2].

plementation, they can be updated manually if users want to assess based on different FAIR tables. The assessments of the tools are adjusted to always be in-line with the FAIR assessments [2].

Inputs: Stakeholders (i.e., security experts) give assessment for the four factors: Contact (C), Action (A), Threat Capability (TC), and Control Strength (CS). Inputs can be either fixed (similar to the original FAIR) or flexible (fuzzy), for example:

Fixed inputs: [C A TC CS] = [H M L H]

Flexible inputs: [C A TC CS] = [H 40%M-60%H L H]

Outputs: Numerical assessment according to the inputs.

3.2.4 Further reference

For further information, please refer to:

- WP2 deliverable D2.2 [2].
- [22], which explains the method for constructing a Bayesian network that extends FAIR, for obtaining quantitative loss event frequencies results of high granularity, by means of a traceable and repeatable process, even for fuzzy input.
- [23], which proposed the method of distilling the list of all possible threat events in a traceable and repeatable manner, given a set of assumptions about the attackers.

3.3 MICROGRID EVALUATION TOOL

3.3.1 Responsible partner

Responsible partner for this tool is AIT.

3.3.2 Demand Side Management in MicroGrids

Demand Side Management (DSM) in micro-grids with flexible loads, distributed generation (DG) and storage has been addressed previously [7]. However, few works have studied the impact of flexibility information exchange and the DSM effect on the microgrid operation during long lasting outages. Using the classification in [7] we focus on a secondary control centralized architecture, in which the time horizon is from minutes up to hours, i.e. significantly larger than for primary control systems.

The control system covers only the microgrid [8] and consists of the *Microgrid* (MG) controller and a number of *Customer Energy Management Controllers* (CEMS). In contrast to the passive control of distribution grids conceived at planning time, in the current approach controllers use flexibility, demand management and scheduling to cope with changes in the power supply, caused by an outage [8]. The *Model Predictive Control* (MPC) technique [9] is used for the realization of the control loop, meaning that the power consumption (and generation) is predicted for a certain time horizon (e.g. six hours). However, the actuation is performed only for the next period.

The MPC mechanism is combined with a novel exchange of flexibility information. Energy flexibility is defined for assets such as HVAC (*Heating, Ventilation, Air Conditioning),* electric vehicle charging or battery storage. Each CEMS controller aggregates the flexibility of its assets and reports the resulted profile (for the next six hours) together with the planned consumption profile. The latter is the result of an optimization step, taking into consideration local goals, MG set points and constraints from all the local assets.

The MG controller reads the latest flexibility and consumption plans from the CEMS and computes updated set points (six-hour profiles). In case the proposed consumption is too high, it sheds certain demands within their flexibility limits.

3.3.3 The Tool

Inputs. As depicted in Figure 2, the inputs for the microgrid evaluation tool can be classified as:

- Configuration of planned grid scenarios and evolution steps to enhance the microgrid
- Grid components, mostly building types, which are associated with consumption profiles
- Environmental input such as outside temperature, sun irradiation, (day ahead) energy prices
- Characterization of the outage, start time, duration,
- Loads and appliances using a technology library of models for EV charging, PV generation and battery storage, microgrid load limits, local generation, etc.

The tools use certain demand optimization architecture, algorithms and control exchange messages between the MG controller and the building controllers (CEMS). Theoretically, the optimization problem objective and constraints are not unique and subject to modification. The simulation system is implemented in Java.

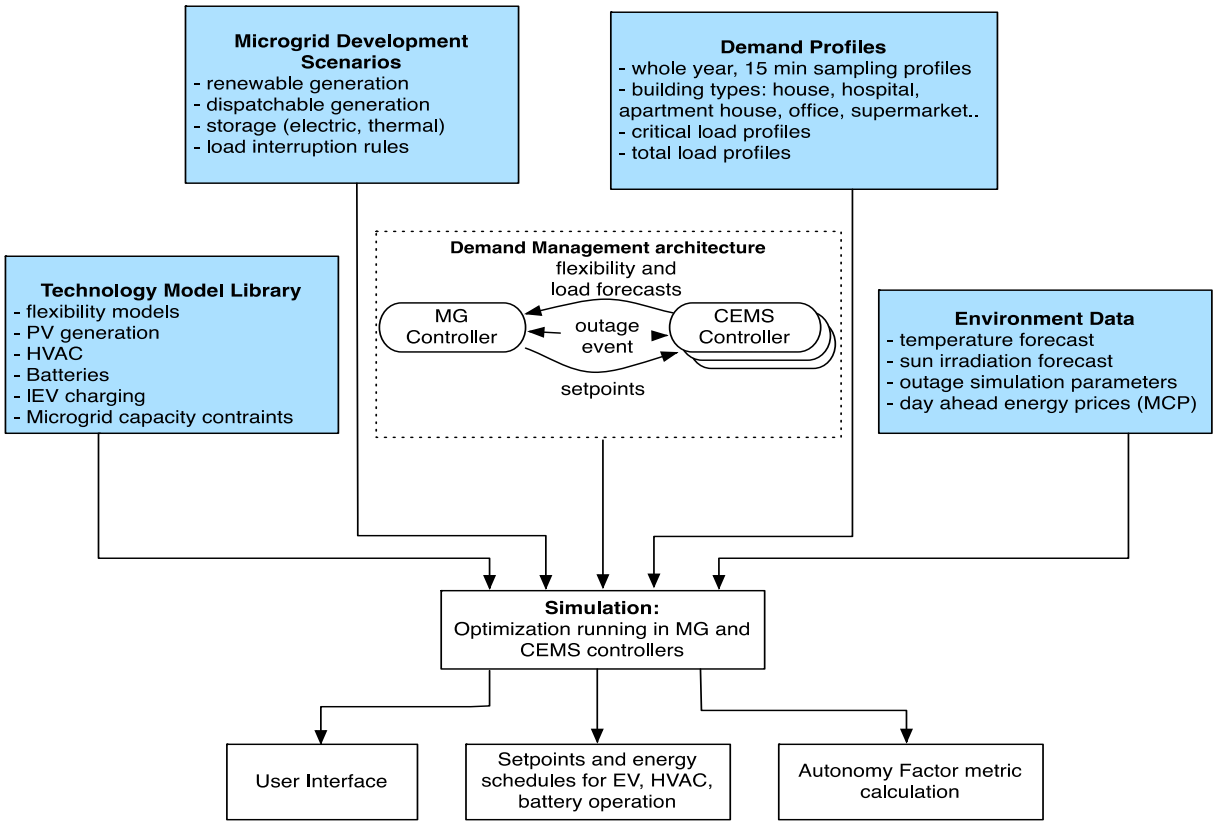

Figure 2: Microgrid planning system overview

Outputs. The runs under different configurations produce the energy schedule prior and during the outage. The local control actions for each CEMS are reported, as well as the efficiency of generation, storage and load shifting. The net consumption of the microgrid can be used for designing appropriate dispatchable generation or, using the total MG load, for outage simulation at the higher grid level.

A user interface shows the variation of power consumption and generation during the simulation (see **Figure 7**). The autonomy factor metric is computed to the energy management performance in a particular grid scenario.

3.3.4 Further reference

For further information, please refer to:

- WP3 deliverable D3.1 [5].

3.4 SINGLE LINE FAILURE SIMULATION TOOL

3.4.1 Responsible partner

Responsible partner for this tool is AIT.

3.4.2 The Tool

We consider a mid-voltage grid topology in which the buses and branches characteristics are known (given). The loads on the buses are also given and they correspond to entire microgrids or low-voltage radial grids that are considered in detail in the MGE tool.

SILFAST analyses the response of the grid to single line (branch) failure. Line failures are frequent consequences of threats that can be either natural disasters (such as fires, floods, earthquakes, storms) or cyber-attacks which could lead to opening line circuit breakers. If a line is disconnected, power distribution takes place via the remaining lines, and since the loads remain the same, an overload situation is created on some of these lines. If not handled by disconnecting loads or adding generation, the lines will trip after some time creating cascading failures and leading to blackout.

The mechanism to determine this overload is to calculate power flows on the topology created by removing one branch and reporting overloaded links.

The microgrid tool described in Section 3.3 provides values for a reduced total load in the microgrid that corresponds to each of the nodes in the higher-level grid (mid voltage).

3.5 OVERALL GRID MODELLING

3.5.1 Responsible partner

Responsible partner for this tool is QMUL.

3.5.2 Description

A comprehensive holistic approach of a supply, demand and load balancing optimization module is developed for grid distribution planning purposes. The optimization model allows the full integration of the demand forecast, wholesale electricity market price, distributed generators (renewable and non-renewable), energy storage systems, and the perturbation of outage events. The demand forecast and assimilation is performed using the active-aware-based *Ensemble Kalman filter* (EnKF). EnKF is a Monte-Carlo based recursive filter approach for generation of an ensemble of model representations. EnKF aims at minimizing the mismatch between the forecast and the ensemble state updates. The outage event is included to evaluate the capability of the grid to sustain the outage by isolation from the main grid and operation in islanded mode, or by isolating grid portions and dropping the load (normal grid-connected operation for unaffected grid nodes). The ability to sustain the islanded operation allows evaluation of the resilience of the urban grid. The developed optimization model acts as the base model for the urban electricity grid. Such model can be adapted to other type of network topology with high flexibility. This means that any kind of real system architecture can be applied to the model to demonstrate the real control/simulation of the urban electricity grid.

3.5.3 The tool

Figure **3** shows the overall grid modelling system. The system starts by defining the components inside the grid, and applying the grid operation state (normal or outage simulation). Once the input settings are accomplished, the optimization algorithm is performed. The output simulation will report on cost of savings based on optimized generation costs and the resilience of the network during the islanded operation. In D4.1 [21] we developed the tool interface that can be manipulated by users is presented as shown in Figure 4.

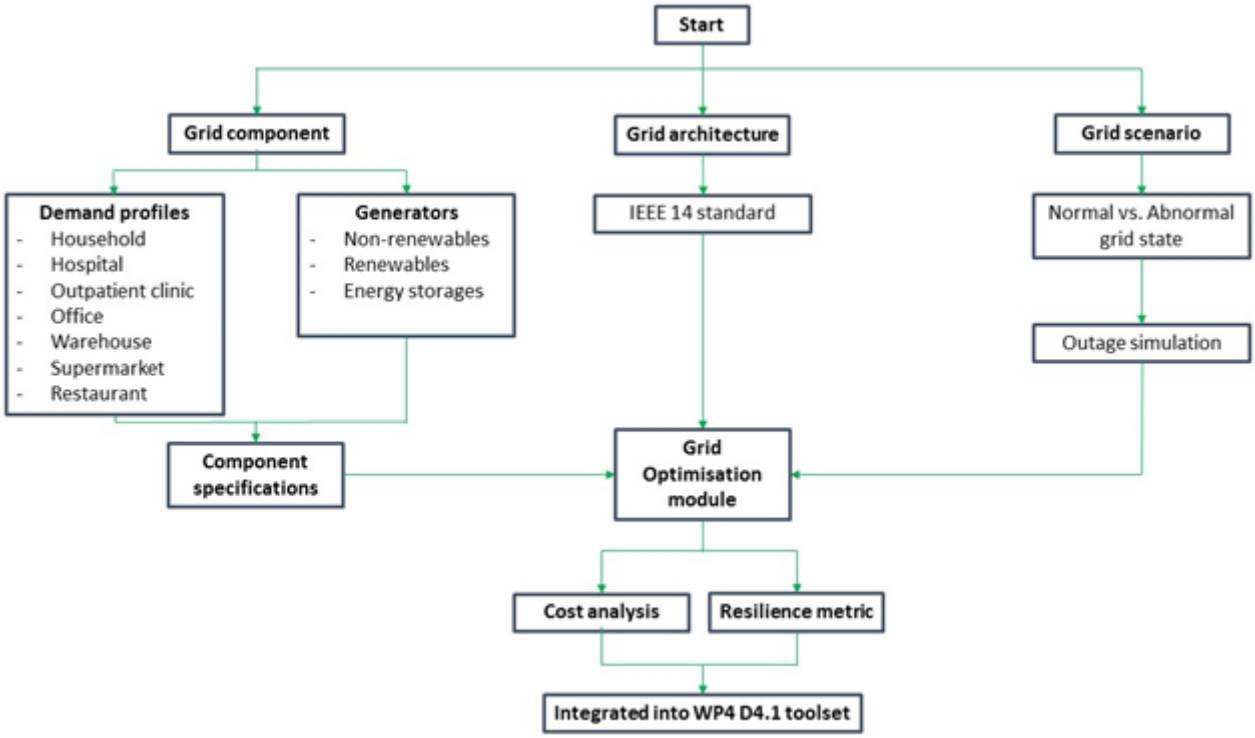

Figure 3: Grid overview

Overall, the optimization module will enable sets of optimal designs and strategies that maximize the economic benefits through the full integration of demand by automatically optimize the load during grid-connected or islanded operation. The optimization problem is typically the economic dispatch in the combination of unit commitment problem comprising the distributed generators and energy storages. Both problems are associated with the amount of electrical power production problems. In responding to contingency analysis, an *N*-1 contingency criterion is considered in the model. The *N*-1 system compliance ensures the grid can survive any single outage in any grid nodes, and the outage of the transmission line between the grid and microgrid.

In order to assess the resiliency of the grid, a performance metric indicator is established. Such a metric presents the extent to which the amount of energy demand within consumers is met when there is a disturbance in the grid [15]. The performance metric to calculate the resiliency is based on the fraction of demand served (or the system performance) and the total magnitude of the demand in the contingency state [15], [16].

The optimization module is performed using the *Matlab* software. The dual-simplex algorithm is applied for *the Linear Programming* (LP) problem of the microgrid optimization. Sensitivity analysis is also performed though the creation of different scenarios in order to evaluate the effectiveness of the grid optimization module.

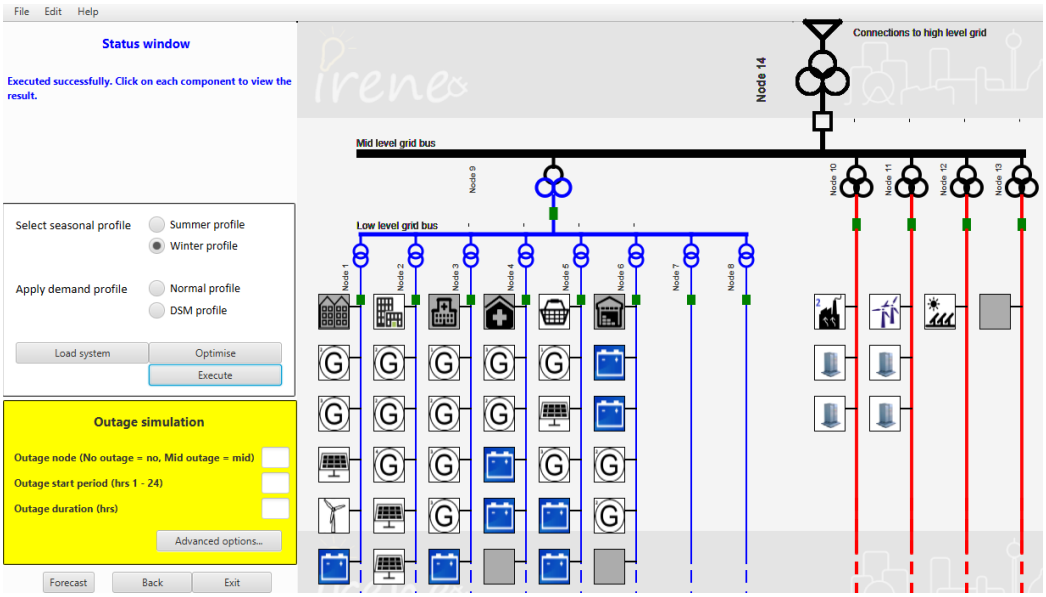

Figure 4: Example of OGM tool interface [21]

Inputs.

- Input demand profiles (e.g., demand profiles for household, hospitals)
- Number of input components/profiles in each node
- Specification of distributed generators (i.e., a default specification of generators)
- Specification of storage systems (i.e., a default specification of generators)
- Number of input profiles, distributed generators and storage systems in each node
- Perturbation of a node for contingency analysis due to the happening of a threat as it is described in an outage scenario, together with the expected duration of such outage
- Number of used-cased scenarios

Outputs.

- Cost of savings based on optimized generation costs
- Resilience of the network during the islanded operation

The next stage involves the implementation of the grid optimization model into a toolset in [21]. Such a model is deployed into a graphical user interface using the Java environment to allow users to manipulate and control the simulation of the toolset as developed based on the grid optimization model.

3.5.4 Further reference

For further information, please refer to:

- WP3 deliverable D3.1 [5].
- WP4 deliverable D4.1 [21], for the technical specifications of the toolset constituting the open modelling framework through methodologies developed in WP3 deliverable D3.1 [5]

4 INTEGRATION PROCESS

The integration between IRENE tools aims at structuring an open modelling framework that can support city planners – or, in general, stakeholders – during their activities. We proceed with the integration with the description of the *workflow*, or rather the flow of information and actions that a planner can follow to fully take advantage of the tools included in the IRENE open modelling framework.

In particular, we describe the flow of information and actions that the IRENE user should follow to use the framework taking full advantage of the findings of the project.

4.1 WORKFLOW ITEMS

The Diagram involves the following items and functions, organized in i) functional to the execution of the workflow, and ii) related to the introduction of the tools into the workflow.

4.1.1 Functional to the workflow

- **Grid *Components List* (CL):** the list of considered components for all the scenarios and the possible grid topologies (see Section 2.2);
- ***Scenario* (S):** a grid scenario defines the involved components defined in CL and relations between them in building a topology. It includes also assumptions and descriptions of the environment;
- ***Grid Change* (GC):** a grid change represents a generic evolution of the grid (see Section 2.1), which could be due to planned evolutions, application of mitigation strategies or generic topology changes;
- ***Threat List (TL):*** the list of the possible threats T that can occur in a generic grid (see Section 2.4);
- ***Current Threats (CT):*** the list of the threats that affect the current grid scenario. The list is composed by threats LT that can be mitigated locally (e.g., enhancing a physical protection on a wire) and others that can cause outages in wide areas of the grid (outage threats - OT) described by the grid scenario;
- ***Threat Severity (SE):*** classification of the severity of a defined threat, defined as a category (very low, low, medium, high, very high). The set of all the severities that were estimated for a set of threats is reported in the diagram as SES.
- ***FAIR parameters (C, A, TC, CS):*** the FAIR inputs for assessing threats, including Contact (C), Action (A), Threat capability (TC), and Control Strength (CS).
- ***Outage Scenario (OS):*** represents a type of outage that can be triggered by the happening of one of the threats in TL (e.g., fire on a carbon power plant can lead to pollution, damaging wires and electric components);
- ***Set of Outage Scenarios (OSS)***: the set of all the possible outage scenarios defined by city planners.
- ***selectOutageScenario: T x* OSS → COS:** This function maps a defined threat with one or more outage scenarios COS that can result from the occurrence of the targeted threat (see Section 10.2.5 of [2] for examples);

- ***Consumption Profiles (CP):*** the set of consumption profiles for all the considered components. This includes the amount of the expected daily energy consumption, and it depends on the targeted season of the year;
- ***Outage Load (OL):*** an outage load is a specific consumption profile that is calculated considering that an outage is affecting a microgrid. Considering the microgrid node *i*, the associated outage load is often labelled as OL_i.
- ***Current Consumption Profiles (CCP):*** the set of consumption profiles for all the components of a given grid scenario;
- ***Grid State (GS)***: is the solution of power flows and load distribution for a defined period, and depends on the components, their configuration and the topology. GS can be normal GS(N) or abnormal GS(A), in which overloads, alarms, power loss, etc. occur;
- ***Resilience Index (RI)***: is the set of metrics calculated for a given grid scenario that quantitatively evaluates the ability of the smart grid to guarantee correct functioning through time, also when outages are affecting the targeted configuration.

4.1.2 Interfaces of the tools

Consequently, the interfaces of the tools are the following:

- **Evolutionary Threat Analysis (ETA):**
  - Summary: taking the current grid scenario and an envisioned grid change, this tool associates threats of TL that can happen when the envisioned change in GC is applied to the scenario mentioned above. In other words, it allows identifying CT due to the planned grid evolution.
  - Interfaces:
    i. $ETA: S \times GC \times TL \rightarrow CT$
- **BayesianFAIR Threat Evaluation (BF):**
  - Summary: the BayesianFAIR Threat Evaluation tool calculates the severity SE of a current threat (CT) based on the four FAIR inputs, namely Contact (C), Action (A), Vulnerability (V), and Control Strength (CS). This is used to rank threats in relation to the grid components in which they can happen.
  - Interfaces:
    i. BF: CT x C x A x V x CS → SE
- **Microgrid Evaluation (MGE):**
  - Summary: the tool has as input a grid scenario (characterization of critical and interruptible demands, storage, PV generation, weather, date and time), and the outage characterization (time and duration of the outage). The result is an upper bound to the total load values during the outage.
  - Interfaces: the consumption profiles (CP), weather, prices, sun irradiance are inputs, the outage scenario OS is external to the microgrid.
    i. MGE: CP x OS → GS(A) x OL
- **SIngle Line FAilure Simulation Tool (SILFAST)**
  - SILFAST employs a mid-voltage grid topology and the outage scenarios (OS) characterized by single line failures. Using the reduced loads OL_i calculated by the MGE tool in every microgrid node i, SILFAST identifies those outages in which the over-

load persists. The result consists of a set of link outages and the corresponding overloaded lines.
    - Interfaces:
        i. SILFAST: S x OS x OL → GS(A)
- **Overall Grid Modelling (OGM):**
    - Summary: the tool simulates a certain grid scenario, including the implemented threat. The calculated grid state shows different disconnected loads and other alarms for outage simulation integrated together with different sets of consumer profiles. Resilience metrics are computed for the grid state and further inferred in terms of the fraction of demand served. This additionally provides the indication of the capability of the grid in sustaining failures and restoring to the normal operating state efficiently. For example, poor resilience metric obtained (possibly the huge deviated loads but with low grid resilience metric computed during the outage) indicates the poor steps/actions adopted in sustaining the required loads.
    - Interfaces:
        i. OGM: S x CP → GS(N) (No RI when no outage simulation is performed)
        ii. OGM: S x CP x OS → GS(A), RI
        iii. OGM: S x CP x OS → GS(N), RI

4.2 WORKFLOW

The open modelling framework includes a toolset that is supported by a workflow, as depicted in Figure 5. Since the diagram is quite complex, we painted with different colours the different phases of the flow.

4.2.1 High-level description of the workflow

We consider as initial step:

- a grid scenario (i.e., the *initial grid scenario*)
- a set of grid changes (from Section 2.1) of such initial grid scenario.

First, we analyse the initial grid scenario through the ETA and the BF tools. We observe all the possible threats that can affect the proper behaviour of the grid. Some of these threats only have a local effect and can be mitigated with local intervention; we call them *local threats*. Other threats can generate outages that impact the whole grid (e.g., an earthquake can damage a power plant leaving the city without energy).

If the city planner decides to implement mitigations only for the local threats (e.g., only local threats are relevant), there is no need for further investigation on the grid and the balancing of components, cascading threats, energy efficiency. Thus, we can restart the workflow and proceed to analyse a different grid change if the GC set is not empty.

Otherwise, if the city planner decides to go further than local threats (note that this is the expected decision), they have the possibility to study the grid response either only using the OGM tool or the MGE and SILFAST tools in combination with the OGM tool.

4.2.2 Detailed description of the workflow

(Blue blocks) Starting from the upper left corner of the figure, the current grid scenario *s* is initialized with the grid scenario *is* given as input. Then, the process can start.

(Orange blocks) We analyse the current grid scenario *s* looking for all the threats that can occur using the *ETA* tool. This provides a set CT of current threats that is composed by local threats (LT), which can be mitigated taking actions affecting the single components, and outage threats OT, that instead can directly lead to outages and cannot simply be mitigated locally. The current threats are next estimated using the *BayesianFAIR* (BF) tool, which applies a probabilistic method to estimate a severity *se* of each threat depending on some inputs that are provided by RA experts. This produces a severity set SES that can be used to link each current threat with its estimated severity.

All the LT threats can be mitigated according to the links between threats and mitigations summarized in [1]. Moreover, the availability of SES can help city planners to choose which threats have to be mitigated earlier. Once LTs are mitigated, the planner can choose to analyse the grid in more detail, considering how the grid reacts when one of the OT actually generates an outage.

(Yellow blocks) In particular, using the set of all the possible outage scenarios OSS we can map each of the OT outage threats to one or more outage scenario COS that the current threat can generate (e.g., a Denial of Service attack targeting a critical node of the grid can let some connected buildings without energy). For each of these outage scenarios *cos* we run the MGE and the OGM tools to evaluate the ability of the grid to react to these detrimental events.

(Green blocks) The green marked steps in Figure 5 deal with the proposal and the evaluation of the response mitigation to an outage. The path to be followed in Figure 5 depends on outage type:

a) *Additional generation approach.* Complete supply failure of a radial grid, i.e. the microgrid, or a generic low-voltage grid is completely cut out from the main grid supply (path on the left).
b) *Reduced Demand Approach.* Supply bottleneck due to specific line failures (path on the right).

In case a), the microgrid under investigation is completely cut out from the main supply grid. This means that the loads of the microgrid can be satisfied only by using internal generation plants and / or energy storages that were previously charged. In this situation, we propose to use only the OGM tool, which is able to suggest an optimized allocation of additional generation plants to avoid anomalous grid states GS(A).

In case b), a single line of the grid failed due to some threats that happened as defined in the selected outage scenario *os*. In this situation, SILFAST provides a check of all link failure situations using the reduced loads provided for each microgrid by the MGE tool. Remaining overloads are identified and they can be removed only with additional local generation. Possible ways to remove the remaining overloads are provided by the OGM tool that, together with the resilience evaluation of the considered grid, can suggest adding local generation in strategic key points of the considered grid.

(Purple Blocks) Once all the outage scenarios that can affect the current scenario *s* are investigated, we proceed to check if some grid changes are provided by the city planner. If he predicts several evolutions for the grid, he builds a non-empty GC set, that triggers a new analysis of the threats and the energy provision considering each grid change *gc* in GC (see purple boxes in Figure 5). If GC is empty, or after examining all the changes in the set, the workflow ends. The result is a grid scenario after consideration of all grid changes and in which all mechanisms to mitigate the identified threats are implemented, guaranteeing energy provision to all the components of the grid according to their requirements also in presence of some outage scenarios due to the occurrence of some threats.

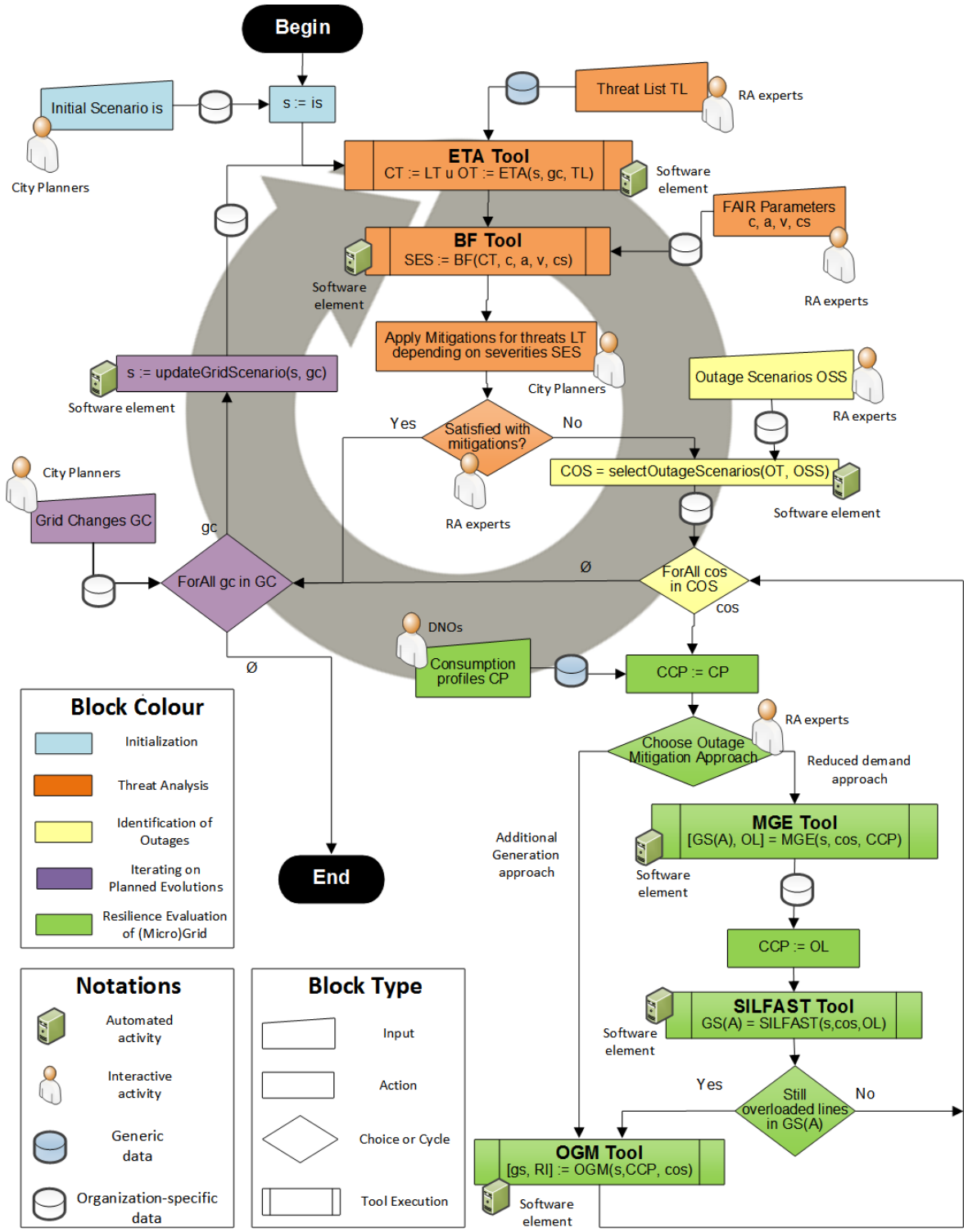

Figure 5: IRENE Workflow

5 VALIDATION OF THE IRENE WORKFLOW

In this section, we evaluate two sample grid scenarios (i.e., the Initial and Decarbonisation scenarios) following the workflow described in Section 4. This provides validation of the integration of all the specific tools developed within each WP, demonstrating how to put the workflow into practice. Our aim here is to validate exclusively the *integration*, showing that the framework can be executed with the adequate synergies between partners according to the workflow. We will not consider issues as realistic initial scenarios or plausible input data, which are instead currently under investigation in WP5.

5.1 DEFINITION OF SCENARIOS

Here we describe the scenarios we used for the validation of the IRENE workflow. More in detail, we report on the reference benchmark grid that is used as baseline to populate some of its nodes by representing different microgrids. Then, general assumptions and information on components are provided. These information are finally used to define "Initial" and "Decarbonisation" scenarios that will be used as reference scenarios for the validation of the workflow.

5.1.1 Benchmark Grid

Within the IRENE project [5] it has been decided to use a known test grid network, the IEEE 14 node grid, which is depicted in Figure 6.

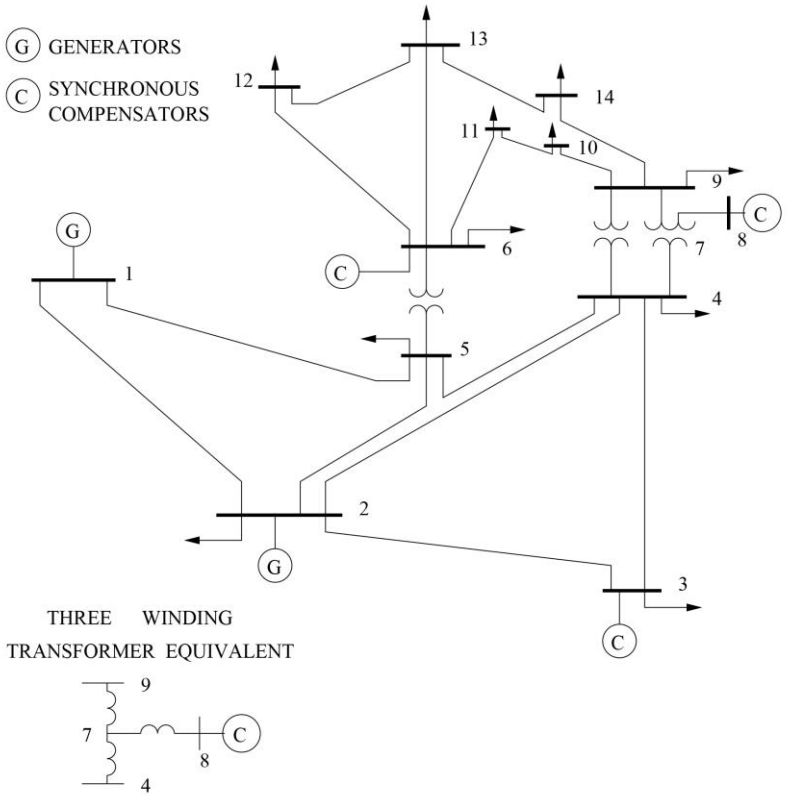

Figure 6: Topology of the IEEE 14 node grid

The IEEE 14 node grid representing the IRENE's grid topology is applied to examine the overall operation of grid during the normal and islanded mode of operation. Each bus number in the figure represents a different micro-grid, which is the target topology of most of the tools developed within the IRENE project. To start, we have built the generation and load distributions of each of the micro-grids involved in the IEEE 14 node grid

5.1.2 General Assumptions

Since the original grid capacity is 230 MW, we scaled it down and populated the microgrids. We assume that the nominal voltage of each bus is 2kV (i.e., a secondary station transformer 2/0.4 kV). Moreover, it is assumed that only Node 2, Node 3, Node 4 and Node 9 are able to reduce their loads during an outage, i.e., the loads of the other nodes in the IEEE 14 node grid are considered static.

Moreover, other assumptions are needed to outline the properties of the whole city under analysis. For instance, the assumptions include i) the city has an important strategic relevance and is consequently exposed to terrorism, and ii) the city is in a seismic zone (see p.70 of D2.2 [2]).

5.1.3 Populating the grid nodes

A node in the IEEE 14 node grid (see Figure 6) is generally modelled as a whole microgrid associated to an urban neighbourhood. For instance, the total load of Node 3 is 940 kW and indicates a microgrid constituted by the following components (see Annex A for component codes):

- CP - 1 charging station (with parking lot for 12 EVs)
- SH - 17 single smart houses
- O - 8 small offices
- AB - 10 apartment blocks without smart functionalities
- MKT - 1 supermarket
- DES - 1 energy storage (i.e., a battery with fixed capacity).

Moreover,

- Node 2 (217kW) consists of 6 smart houses and an outpatient clinic,
- Node 4 (478kW) consists of 4 small offices, 3 apartment blocks and a supermarket,
- Node 9 (295kW) consists of 8 houses, 7 small offices, and 5 apartment blocks.

5.1.4 "Initial" Scenario

The topology of the "Initial" scenario follows the definition of Node 3 in the previous section. More in detail, this node represents a microgrid in an urban area, where housing (SH, AB), infrastructures (O, MKT) and smart components (CP, DES) are installed. Other nodes of the grid are populated, providing energy loads that can be used – if needed – to supply the Node 3 microgrid if its primary source of energy fails. DSM techniques can avoid outages by reducing loads and disconnecting

non-critical components, also balancing the loads from operating microgrids to faulty areas of the grid.

5.1.5 "Decarbonisation" Scenario

In this "Decarbonisation" scenario, the distribution and configuration of DGs and storage remain unchanged. Instead, an additional renewable source (see Unit R2 in Table 4) is added to the microgrids in Node 3, Node 4 and Node 9 of the IEEE 14 node grid.

Table 4: Characteristics of renewable generation for Decarbonisation scenario

Unit	Generation Cost (£/MWh)	Units installed (buses)	Minimum capacity (kW)	Maximum capacity (MW)
R1	80	3, 4, 9	0	0.5
R2	120	3, 4, 9	0	0.5

5.1.6 Considered Outage Scenario

After a preliminary analysis using the ETA tool on the "Initial" and "Decarbonisation" scenarios, we observe that a threat due to possible earthquake (i.e., IRENE threat 33 [1]) damaging Node 3 of the grid (i.e., the "Energy storage" component DES) affects both scenarios. To clarify the validation process, we will consider the earthquake threat in both "Initial" and "Decarbonisation" scenarios.

5.2 INVESTIGATING "INITIAL" SCENARIO

5.2.1 Threat Analysis

According to the workflow, the first part of the methodology aims at estimating the exposure to threats of the grid scenario that is under investigation.

ETA Tool. As for the other tools, we targeted Node 3 of the grid as it is described in Section 5.2.2. For the sake of simplicity, we considered Node 3 microgrid without repeated components. This resulted in a simplified scenario with 6 buildings (i.e., DES, CP, AB, MKT, O, SH) that is therefore analysed using the ETA tool. We lastly remark that considering multiple copies of the same buildings would lead to identify multiple instances of the same threats. Therefore, the threat analysis on the simplified topology will not leave any threat out from the results.

First, we run the ETA tool, obtaining the results reported in Table 5 and Table 6. We highlight that the 11 components building the "Initial" scenario configuration are exposed to a sum of 251 (i.e., 172 structural and 79 emerging) possible threats, roughly 69% structural and 31% that emerge from the interconnections and the relations among different components.

Table 5: ETA Summary for the "Initial" Scenario

Components			Structural Threats			Emerging Threats			Threat Stats (%)			
Buildings	Connections	Tot	Tot	+	-	Tot	+	-	Structural	Emerging	+	-

6	5	11	172	172	0	79	79	0	68.52	31.48	100.00	0.00

Looking in detail at the identified threats (see Table 6), we point out that 37 out of the 38 IRENE threats [1] can occur in Node 3: 14 of these 37 types of threat can also emerge from the interconnection of previously disconnected components. In particular, we can observe how the IRENE threat 20 "Conduct cyber-physical attacks on organizational facilities, session hijacking or brute force attempts" and the IRENE threat 31 "Incorrect Privilege Settings" emerge in the higher number of cases in this scenario. For example, cyber-physical attacks can be conducted from a smart home to the offices through the data line that is used by employees to log on organizational services using unsafe connections. Looking at the last column of Table 6, we can observe how each of the 37 threats occurs on average in 6.46 different parts of the grid (e.g., on average 6 components of the grid are exposed to DoS or MiM attacks), with a standard deviation of 3.35. Moreover, on each of the 172 identified threats, 2.89 ± 1.39 high-level mitigation strategies (see Section 2.1.2) can be implemented to reduce its impact or avoid its happening.

Table 6: ETA Detail for the "Initial" Scenario

	Structural	**Emerging**	**Total**
Threat Types	35	14	37
Most Frequent Threat	(IRENE 3) Perform reconnaissance and surveillance of targeted organizations	(IRENE 20) Conduct cyber-physical attacks on organizational facilities, session hijacking or brute force attempts.	(IRENE 20) Conduct cyber-physical attacks on organizational facilities, session hijacking or brute force attempts.
	(IRENE 19) Conduct physical attacks on organizational facilities.	(IRENE 31) Incorrect privilege settings	(IRENE 19) Conduct physical attacks on organizational facilities.
Occurrences	(Avg) 4.71 (Std) 2.30	(Avg) 4.93 (Std) 2.91	(Avg) 6.46 (Std) 3.35
Mitigations	(Avg) 2.91 (Std) 1.42	(Avg) 3.20 (Std) 1.01	(Avg) 2.89 (Std) 1.39

BF Tool. The scenario describes a grid in a seismic zone. Consequently, the frequency of the happening of an earthquake is *High.* In this case, the first input state of the FAIR factor (C) is *High* and is the same for all rows in the grid components. However, the remaining input states are different for grid components, dependant on the structure and resistance within the grid components to the disaster. Different grid components will have different configurations of the FAIR factors (e.g. houses with low-disaster-proof structures, offices with advanced-resistant structure, installation of backup generations, depending on the frequency and the severity of such disaster may cause). After several SE values for different components (and for different threats, if needed) are computed, these values can be compared to each other. The goal of this step is to relate individual threat-component relations to each other. This can help in prioritizing how to spend limited resources to improve

some controls. Table 7 shows the numerical results of traditional FAIR, SE through BayesianFAIR, and the overall ranking of SE.

Table 7: Numerical results of BayesFAIR and FAIR method on some components.

Component	Input state	FAIR	BayesFAIR (SE)	Rank (overall)
SH	[H,H,H,M]	VH	842	4
AB	[H,H,M,M]	VH	835	5
O	[H,VH,H,M]	VH	863	2
MKT	[H,M,L,VL]	VH	825	6
OC	[H,VH,VH,M]	VH	865	1
PVG on SH	[H,L,M,H]	M	656	9
PP	[H,H,VH,M]	M	844	3
DES	[H,L,VL,M]	M	583	10
PVG	[H,M,M,M]	H	757	7
WF	[H,M,M,H]	H	754	8

Based on Table 7, the Outpatient Clinic (OC) has the highest SE due to *High* probability of large scale damages (i.e., power failure of the connected power lines to Outpatient clinic), and the Low resistance to the damages from the disaster (with Earthquake-resistance structure but no installation of backup-generations). Henceforth, such SE value informs the city planner that actions need to be taken in order to reduce the SE level of Outpatient clinics, e.g., installing backup-generation to supply the emergency power during the earthquake. Since the *Medium* SE values are obtained for DGs and battery storages, they are suitable for implementation as backup-generation for Outpatient Clinics. With such implementation, the SE value for the Outpatient Clinic can be lowered by increasing the level of resistance to the disaster. The SE for all components can be updated easily if users wish to assess the updated input states.

5.2.2 MicroGrid Evaluation

The earthquake scenario might be seen by the city planners as a situation in which power stations and line cables would be destroyed. The MGE tool would use demand management and determine the reduced total load of each microgrid during the outage, whereas SILFAST tool would check the response to each single line failure.

The $P_{REDUCED}$ column in Table 8 shows the reduced loads obtained after applying the microgrid simulation tool MGE to most relevant nodes (values in bold).

Table 8: Power loads and reduced loads for the initial scenario [kW]

Node	Type	Pgen	Qgen	P_{LOAD}	$P_{REDUCED}$
1	3	2.32	0.0	0.00	0.000
2	2	0.40	0.0	0.217	**0.160**
3	2	0.00	0.0	0.942	**0.550**
4	0	0.00	0.0	0.478	**0.250**
5	0	0.00	0.0	0.076	0.076

6	2	0.00	0.0	0.112	0.112
7	0	0.00	0.0	0.00	0.000
8	2	0.00	0.0	0.00	0.000
9	0	0.00	0.00	0.295	**0.200**
10	0	0.00	0.00	0.090	0.090
11	0	0.00	0.00	0.035	0.035
12	0	0.00	0.00	0.061	0.061
13	0	0.00	0.00	0.135	0.135
14	0	0.00	0.00	0.149	0.149

With this input data, we can apply the SILFAST test. We perform two series of experiments: one in which loads cannot be reduced during the single line failures (i.e., P_{LOAD} values are used), and one where the bus loads use $P_{REDUCED}$ loads during the link failures. Except for the link 1-2 which can support a current larger than 3.5 kA, the other lines were considered overloaded if the current is larger than 2 kA. Results can be observed in Table 9, where the second column represents the SILFAST test with *normal* loads, while the last column represents the SILFAST test executed using the r*educed* loads calculated by the MGE tool. Using the regular loads, roughly half of line failures produce multiple line overloads causing them to trip after some time, ultimately leading to blackout. This adverse effect is mitigated considering reduced loads. In fact, under these loads blackouts can happen only with the failure of two lines: 1-2 and 4-9.

Table 9: SILFAST results on IEEE 14 node grid (see Figure 6)

Failed line	Overloaded lines (regular bus loads) current [kA]	Overloaded lines (at reduced load)
No failure	1-2:3.5	
1-2	1-5: 5.6, 4-5: 2.8, 5-6: 2.1	1-5: 3.5
1-5	1-2:5.4	
2-3	1-5:2.2, 3-4:2.4, 5-6:2.1	
2-4	1-5:2.2, 2-3:2.1	
2-5	1-5:2.2	
3-4	2-3:2.3	
4-5	5-6:2.2	
4-7		
4-9	5-6:2.4	5-6: 2.26
5-6	4-5:2.4	
6-11		
6-12		
6-13		
7-8		
7-9		
9-10		
9-14		
10-11		
12-13		

13-14		

Insights on the microgrid simulation of Node3 using demand management. We report here a simulation regarding a summer day (July 5), therefore considering typical summer usage of grid components. The total consumption for the selected day is shown in Figure 7. Simulating one day requires 1-2 minutes. We see that the rated load 942 kW (Table 8) is hit at the peak evening time.

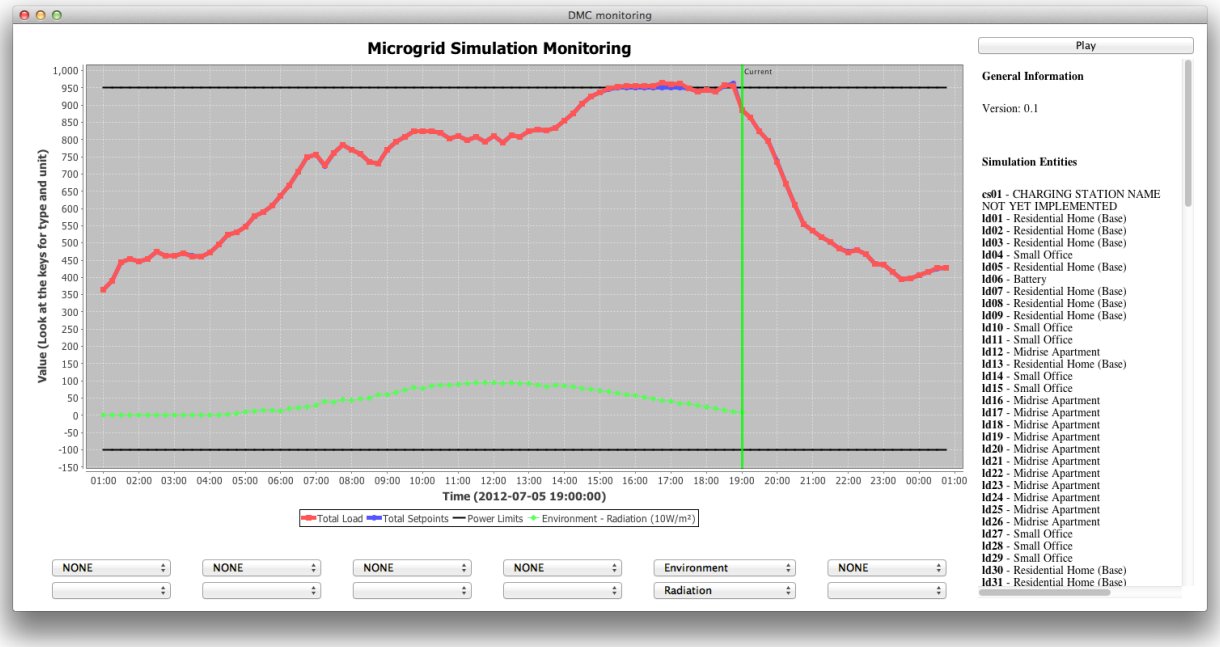

Figure 7: Simulation of the consumption of Node 3, in a baseline situation.

Each component (building) has flexible loads and a model that disconnects in case of outage loads that are not critical. The selected outage of the line 2-3 discussed in the previous section, must alert the microgrid controller that manages the demand of Node 3 (in general the outage should alert all the nodes that may be affected). Once we obtained a baseline model for a node, we can run the outage mode.

Therefore, we rerun the node 3 microgrid simulation defining an outage event between 09:00 and 15:00. As it can be seen in Figure 8, the limit of 500kW imposed for node 3 is quite hard, but 550 kW could be sufficient for such a short outage. Note that the microgrid does not go into islanding mode; instead, it just reduces its demand. Consequently, with the help of the MGE tool we can estimate the demand in case of outage. In Figure 8 we see that the drop of the total demand occurs after one-two 15 minute periods delay. The delay has to do with the demand control cycle time of 15 minutes, which could be theoretically reduced.

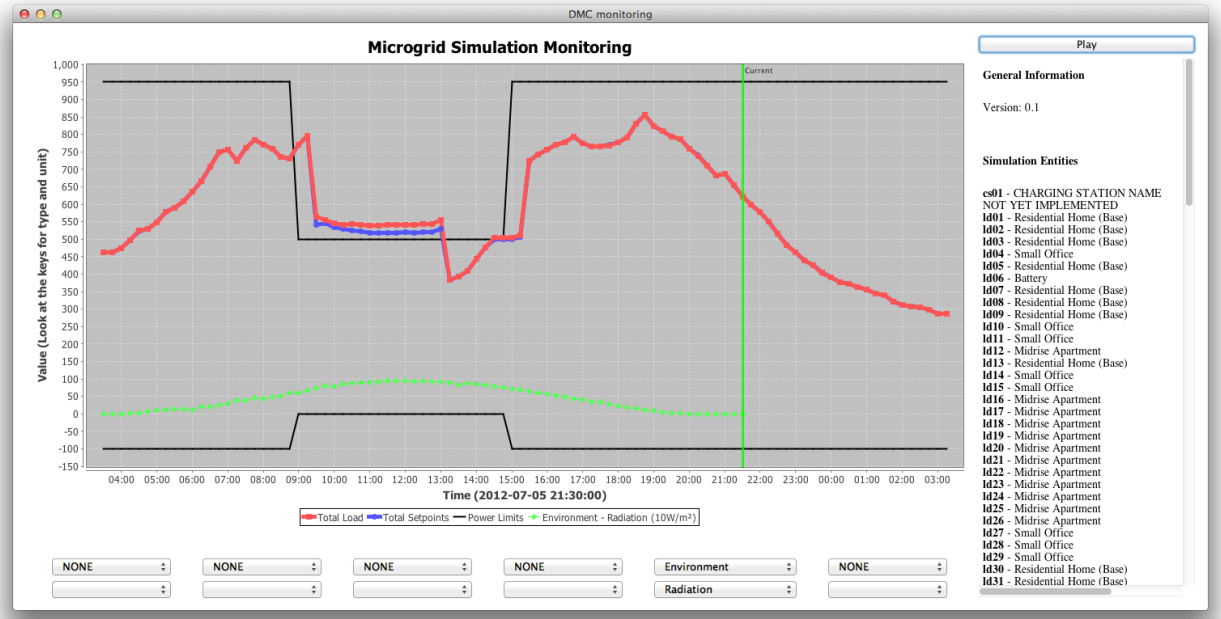

Figure 8: Node 3 simulation with an outage during the hours 09:00-15:00

5.2.3 Grid Resilience

In this case, a complete failure between the main grid and the microgrid level is assumed. Consequently, the microgrid level is isolated from the main grid and the islanding capability for the microgrid level is triggered. The outage scenario describes an earthquake occurring from 09:00 to 15:00. The OGM tool simulates the capability of the islanding operation by optimizing the available DGs and storages to generate electricity during the outage periods. Renewable sources are however not optimized by the OGM tool, due to their uncontrollable fluctuating behaviour. Hence the imbalances in renewable outputs are compensated by DGs and storages. Upon the OGM tool simulation, the required dispatching of DG and storage units are known and the associated cost of operations (with or without savings) during the outage are determined.

The grid consuming components are aggregated and loads are descaled in order to obtain the total demand for the microgrid for individual nodes that are similar with the component specifications as illustrated in Section **Fehler! Verweisquelle konnte nicht gefunden werden.** (i.e., Node 3 ≈ 940 kW, Node 2 ≈ 217 kW, Node 4 ≈ 478 kW, Node 9 ≈ 295 kW). We used three types of DGs and single type of storage and renewable as specified in Table 10. The specifications of DGs, storage and renewable are presented in Table 10, Table 11 and Table 12, while the distribution of DGs, storage and renewable in the IEEE-14 node grid topology are presented in Table 13.

Table 10: Characteristics of DGs

Unit number	Node	Cost of generation	Minimum capacity	Maximum capacity	Startup cost	Shutdown cost

		(£/MWh)	(MW)	(MW)	(£)	(£)
Gen 1	3,2,9	35.1	0	1	20	0
Gen 2	2,4,9	47.1	0	1	20	0
Gen 3	3,4	55.0	0	2	40	0

Unit number	Minimum up time (hours)	Minimum down time (hours)	Ramped up rate (MW/hour)	Ramped down rate (MW/hour)
Gen 1	1	1	0.5	0.5
Gen 2	3	3	0.5	0.5
Gen 3	3	3	1.0	1.0

Table 11: Characteristics of storage

Unit number	Node	Min capacity (MW)	Max capacity (MW)	Charge/discharge rate (MW/hr)
S1	2,3,4,9	0.2	0.8	0.1

Table 12: Characteristics of renewable generation

Unit number	Node	Cost of genera-tion (£/MWh)	Min capacity (kW)	Max capacity (MW)
R1	2,3,4,9	80	0	0.5

Table 13: Distribution of DGs, storages and renewables installed in the network topology

Node	Number of generators			Load (MW)
	Non-renewable	Renewable	Storages	
2	2	0	2	0.24
3	2	1	2	1.00
4	2	1	2	0.50
9	2	1	2	0.30

Figure 9 shows the resultant energy generation distribution and its optimized/balanced generation for during the outage operation. The legends '*Main grid'*, *'Nominal'* and '*Balanced*' in Figure 9 denote respectively: i) the normal generation contributed by mid or high level grid, ii) the expected generation in responding to the total demand without islanding capability, and iii) optimized generation dispatches with the islanding capability from DG, storages and renewables in the microgrid. Due to the complete grid outage, the overall main grid load drops to zero at hours 0900 - 1500. Therefore, the islanded mode operates within the microgrid level during the outage periods, where

the loads are successfully balanced through the optimized dispatching of generating units. As soon as the outage is solved, the islanded operation terminates and instantaneous main grid re-connection is achieved allowing the normal grid operation. In this case, the specifications and installations of DGs, storage and renewables in the IEEE-14 node grid are adequate in responding to the complete outage.

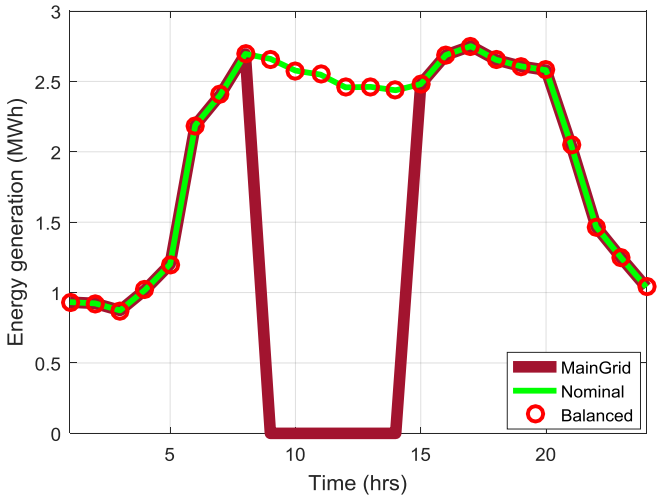

Figure 9: The resultant energy generation distribution and its balanced/optimized generation during a complete grid outage.

The cost of operation for the conventional and optimized grid solution for is illustrated in Figure 10. Marginal cost savings are achieved (£66.54) through the optimized generation dispatches, even though at some instance the dispatching of generation units are more expansive in order to balance the demand during the outage. The overall resilience index RI is based on the demand served during an outage event [5], and is computed as 1.0. The highest RI is expected due to the complete outage mitigation in this case.

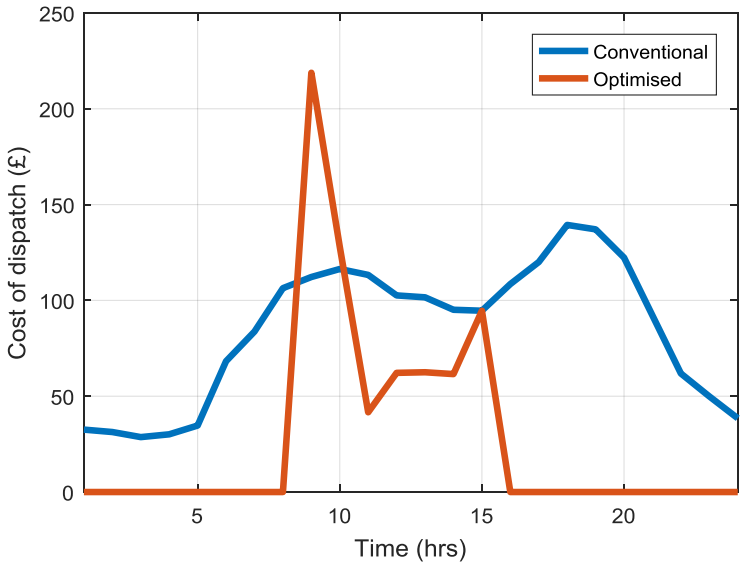

Figure 10: The cost of operation between the conventional and optimized solution during the complete grid outage ("Initial" scenario)

5.3 INVESTIGATING "DECARBONISATION" SCENARIO

Here we focus on the differences introduced by the update of the scenario. Results that are equivalent to the ones listed for the "Initial" scenario are not reported. Instead, we report on the improvements of resilience due to the components that were added in the "Decarbonisation" scenario.

5.3.1 Threat Analysis

ETA Tool. The first step is to analyse the arising threats in the grid scenario "Decarbonisation", which is an evolution of the "Initial" scenario we previously tackled. We also compare this result with the one obtained for the previous scenario. The ETA tool is able to perform an evolutionary threat analysis, meaning that it builds a threat list starting from the results obtained at the previous step. It follows that most of the results are shared with the previous analysis, while some threats are added or removed. As reported in Table 14, in the "Decarbonisation" grid scenario we can find more components and more threats. In particular, the amount of threats grew (totalling 286 threats) due to 35 new threats.

Table 14: ETA Summary for the "Decarbonisation" Scenario

Grid Scenario	Components			Structural Threats			Emerging Threats			Threat Stats (%)			
	Buildings	Connections	Tot	Tot	+	-	Tot	+	-	Structural	Emerging	+	-
Initial Scenario	6	5	11	172	172	0	79	79	0	68.52	31.48	100.00	0.00
Decarbonisation	7	6	13	196	24	0	90	11	0	68.53	31.47	12.23	0.00

With respect to the in-depth results obtained for the "Initial" grid scenario, we obtained that 38 out of the 38 IRENE threats can occur in this grid scenario. Differently from the previous results, in this grid scenario the ETA tool identifies one threat, "*Conduct Man in the Middle attacks*", that occurs in the grid only due to emerging behaviours. This is detected as happening during the communication among different components on a data line, and consequently it cannot be considered as related to a single component.

Overall, as summarized in Table 15, we obtain 38 different types of threats that can impact the grid scenario, with each of them that can occur on average in 7.18 ± 3.90 different parts of the targeted grid scenario. The most frequent threats are the IRENE threats 19 and 20, which call for (cyber)-physical attacks in some part of the grid, and occur respectively in 21 and 18 separate parts of the grid.

Table 15: ETA Detail for the "Decarbonisation" Scenario

	Structural	Emerging	Total
Threat Types	36	14	38
Most Frequent Threat	(IRENE 19) Conduct physical attacks on organizational facilities.	(IRENE 20) Conduct cyber-physical attacks on organizational facilities, session hijacking or brute force attempts.	(IRENE 19) Conduct physical attacks on organizational facilities.
	(IRENE 3) Perform reconnaissance and surveillance of targeted organizations	(IRENE 31) Incorrect privilege settings	(IRENE 20) Conduct cyber-physical attacks on organizational facilities, session hijacking or brute force attempts.
Occurrences	(Avg) 5.25 (Std) 2.86	(Avg) 5.60 (Std) 3.25	(Avg) 7.18 (Std) 3.90
Mitigations	(Avg) 2.94 (Std) 1.41	(Avg) 3.20 (Std) 1.01	(Avg) 2.92 (Std) 1.38

5.3.2 MicroGrid Evaluation

In the "Decarbonisation" scenario, the microgrid simulation can provide valuable information about the resilience increase by adding PV generation, local batteries or flexible charging of EVs. We have studied those effects in [24]. Given the metric α, that describes the degree of energy autonomy during the outage in comparison to normal operation, the results in Table 16 for different scenarios compared to a baseline situation show that, if we add/remove PV generation in some buildings the resilience will increase or decrease. The resilience worsens if the outage duration increases or if the supply during the outage is limited (i.e., 120 kW instead of 200kW). In the case of adding batteries, the results show no impact on the resilience.

Table 16: Impact of system parameters on the autonomy factor.

Scenario	E^n_{in} MWh	E^o_{in} MWh	E^n_{RES} MWh	α
Baseline	4.675	2.46	1.15	0.58
NoPV (offices)	5.11	2.90	0.71	0.50
LessStorage	4.77	2.40	1.04	0.58
6hOutage	1.23	0.55	0.47	0.67
24hOutage-120kW	4.675	2.39	1.15	0.54
6hOutage-120kW	1.23	0.59	0.47	0.65

5.3.3 Grid Resilience

The related outage scenario is studied following the same steps made for "Initial" scenario. In particular, "Decarbonisation" grid scenario promotes the use of additional renewable generations that result fundamental to cope with the outage. Similarly, the imbalance of renewable generation outputs is compensated by DGs and storage.

As a result, by using the OGM tool, the required load during the outage period is successfully compensated by the renewables, DGs and storage. However, as shown in Figure 11, additional costs (£383.09) are charged to operate renewables, DGs and storages through the Decarbonisation strategy in the outage period and no cost savings in this case. Overall, the calculated costs saving should not to be related to the economical operation of dispatchable units during off-peak periods, as the environmental impacts from DGs such as emissions from air particles must take into considerations. The deployment of DGs that affects the severity level of environmental impacts is not covered by the OGM tool.

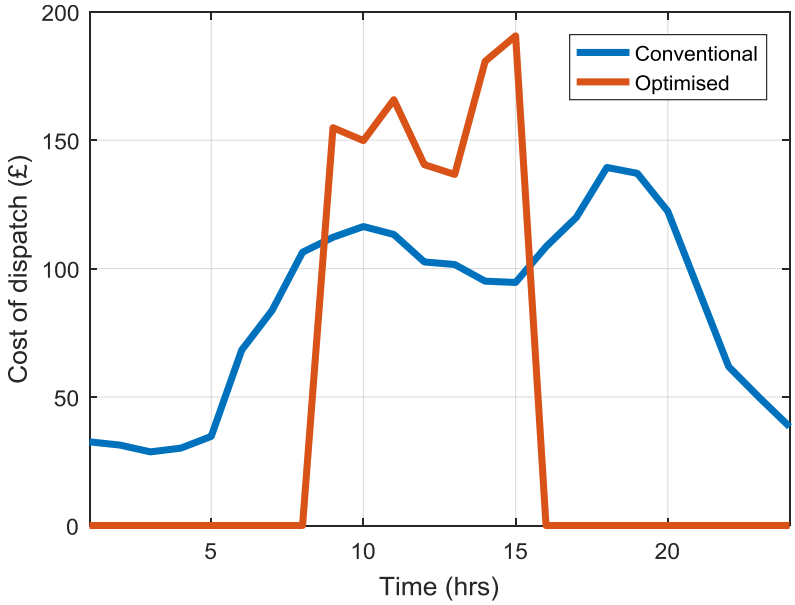

Figure 11: The cost of operation between the conventional and optimized solution during the complete grid outage ("Decarbonisation" scenario)

Similar to the "Initial" scenario, the RI is determined based on the fraction of supplied demand. Therefore, the RI is computed as 1.0 since the demand in the microgrid level is successfully served. The RI in the OGM tool will either increase or decrease if more extreme events are introduced.

Moreover, not all the demands are served due to insufficient generation capacity. Lastly, the RI is also affected by perturbing a line failure/disconnection, for instance, in a particular node, besides the complete grid outage.

6 CONCLUSIONS

This document presents the open modelling framework developed within IRENE. The different elements that constitute the framework have been identified and explored to provide to the user (i.e., the stakeholder) a reliable way to assess the resilience of the targeted smart grid taking into account all the outputs provided by the tools in the open modelling framework.

We summarized all the tools developed within IRENE, with an aim to provide a strategy and workflow to integrate them in a unique framework. This has a key relevance for the whole IRENE project since it transforms some different disconnected tools in a toolset in which each tool is connected to the others. Nevertheless, this gives a final output that summarizes the results of the individual tools, ultimately providing resilience metrics of the grid that are built taking into account all the technical contributions that partners created within IRENE. The toolset and the associated methodology, together with the policies that were defined in WP1, build the open modelling framework that is ultimately able to support stakeholders in their activities.

More in detail, in this deliverable we built the IRENE open modelling framework by subsequently:

- gathering information about the inputs that are needed for the execution of the tools constituting the IRENE toolset;
- summarizing all the tools in the toolset also specifying their interfaces, or rather the expected inputs and outputs;
- proposing a workflow which describes how the tools in the IRENE toolset can interact to ultimately provide the resilience evaluation the stakeholder is looking for;
- executing the tools according to the workflow on a sample grid scenario which is built on the well-known IEEE 14 node grid topology.

Overall, this work together with the policies expanded in WP1 allowed the development of the IRENE open modelling framework. This framework, in association with the collaborative framework described in WP1 and [4], allows the user to address a complete resilience analysis of the targeted smart grid with specific focus on its ability to supply key components during power outages.

Focusing on the scope of the project, the outcome of this deliverable will constitute the base for the evaluation processes that will be investigated in WP5. This is the final step to complete the project by achieving an exhaustive evaluation of the behaviour of the open modelling framework. Use of the open modelling framework is then regulated by the collaborative framework that regulates the interaction among different users of the framework (e.g., generic stakeholders, DNOs, city planners, regulators).

7 REFERENCES

[1] IRENE, D2.1 – Threat Identification and Ranking, 2015

[2] IRENE, D2.2 – Societal impact of attacks and attack motivations, 2016

[3] Grid, NIST Smart. "Guide for Conducting Risk Assessments." NIST Special Publication 800-30, Sep (2012).

[4] IRENE, D1.1 - Smart Grid Scenarios, Collaboration Framework & Requirements (Example Policies, Procedures and Processes), 2015

[5] IRENE, D3.1 – "System architecture design, supply demand model and simulation", 2016

[6] Mori, Marco, et al. "On the impact of emergent properties on SoS security." In proceedings at System-of-Systems Engineering Conference (SoSE 2016).

[7] Lopes, J. A. P., Vasiljevska, J., Ferreira, R., Moreira, C., Madureira, A. (2009). Advanced Architectures and Control Concepts for More Microgrids.

[8] Olivares, D. E., Mehrizi-Sani, A., Etemadi, A. H., Canizares, C., Iravani, R., Kazerani, M., ... , Jimenez-Estevez, G. (2014). Trends in microgrid control. Smart Grid, IEEE Transactions on, 5(4), 1905-1919.

[9] Parisio, A., Rikos, E., & Glielmo, L. (2014). A model predictive control approach to microgrid operation optimization. *Control Systems Technology, IEEE Transactions on*, *22*(5), 1813-1827.

[10] CIGRE, Review of the current status of tools and techniques for risk-based and probabilistic planning in power systems, CIGRE WG C4.601 Technical Brochure n.434, October 2010

[11] Wang, Wenye, and Zhuo Lu. "Cyber security in the Smart Grid: Survey and challenges." Computer Networks 57.5 (2013): 1344-1371.

[12] Neuman, Clifford, and Kymie Tan. "Mediating cyber and physical threat propagation in secure smart grid architectures." Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on. IEEE, 2011.

[13] NIST Smart Grid Interoperability Panel - Cyber Security Working Group, NISTIR 7628 guidelines for Smart Grid cyber security, 2010 http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf [last accessed 15th January 2017]

[14] Cuomo, A. M., et al., Microgrids for critical facility resiliency in New York state, Final report, New York State Energy Research and Development Authority (2014).

[15] Evensen, Geir. "Sequential data assimilation with a nonlinear quasi-geostrophic model using Monte Carlo methods to forecast error statistics." Journal of Geophysical Research: Oceans 99.C5 (1994): 10143-10162.

[16] Johns, Craig J., and Jan Mandel. "A two-stage ensemble Kalman filter for smooth data assimilation." Environmental and Ecological Statistics 15.1 (2008): 101-110.

[17] US Energy Information Adminsitration (EIA), Commercial Building Energy Consumption (CBECS), online: http://www.eia.gov/consumption/commercial/data/2012/index.cfm , last visited: october 2016.

[18] US Department of Energy, Commercial reference Building Models of the National Building Stock, Technical Report NREL/TP-5500-46861, Feb. 2011.

[19] OpenEI, Hourly Consumption of Commercial buildings, online: http://en.openei.org/datasets/files/961/pub/COMMERCIAL_LOAD_DATA_E_PLUS_OUTPUT/USA_IL_Chicago-OHare.Intl.AP.725300_TMY3/

[20] Elexon Ltd, average profiling data per Profile Class (regression data evaluated at 10-year average temperature), Related content, online: https://www.elexon.co.uk/reference/technical-operations/profiling/

[21] IRENE, D4.1 – "Toolsets of supply demand prediction and threat identification and classification", 2016

[22] Le, A., et al. "Assessing loss event frequencies of smart grid cyber threats: Encoding flexibility into FAIR using Bayesian network approach." In proceedings at the first EAI International Conference on

Smart Grid Inspired Future, 2016.
[23] Vasenev, A., A. L. Montoya Morales, A. Ceccarelli, A. Le, and D. Ionita. "Threat navigator: grouping and ranking malicious external threats to current and future urban smart grids." In proceedings at the first EAI International Conference on Smart Grid Inspired Future, 2016.
[24] Bessler, S., Jung, O., Hovie D., Energy Management in Microgrids with Flexible and Interruptible Loads, IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Minneapolis, US, 4-9 Sept. 2016
[25] J. Jones, "An introduction to factor analysis of information risk (fair)," Norwich Journal of Information Assurance, pp. 67, vol. 2, no. 1, 2006.

8 ABBREVIATIONS

Partners	
AIT	Austrian Institute of Technology
ETHOS	EthosVo Ltd
QMUL	Queen Mary University of London
UNIFI	UNIversity of FIrenze
UT	University of Twente
Technical	
SG	Smart Grid
DNO	Distribution Network Operator
NIST(IR)	National Institute of Standards and Technology (Interagency Report)
ICT	Information and Communication Technology
EIA	Energy Information Administration (US)
DG	Distributed Generator
EnKF	*Ensemble Kalman Filter*
FAIR	Factor Analysis of Information Risk
MG	Micro Grid
DSM	Demand Side Management
HVAC	Heating, Ventilation, Air Conditioning
PV	Photo Voltaic
EV	Electric Vehicle
FCA	Formal Component Analysis
(D)DoS	(Distributed) Denial of Service
CEMS	Customer energy management controllers
MPC	Model Predictive Control
Project	
WP	Work Package
IRENE	Improving the RobustnEss of urban city NEtworks (Project Name)
BF	BayesianFAIR Threat Evaluation
OGM	Overall Grid Modelling (Tool)
MGE	MicroGrid Evaluation (Tool)
ETA	Evolutionary Threat Analysis (Tool)
Workflow	
CL	Components List
S	Scenario
TL	Threat List
LT	Local Threats
CT	Current Threats
SE	SEverity of a threat
C	Contact (FAIR Parameter)
A	Action (FAIR Parameter)
V	Vulnerability (FAIR Parameter)

CS	Control Strength (FAIR Parameter)
OT	Outage Threats
GC	Grid Change
OSS	Outage ScenarioS
COS	Current Outage Scenarios
CP	Consumption Profiles
CCP	Current Consumption Profiles
GS(N)[A]	Grid State (Normal)[Anomalous]
RI	Resilience Index

A LIST OF COMPONENTS

Table 17 shows the list of components that is shared among the IRENE tools, and therefore constitutes one of the inputs to the integrated toolset. We reported the name and the code of the components. All the tools within the toolset have a dedicated column in which we put a tick or a cross indicating the compatibility of a given component with the targeted tool. Note that we do not report here the BayesianFAIR tool since it is based on threats and not on components and it is fully compatible with all the threats specified in the IRENE threat list [1].

In particular, the "IRENE toolset" column marks with a tick the rows identifying the components that can be used to model grid scenarios that will be analysed by all the tools developed within the project.

Table 17: Shared list of components

Component		Compatibility with Tools			
Name	**Code**	**Evolutionary Threat Analysis Tool**	**MicroGrid Evaluation Tool**	**Overall Grid Modeling Tool**	**IRENE Toolset**
Connection					
Electricity Connection	EC	✔	✔	✔	✔
Data Connection	DC	✔	✔	✔	✔
Micro Grid Connection	MG	✔	✔	✔	✔
Primary Power Substation	PS	✔	✔	✔	✔
Secondary Power Substation	SS	✔	✔	✔	✔
Circuit Breaker	CB	✔	✔	✔	✔
Long-Range Connector	LRC	✔	✔	✔	✔
Energy Provider					
Power Plant	PP	✔	✘	✔	✔
Photo Voltaic Energy Generator	PVG	✔	✘	✔	✔
Wind Farm	WF	✔	✘	✔	✔
Building					
Factory	F	✔	✘	✘	✘

Stadium	S	✔	✘	✘	✘
Hospital	H	✔	✘	✔	✘
Outpatient Clinic	OC	✔	✔	✔	✔
Office	O	✔	✔	✔	✔
Offices District	OD	✔	✘	✘	✘
Smart Home	SH	✔	✔	✔	✔
Special Building					
Supermarket	MKT	✔	✔	✔	✔
Midrise Apartment Block	AB	✔	✔	✔	✔
Restaurant	RS	✔	✘	✔	✘
Others					
Data / Electricity Storage	DES	✔	✔	✔	✔
EVs Charging Point	CP	✔	✘	✘	✘
Basic Data Centre	BDC	✔	✘	✘	✘