Improving the robustness of urban electricity networks
IRENE

D2.1 – Threats identification and ranking

Document version: 2.0
Document status: Final
Project Document Date: 28/10/2015
Workpackage Contributing to the Project Document: WP2
Dissemination level: confidential
Editor(s): *Andrea Ceccarelli, Tommaso Zoppi (University of Florence)*
Author(s):
Andrea Bondavalli, Andrea Ceccarelli, Marco Mori, Tommaso Zoppi (University of Florence)
Oliver Jung (FTW)
Alexandr Vasenev (University of Twente)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This deliverable is the first report of WP2 “Threat and Risk Analysis”, and it contains a description of the activities performed in Task 2.1 “Threats identification and classification”. The activities here reported investigate threats as cyber-security vulnerabilities, with a particular focus on those threats that result from the interconnection of previously unconnected grid system parts, which is a relevant topic in IRENE. Also the inclusion of new components in the Smart Grids due to its evolution is central to this report and it is considered highly relevant to the scope of the activities here performed and of the IRENE project in general.

The deliverable first reports on the state of the art on threat analysis, considering the main standards and regulatory activity. Then the deliverable presents the scenarios and the reference architectures that are considered for IRENE threat analysis. It should be noted that in the present phase of the project a concrete architecture is not available; moreover, the approach we define is intended to be generic enough to be applied to different implementation of the Smart Gird architecture. Thus, despite the scenarios defined are considered sufficiently generic, these are also mapped to the Smart Gird reference architecture to facilitate contextualization and identify assets and most relevant parts of the grid that are affected.

Further, the deliverable describes the overall methodology that has been devised for the analysis of evolutionary smart cities, where new threats may emerge due to the interconnection of previously unconnected grid parts. It should be noted that methodology maintains compliance to the steps and activities of the NIST 800-30 standard “Guide for Conducting Risk Assessments” which we consider the reference standard for the work done in this task.

The rest of the deliverable reports on the application of such methodology, with the identification of threats, and of possible mitigations (security requirements). To ease the reading of the document, details on the several tables are reported in the annexes and available as an excel file upon request.

The activities here reported started from the scenarios identified in WP1. The identification of relevant threats will allow further refining of the use cases and thus they will support the identification of requirements of the collaborative framework (WP1). Also, the threat list and the identified mitigations (security requirements) here developed is relevant input for the successive activities of the project, in particular for the task 2.2 “Societal impact of attacks and attack motivations “ of WP2, for the identification of the main architectural solutions based on the identified security requirements (WP3), as input to the toolset that implements the collaborative framework (WP4), and for the assessment of the collaborative framework itself (WP5) where different actors are interacting to plan a secure Smart City that is able to react to disaster events that threats may cause.

1 INTRODUCTION

This work builds on outputs of WP1, where a comprehensive description of possible future smart grid energy provision scenarios was performed. The threat analysis process is built starting from the abovementioned conclusions, focusing on the identification and the evaluation of the possible threats that can affect the scenarios.

As described in the DoW for WP2 (Threat and Risk Analysis),

> This WP conducts a holistic (physical and cyber) smart grid (ICT & grid) security analysis to identify
> - system **threats** and their root causes;
> - the impact on the connected components, or constituent systems, especially as to how and where there may be **emergent** behaviour.
>
> This analysis will be used to devise strategies for mitigating malicious, natural, and accidental faults.

and T2.1 (Threats identification and classification),

> This task will investigate threats as cyber-security vulnerabilities that result from the **interconnection** of previously unconnected grid system parts as well as the **inclusion of new sensor and actuator devices** in the Smart Grids. This will use the scenarios identified in WP1 as the start for point for this research.

The aim of this deliverable is to explore and analyse the possible threats that could affect a smart grid scenario (system) according to the requirements of the IRENE project. Particular relevance will be given to threats due to changes and updates of the observed scenario, which are the main additional features we are interested to observe. This is specifically intended to meet the Task 2.1 requirement of exploring the "*interconnection of previously unconnected grid system parts as well as the inclusion of new sensor and actuator devices in the Smart Grids",* from the DoW. Following the threat identification process, as a fundamental part of the analysis, strategies for the mitigation and the facing of the involved threats will be proposed, as a mean to support the managements of the connected consequences. The examination of the root causes and attackers profile will be instead explored in T2.2.

1.1 MOTIVATION OF OUR WORK

The target of this work is to conduct a threat analysis process focused on the identification of threat events that could emerge due to several interactions between grid components. To achieve a better understanding of the motivation of our work, we will first introduce the technical context, including the concept of emergence and the relationships between this property and the main characteristics of the IRENE project.

1.2 TECHNICAL CONTEXT

1.2.1 Emergence

A smart grid can be viewed as a complex system in which different constituent systems (smart meter, DER, Power Plants …) act their role depending on the implemented requirements and the mechanisms. The interaction between these separate components could lead to new macro level behaviours (considering the constituent components belonging to the micro level) which therefore are emerging ones because they are not built-in micro level properties but are generated due to these interactions. In [16] the authors formalize the following definition

> Emergence: A phenomenon of a whole at the macro level is emergent if and only if it is new with respect to the non-relational phenomena of any of its proper parts at the micro level.
>
> Resultant phenomenon: A phenomenon at the macro-level is resultant if it can be reduced to a sum of phenomena at the micro level.

These emerging phenomena can be beneficial or adverse: for example, if we consider a plurality of water molecules under appropriate environmental conditions fluidity and wetness are beneficial concepts while a traffic jam due to the interaction between cars (that are the micro level components) is an example of adverse emergent behaviour. Especially when you are looking for protecting your system from dangerous actions, it is mandatory to predict as best as you can the emerging behaviours with the aim to avoid situations in which some unexpected adverse behaviours compromise the correct execution of the system functionalities [16]. Being this work focused on threats, we focus on detrimental emergence.

For clarity of the following of the work, we also introduce the following definitions [16]:

Evolution: Process of gradual and progressive change or development, resulting from changes in its environment (primary) or in itself (secondary).

Managed evolution: Evolution that is guided and supported to achieve a certain goal.

Dynamicity: The property of an entity that is constantly changing in terms of offered services, built-in structure and interactions with other entities.

1.2.2 Managed evolution and Threat Analysis

Some useful contributions from the state of the art helped us to understand the common methodologies and the general approach to the dynamic system assessment problem, and need to be adapted to the IRENE context, that is centred on the concept of evolution and dynamicity of the smart city and the connected Smart Grid. While obviously the "classical" approach to threat analysis that aims to identify and assess the risks and where possible highlight the mitigation strategies is suitable, some clarifications are first needed.

The scenarios that come from D1.1 [19] follow this idea of evolution: starting from 4 different initial high level contexts (No Change, Constrained Response, Best Endeavours, Freedom To Act), these scenarios are described and realized keeping in mind that the final objective is reaching a future state (described by the "Baseline Model" in D1.1 [19]) in which most of the smart functionalities will be improved.

1.3 OBJECTIVES AND OUTCOMES

Considering the requirements of the task T2.1 and of the IRENE project, it emerges the need to define a methodology that is not focused on the analysis of a static scenario, as it is usually done in practise and in the state of the art, but that assesses the different steps of Smart City evolution.

The following main outcomes are expected from this approach, distinguished in i) outcomes of which the project will directly benefits, and ii) research objectives.

Outcomes specifically tackling IRENE objectives:

- The threat analysis is an input for Task 2.2 and for the continuation of WP1, especially as it allows completing the definition of the use cases.
- The output of the Threat Analysis will identify threats that are related to the evolution of the smart grid, including most likely also emergent threats. This analysis can be easily applied in the remaining of IRENE for the **assessment of the collaboration framework**. In other words, the threats here identified, if proposed as input to the collaboration framework and architectural framework, will allow to observe how the actors (stakeholders, DNOs, city planners, regulators) using the collaboration framework will operate to address them. In particular, emergent threats will most likely require a deeper collaboration of the different actors in order to be predicted and/or mitigated efficiently.
- Modelling different phases of the Smart City/Smart Grid evolution will allow us to distinguish between threats that are due to emergent properties and threats that are inherent to the inclusion of new connections and structures. Understanding the threats connected to non-relational phenomena will **support the definition of requirements** for the solutions for energy prediction and management, as well as **for the methodology** to be implemented in the collaboration framework.

Research-related outcomes:

- Explore the relations between **emergence and (cyber)-security**, in particular related to attacks, trying to investigate if attacks can be considered as emergent phenomena of a system. To the authors' knowledge this has not been explored up to now. The analysis aims to show that the evolution of the Smart City may expose components to attacks that can be classified, **from the point of view of the System of Systems**, as a detrimental emergent property of the SoS.
- Propose threat analysis as a mean to understand emergent properties and/or resultant phenomena related to cyber-security, offering SoS designers information for planning SoS evolution taking into account detrimental emergence. To achieve this objective, as it will appear clear from the text, the appropriate level of granularity is required, in order to reduce the complexity of threat analysis. This granularity needs to consider macro-components and their interactions, always considering the whole grid/city, rather than focusing on protecting the single component newly introduced. Also, this analysis needs to assume that vulnerabilities can be present (despite accurate security countermeasures can be defined for each component) and these can be exploited by attackers to create chains of attacks.
- In common practise, when introducing a new component in a Smart Grid, the threat identification process is generally applied only to that specific component and the

components with direct relations. This is a necessary approach, motivated by the complexity of the Grid. However threats may be provoked by the interactions of all its constituent systems and not merely the additional ones. To this end, we aim at revealing threats appearing only by looking to the whole system (emergent threats) which are new with respect to non-relational phenomena occurring at the level of a single component. In particular we are interested in emergent threats leading to detrimental consequences.

- While emergence is nowadays an hot and debated topic, at present few or no works have tried to identify comprehensively and systematically the detrimental emergence that is part of a system, and especially analysing the "flowering" of detrimental emergent due to evolution. Our approach is a tentative in such direction, with the intention to bring a contribution to describe emergence in complex System of Systems.

At the end of the threat identification process, mitigation strategies will be proposed following suggestions from the state of the art.

1.4 DOCUMENT STRUCTURE

The rest of the document is structured as follows:

- Section 2 surveys the state of the art on threat analysis

- Section 3 contains a library of the threats that will be considered in the rest of the document. This list is derived starting from the standard NIST 800-30 [2] and adapted to the purposes and the granularity of the scenarios considered in IRENE.

- Section 4 debates on the scenarios, further enriching the discussion that was presented in D1.1. This Section introduces the assets, components and their connections that are the target of the threat analysis. This section also maps the scenarios and the threats to a Smart Grid reference architecture and its assets.

- Section 5 presents the methodology and approach for threat analysis.

- Section 6 and Section 7 applies the methodology, identifying the threats for each scenario and defining security requirements that mitigate the different threats.

- Section 8 concludes the deliverable.

- The deliverable further includes a reference section and Annexes that contains details on the threat analysis. These are reported at the end of the document to simplify the reading.

2 STATE OF THE ART

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. Therefore the cyber security of information and communication networks, that constitute the core of the next generation delivery system, represents an emerging research topic as well as a European priority [1]. The key issues about dependencies in critical infrastructures were addressed the first time in the United States by [2], where 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.

2.1 GENERAL OVERVIEW

Since 2004 the Swiss Federal Institute of Technology started to publish an inventory of national and international infrastructure protection policies updated on a bi-annual basis [9]. At governmental level the U.S. Department of Energy stipulated a huge research program specific to a National SCADA Test Bed for the energy sector [10].

Within the community of experts in power system security the problems arising from system interdependency stressed the need to extend the power system transient analysis with new approaches able to deal with cascading contingency chains [11], [14], [15]. The intensive networking at the core of advanced grid control favours the occurrence of cascading phenomena in the power system.

No standard methodology for conducting cyber risk analysis of energy control systems is available, while the IEC and NIST recently published, respectively, a Roadmap [12] and a Guideline document called "Towards the standardisation of cyber security in Smart Grids". The use case typical for future Smart Grids, like the new Distribution Management and Automation Systems for the management of Distributed Energy Resources, the Demand Side Management Systems exploiting the load and production flexibility, the smart charging of Electric Vehicles, are characterised by distributed ICT architectures whose internetworking is based on open communication technologies exposed to a plethora of cyber threats. Therefore the cyber security analysis of their communication flows becomes essential to the development secure ICT architectures integrating appropriate protections to networking risks.

The above mentioned standardization committees are currently working on the development of functional architectures for Smart Grid use cases to be used as a basis for conducting the ICT security analysis. At European level the European Standardisation Organisations (ESOs) in charge of the European Smart Grid Standardization Mandate M/490 EN [13] are currently working to identify the gaps to be filled in order to support the deployment of Smart Grids in Europe. As regards cyber security, the current activities focus on the development of tools for the assignment of impact and risk levels to information assets of Smart Grid use cases, and for the identification of possible gaps in available security standards and guidelines.

2.2 ABOUT SPECIFIC PROJECT FEATURES

As already mentioned, the main goal for this task is to conduct a threat analysis process paying attention on the evolution of the smart grid scenarios. To reach this target, an analysis of the state of the art was conducted in order to understand if existing threat libraries, analysis methodologies or mitigation strategies might be useful in our context.

Some interesting and well-known documents aimed to classify and list the possible threats are available, but each of them focuses the attention on a different aspect of the process. For example, the INTEL [1] paper focuses the attention on the attacker and not on the threats, whiles the NIST [2] one gives more relevance to the threat events. Another NIST document [3], instead, gives some relevant contributions about smart grid security requirements aimed to classify the most important features that such systems must implement in order to reach higher levels of security (see Annex C). This work fits very well with our context because it gives information about mitigation strategies that could help to limit – and where possible, avoid – the effects of the threat events.

Regarding the methodology, the main reference we found is a guide for conducting risk assessment [2] provided by NIST, which lists the main steps that a threat analysis / risk assessment process should follow to comply with the general expected outcomes. In particular, a very interesting suggestion concerns the analysis approach: three ways to perform the process are suggested, each of them fitting better than others depending on the specific context. Other methodology contributions [4], [5] are based on Smart Grid Architecture Model (SGAM, [6]), an high level model structured in zones, domains and interoperability layers that aims to support the smart grid standardization process. This is a quite different point of view with respect to the one described in NIST documents, and seems less fitting that the latter.

Finally, we want to highlight the relevant contributions that we used to define this work:

- Threat library: from an annex of [2], list of threat events that need to be shortened and filtered to adapt it at IRENE context;
- Methodology: [2], following a threat-oriented approach, that allows to start identifying threat sources and events before focusing the attention on the assets that can dynamically added or removed;
- Mitigation strategies: NIST [3] publication, listing smart grid security requirements.

2.3 OVERVIEW OF THREAT ANALYSIS GUIDELINES

Due to the relevance of [2] for our context, it is appropriate to remark the most interesting points reported in that document. The first important contribution regards the analysis approach, which differs from the others with respect to the orientation or starting point of the risk assessment, level of detail in the assessment and how risks due to similar scenarios are treated. Three different possibilities are listed:

- **threat oriented**: starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent;
- **asset/impact-oriented**: starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying threat events that could lead to and/or threat sources that could seek those impacts or consequences;
- **vulnerability-oriented**: starts with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environments in which the systems operate, and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised.

The three approaches investigate the same elements (threat sources and events, vulnerabilities, impacts), but start from different points of view, making each approach more suitable depending on the context.

The main contribution that comes from the same document regards the general guidelines for the risk assessment, helping us to identify the main steps that must be performed, especially respect to the conduction of the assessment:

- **Identify threat sources** that are relevant to organizations;
- **Identify threat events** that could be produced by those sources;
- **Identify vulnerabilities** within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;
- **Determine the likelihood** that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
- **Determine the adverse impacts** to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events);
- **Determine information security** risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

2.4 MITIGATION STRATEGIES

The problem of mitigate or mediate 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 [17] 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 [18], 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 THREATS LIST

The threat library offered by NIST is based on the list reported in Annex E of [2], in which adversarial, structural, natural threat events are described. For each of them, the authors reported the category, the name and an extended description of the threat that is very useful also to understand which mitigation policies might be adopted to limit the adverse effects of each event.

3.1 EVENTS

The list of 102 NIST events needs to be filtered and shortened due to the level of detail, which is in general exceedingly deep wrt the level of details addressed in the identified scenarios. Some distinctions become useless, as example, because they are based on architectural details that are not investigated. Other events, instead, involve some characteristics that are similar to others, considering the selected level of detail.

Considering this observation, we build a threats list significantly shorter that the starting one but adequate to our needs where each event is linked with useful descriptions and references to the NIST corresponding events. The detailed threat list can be found in Annex B.

3.2 CATEGORIES

Another update that was conducted is related to the threat categories: in the reference document [2] the events are splitted into 9 categories, 8 for adversarial events and 1 for non-adversarial ones.

Since the NIST focus is more on adversarial events (only 1 category is about non adversarial ones), we changed the distribution of the categories, reaching a final categorization that is composed from 7 adversarial (ADV) categories and 3 (accidental, structural, environmental) non adversarial (NA) ones. This result is the output of a process aimed to

- a more detailing classification of non-adversarial threats and
- to exclude the adversarial threats that are too specific regarding our scenarios.

The changes with respect to the initial NIST version are highlighted in the table below; further details can be found in Annex A.

Table 1: NIST and IRENE threat event categories

Type	Category	NIST Events	Considered Events
ADV	Perform reconnaissance and gather information	5	3
ADV	Craft or create attack tools	6	1
ADV	Deliver/insert/install malicious capabilities	14	3
ADV	Exploit and compromise	17	7
ADV	Conduct an attack (i.e., direct/coordinate attack tools or activities)	21	8
ADV	Achieve results (i.e., cause adverse impacts, obtain information)	13	3

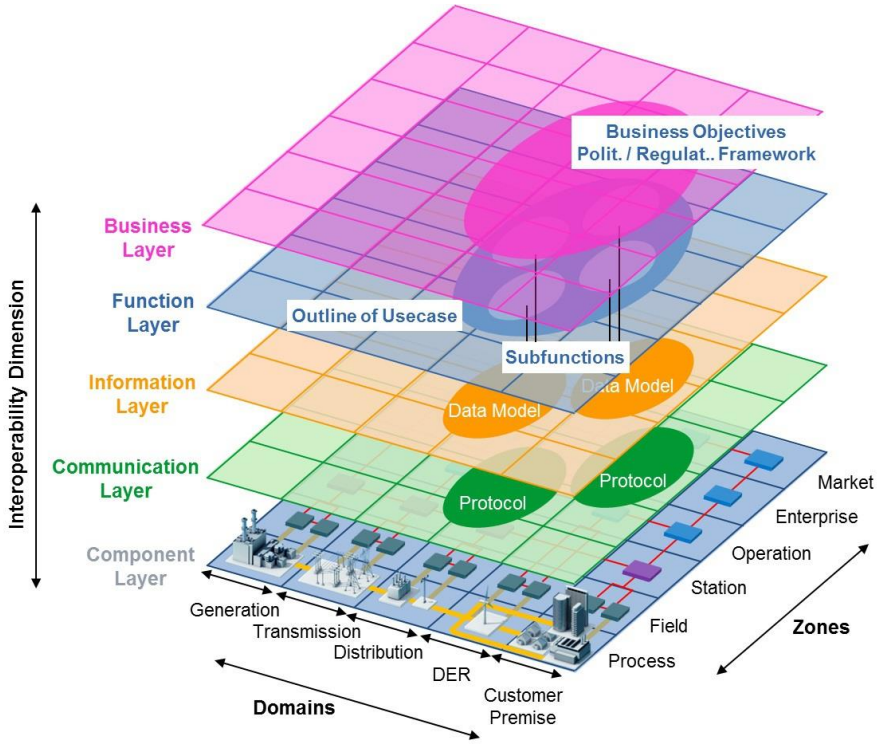
Type	Category	NIST Events	Con-sidered Events
ADV	Coordinate a campaign	6	3
NA	Accidental	4	3
NA	Environmental	9	4
NA	Structural	5	3
-	Other	2	0
	Total	102	38

4 REFERENCE ARCHITECTURE AND SCENARIOS

We described the architecture of the Smart Grid that is at the basis of the IRENE threat analysis. In the present phase of the project a concrete architecture is not available. Moreover, the approach we define in this document is intended to be generic enough to be applied to different implementation of the Smart Gird architecture. Thus, we defined nine different evolutionary scenarios that show how possible future extensions and updates to the electricity grid could look like.

4.1 SMART GRID ARCHITECTURE

The Smart Grid reference architecture is a three dimensional architecture defining layers, domains and zones. Its purpose is to support the design of Smart Grid use cases. The Smart grid plane consists of the representation of power system management by zones and the representation of the electrical grid by domains. The layers represent the different categories where the interoperability between organizational or technical entities should be taken into account.



The domains (Table 2) represent the electrical grid and also show the hierarchical structure of the electricity grid of today. Most of the electric energy is produced by bulk production in large power plants in the generation domain. This energy is transported over long distances using the lines of Transmission System Operators what is represented by the transmission domain. The transmission lines are terminated in primary substations that convert the high voltage used in the transmission grid into medium voltage used in the distribution grid. The distribution domain is responsible for supplying the industrial, commercial and residential customers. The DER domain comprises of components that support distributed generation of energy in the distribution grid. Compared to the generation domain the resources are small and operated by the DSO itself. The end user and its components are placed in the customer premises domain.

In general the components located in the customer premises domain are the ones that are mostly affected by the threats. Due to the sheer number of e.g. smart meters or home gateways it is difficult to protect them. Although smart meters do use cryptography several cases have been reported already where unauthorized access to smart meters was gained [20], [23]. Another problem in this domain is that customers have physical access to the devices what provides them the opportunity to get access.

IRENE is only focusing on the distribution, DER and customer premises domains as these are the ones that can be influenced by cities and where mitigation measures like islanding need to be installed. The distribution gird is however also affected by outages occurring in the transmission grid.

Table 2: Smart Grid Domains [6]

Domain	Description
Bulk Generation	Representing generation of electrical energy in bulk quantities, such as by fossil, nuclear and hydro power plants, off-shore wind farms, large scale solar power plant (i.e. PV, CSP)– typically connected to the transmission system
Transmission	Representing the infrastructure and organization which transports electricity over long distances
Distribution	Representing the infrastructure and organization which distributes electricity to customers
DER	Representing distributed electrical resources directly connected to the public distribution grid, applying small-scale power generation technologies (typically in the range of 3 kW to 10.000 kW). These distributed electrical resources may be directly controlled by DSO
Customer Premises	Hosting both - end users of electricity, also producers of electricity. The premises include industrial, commercial and home facilities (e.g. chemical plants, airports, harbors, shopping centers, homes). Also generation in form of e.g. photovoltaic generation, electric vehicles storage, batteries, micro turbines… are hosted

Similar to the domains also the zones in Table 3 are arranged hierarchically by representing the different levels of power system management. The zones follow a concept of data and spatial aggregation. Each of the zones represents another level of data aggregation from the process zone with numerous sensors and actuators to the operation zone with e.g. few workstations controlling a whole transmission or distribution grid. This is also a spatial separation from meters measuring the consumption relevant in a single residential building to aggregated measurements for a whole district.

More over the zones provide also a functional partitioning. Functions in the station and field zone are usually subject to hard real-time requirements, e.g. for protection, automation, and phasor measurements. Superordinate functions that concern several substations or a city district are located in the operations zone. This includes functions like load management, wide area monitoring, or generation scheduling.

The impact of threats that are targeted to a specific zone can thus be deduced from their spatial responsibility. Attacks on process zone only effect e.g. single building or if substation

equipment is affected a single feeder or district, whereas attacks on operation zone can affect multiple substations and thus whole cities.

Table 3: Smart Grid Zones [6]

Zone	Description
Process	Including the physical, chemical or spatial transformations of energy (electricity, solar, heat, water, wind …) and the physical equipment directly involved. (e.g. generators, transformers, circuit breakers, overhead lines, cables, electrical loads any kind of sensors and actuators which are part or directly connected to the process,…).
Field	Including equipment to protect, control and monitor the process of the power system, e.g. protection relays, bay controller, any kind of intelligent electronic devices which acquire and use process data from the power system.
Station	Representing the areal aggregation level for field level, e.g. for data concentration, functional aggregation, substation automation, local SCADA systems, plant supervision…
Operation	Hosting power system control operation in the respective domain, e.g. distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems.
Enterprise	Includes commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, energy traders …), e.g. asset management, logistics, work force management, staff training, customer relation management, billing and procurement…
Market	Reflecting the market operations possible along the energy conversion chain, e.g. energy trading, mass market, retail market..

This reference architecture is being used to identify the location of the components under threat. As a first step the Smart Gird assets and their location in the reference model is being describes.

4.2 SMART GRID ASSETS

In [20] the Smart Grid assets related to information and communication technology and thus relevant to be considered for information security are identified. In the Market, Enterprise, Operation and Station Zone general purpose equipment is considered as an asset for the smart grid. In the Field zone components specific for the control of electricity networks are predominant while finally in the Process zone non-IT assets have been included as they closely interact with IT assets.

Table 4: Smart Grid Assets [20]

ZONES	**Market**	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Enterprise	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Operation	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Station	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations	Routers, Switches, Firewalls, Servers, Workstations
	Field	RTUs, IEDs	RTUs, IEDs	RTUs, IEDs	RTUs, IEDs	IEDs, Router, Servers, Workstations, Firewalls
	Process	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with RTUs or IEDs at Field level)	Actuators and Sensors (local communication line wired with IEDs or Customer Energy Management Systems at Field level)
		Generation	**Transmission**	**Distribution**	**DER**	**Customer Premises**
		Domains				

4.3 THREAT MAPPING

After identifying the threats that are relevant for smart grids we want to know which parts of the smart grid are affected by these threats.

Numerous threats affect in principle all IRENE assets. However, some of the assets are more exposed then others while the impact of attacks is getting more severe the further it targets assets in the upper layers of the model.

An attacker who is able to exploit vulnerabilities on the upper layers, e.g., a secondary substation would be able to induce an outage in a whole district. But assets residing in the upper layers of the model are on the other hand for several reasons easier to protect [4]:

- there is only a small number components;
- attackers barely have physical access to them;
- they are maintained by well-trained experts;
- security measures on upper layers are not subject to cost pressure.

In contrast there is a higher probability of attacks on the lower layers of the model. Attackers can get more easily access to assets in the field and process zone like data concentrators or Remote Terminal Unites (RTU) or even have full control over the assets as they are located in the customer premises. Attacks on the low layers of the model are expected to have only limited impact on the grid as they geographical region that would be affected is considered to be small. However, if many devices are affected by a publicly known security flaw, the enemies can conduct a large scale attack with the potential to severely impact also the higher layers and span across e.g. a city.

In the Smart Grid most of these assets are connected via IP, in particular in the wide area network communication like between substations, between substations and central controllers, or between data aggregators and equipment in the customer premises like Customer Energy Management Systems (CEMS). In contrast intra-substation communication with tight timing requirements does to use IP. IEC 61850 [22] messages are directly mapped to Ethernet frames that cannot be routed beyond the local Ethernet LAN. This prevents attackers from getting direct access to the intra-substation communication. However, there are points of interconnection between the local LAN and the IP network that could be exploited by attackers.

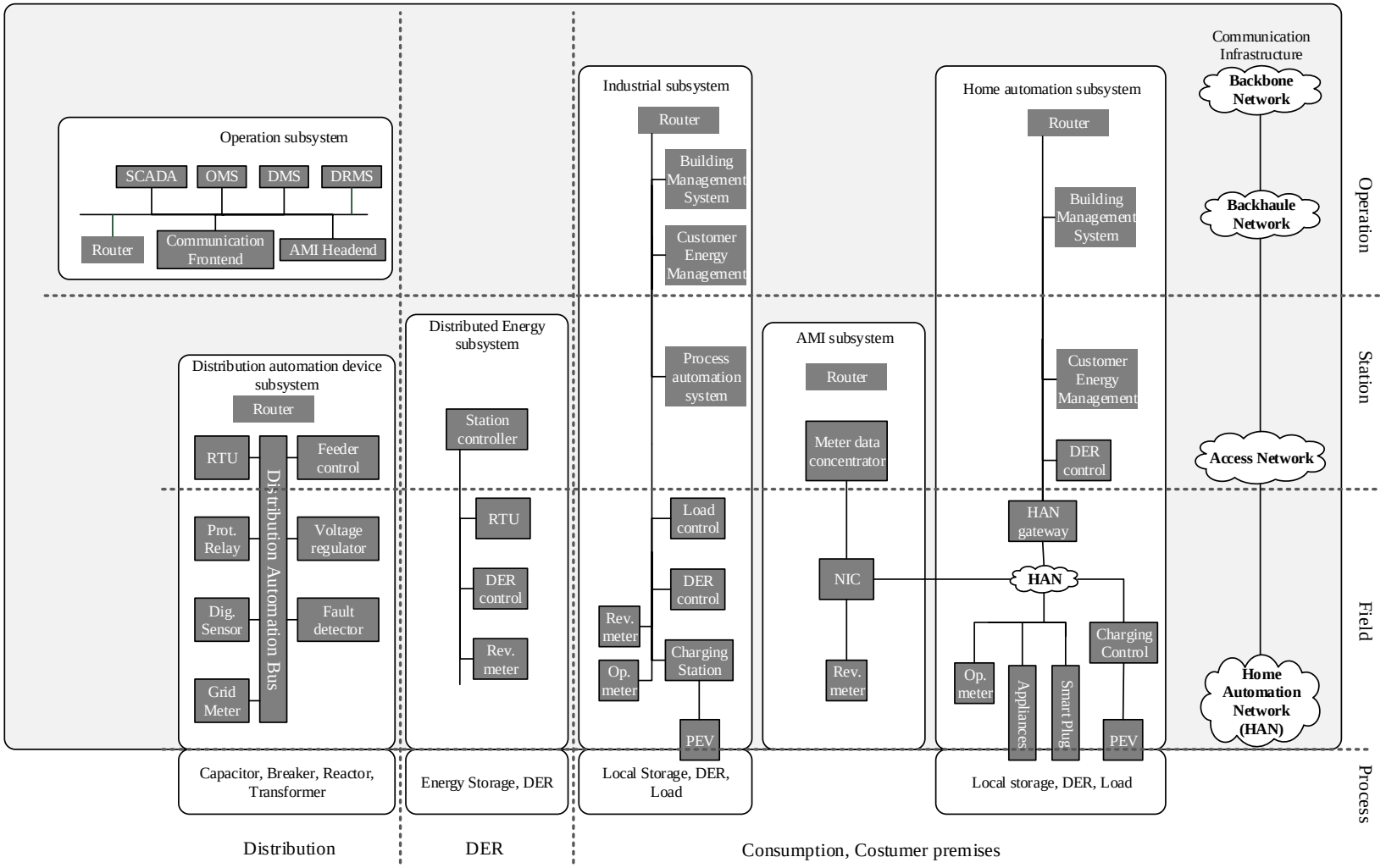


Figure 1: Smart Grid components

4.4 SCENARIOS

The scenarios are mandatory to develop an adequate threat analysis process. To build the following ones, we considered as a primary source the "mapping of smart grid components" depicted in Figure 1, which provides a description of the interactions and the hierarchies between different kinds of components. We also needed to ignore some intermediate components because considering all of them might raise a lot the complexity of the scenario under construction. As described before, for our purpose it is also necessary to take into account the evolution of the structure, trying to define some evolution steps in which the grid described in the scenario could incur.

These features, the involved components and the description of the scenarios are reported below.

4.4.1 Evolutionary features from the baseline model

We report below a brief summary of the evolutionary features already reported in D1.1 (Annex D.1) to facilitate the reader.

1. **Reduce carbon intensity**.
2. **Standardize different types of Smart Grid** in a specific city.
3. Utilization of **Combined Heat and Power (CHP) techniques**.
4. Encouragements to adopt **Electric Vehicles (EVs).**
5. Incentives to citizens, factories and companies to **adopt renewable energy sources**.
6. Utilization of **advanced Metering Tools** (complex Smart Meters, Smartphones, …)
7. **Growing number of citizens**.
8. **Decentralization of the energy production.**
9. **Increasing number of sensors** distributed in a specific or in a wider area.
10. **Changing grid maintaining strategy**.
11. Changes about **data collection and analysis policies**.
12. Incentives to the **electrification of Heating Systems**
13. **Improved Load Balancing strategies.**
14. Adoption of an **Automated Metering Infrastructure (two ways)**.
15. Creating specific **micro-grids** with specific requirements and functionalities.
16. **New energy storage or distribution points.**
17. Adoption of some kind of **protection from natural disasters.**

18. Adoption of some kind of **protection from external attacks.**

19. **Growing support of Internet of Things**

20. New **availability of energy service companies** that want to operate in our city.

21. **Promotion of community projects**.

4.4.2 Components

The scenarios that are the basis of the threat identification process were built according to the outcomes of the T1.1 (especially the contributions in Annex C of D1.1), adding a graphics to the textual description. Here follows the list of the involved components.

Table 5: Considered grid components

Image	Name	Code	Description
Connections			
	Electricity Connection	EC	Represents a simple electricity connection that carries energy in two ways from a component to another.
	Data Connection	DC	Represents a two-way data exchange channel used to send digital data.
	Micro Grid Connection	MG	Micro grid interconnection, that allows to transfer both electric and digital elements with higher performance and reliability power.
	Connection Adapter	CA	Element that can be used to connect parts of the grid that have different connection channels.
	Power Substation	PS	Power Substation that has switching, protection and energy transforming utilities used to convert medium to low voltage. The implementation of circuit breakers gives to this component mechanism to switch lines or to interrupt short circuits or overloads that may occur on the network.
	Long-Range Connector	LRC	Component that indicates connections between far elements at the edges of the connections.
Energy Provider			

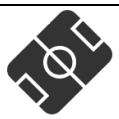
Image	Name	Code	Description
	Power Plant	PP	Represents a power plant that generates energy using the combustion of carbon, not a renewable energy source.
	Photo Voltaic Energy Generator	PVG	Photo Voltaic station in which some panels are connected to a central tower that transforms solar power into electricity.
	Wind Farm	WF	Another renewable energy source that uses the wind power to activate turbines that generate electricity.
Building			
	Factory	F	Building that represents a generic factory, one of the primary energy leechers of the city.
	Stadium	S	A stadium represents an occasional leecher of energy, which can negatively affect the existing load balancing strategies.
	Hospital	H	A hospital carries some security and continuity of energy constraints that needs to be fulfilled in order to guarantee the health of the citizens.
	Offices	O	Representation of a general office in which some energy is requested to the workers.
	Offices District	OD	District of offices requires more energy and dedicated energy providing policies.
	Smart Home	SH	Basic smart home in which we suppose a Smart Meter and some smart components are running.
	Generic Special Building	SB	A special building (e.g. Hotel, Restaurant, Thermal Center …) that have different requirements with respect to a simple smart home: it can be a hotel outside the city that needs of energy to provide its services …
Data Center			

Image	Name	Code	Description
	Basic Data Center	BDC	A simple Data Center that implements mechanisms for data analysis and basic DSR techniques.
	SCADA	SCADA	Supervisory Control And Data Acquisition provides the basic functionality for implementing EMS or DMS, especially provides the communication with the substations to monitor and control the grid
			Others
	Data and Electricity Storage	DES	The generated and not used energy is stored here and remains available for any request coming from the connected components that needs energy. A storage point can also hold come mechanisms and structures for data retention.
	EVs Charging Point	CP	Public charging point in which the citizens can charge their electric vehicles.
	Access Point	AP	An access point that allows the near components to be connected to the data exchange network; it can be used when most of the components in the area don't have direct connections with the data channel.

4.4.3 Categorization of Components

Some of the involved components have similar behaviours, essentially related to their role in the smart grid: for example, some of the energy sources such as Power Plant, Wind Farm, etc. have common requirements – provide energy - and functionalities, in addition to features that characterize the specific role of each component. Components that share some features can share also threat events that can happen due to those common behaviours, so we grouped the components into the basic categories shown in the table below.

Table 6: Categories of considered components

Category name	Category Tag	Description	Components
Connection	CON	Elements that are in charge to carry energy, data or both from a set of components to another	EC, DC, MGC, CA, PS, LRC

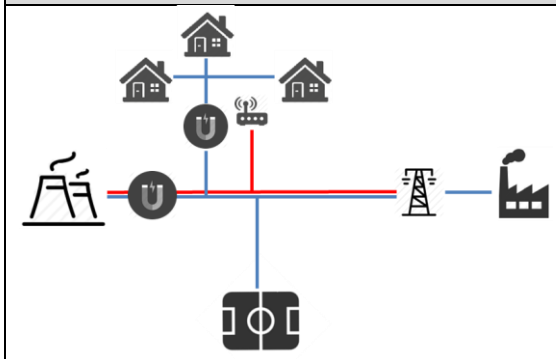
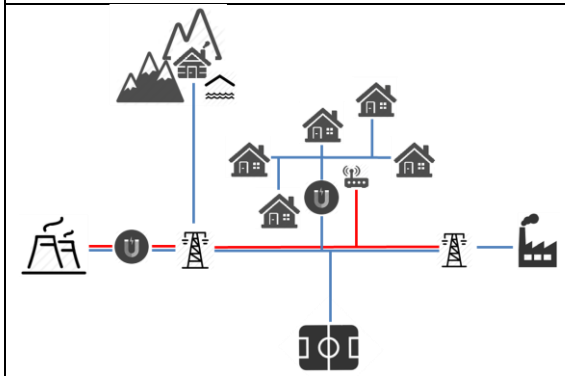
Energy Provider	EP	Buildings that provide energy for the entire grid	PP, WF, PVG
Building	BLD	Represents the city buildings	F, H, S, O, OD, SH, SB
Data Center	DAC	Components that are able to process data to provide useful information to the authorities	BDC, SCADA

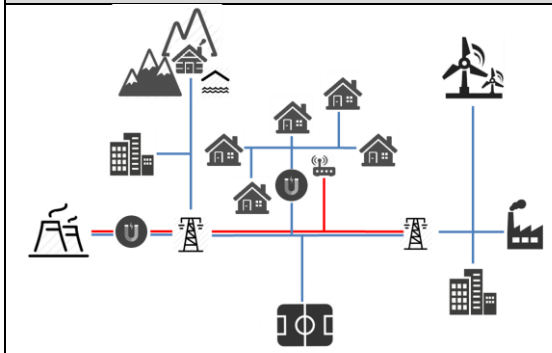
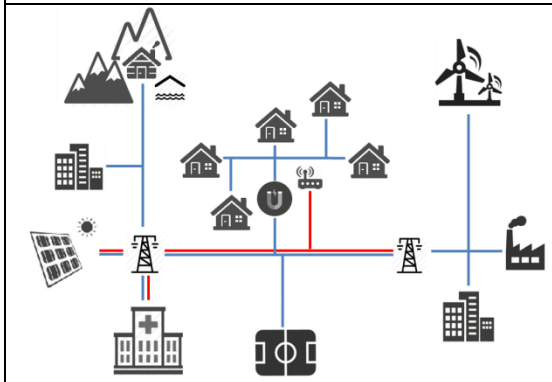
4.4.4 Evolution steps

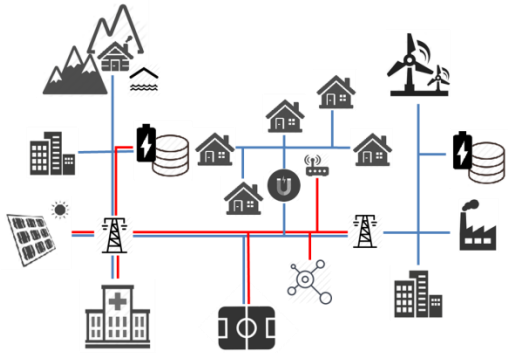
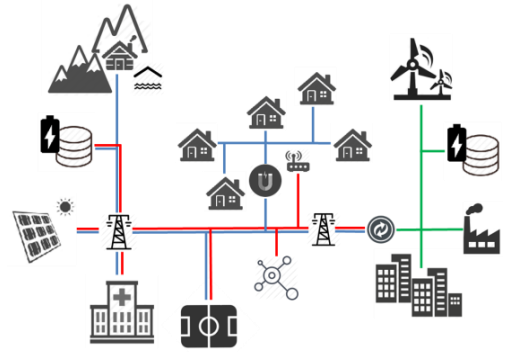
Starting from a simple initial scenario, we tried to imagine the possible changes in which this scenario might incur, using as a basis the evolutionary features described above. The results are in

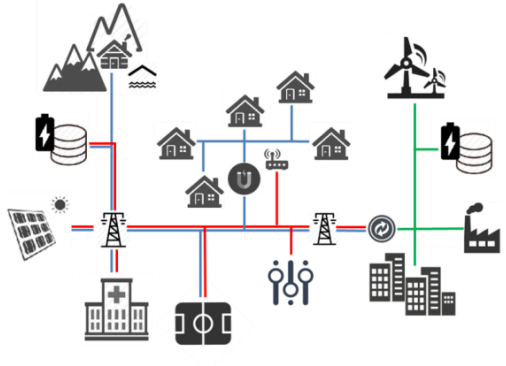
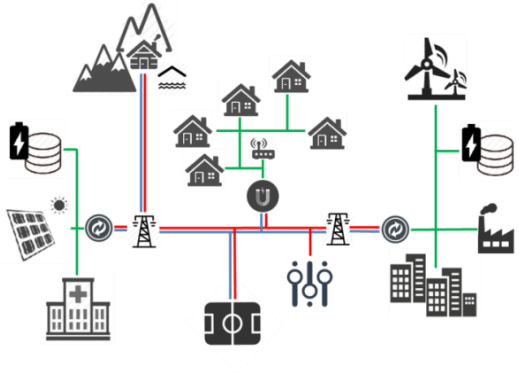
Table 7 where we present the scenario, its description, and an additional discussion on the smart features that are introduced in the Smart City.

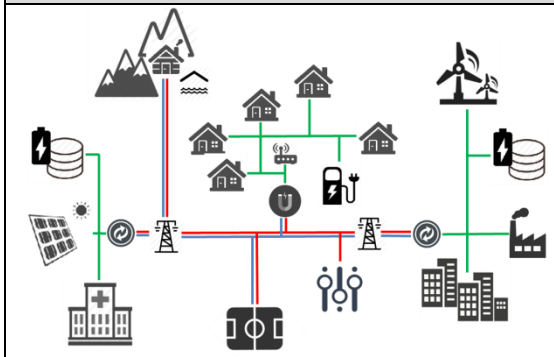
Table 7: Evolutionary Steps

Scenario Representation	Scenario Description	Smart Features
	Name: Initial Scenario Description: Initial grid scenario with a power plant, a factory, a simple residential complex and a stadium. The data connection exists between several buildings but is unused due to the absence of a controller. Two substations are placed in the scenario: one converting from high to medium voltage and another converting from medium to low voltage (used only from the SHs) Evolutionary Features introduced: none	The initial scenario does not provide any Smart Grid functionality.
	Name: Discovering Resources Description: A primary resource is discovered (in this case a thermal source, but it can be a theme park, an harbour, a mine …), resulting in a growing interest directed to the city that encourages the building of new houses and hotels. The richness of city is growing due to the touristic interest Evolutionary Features introduced: 7	The growth in the number of citizens does not imply any changes to the intelligence implemented in the grid. It is expected that only the urban distribution grid is experiencing an extension to supply all consumers (residential, commercial and industrial).

Scenario Representation	Scenario Description	Smart Features
	Name: Growing number of People Description: The growing number of citizens carries the construction of offices to allow the people to work near their new houses. Another energy sources are needed, so taking advantage on incentives to green energy the administration choose to install a wind farm. The smartness of the city remains much undeveloped. Evolutionary Features introduced: 5, 8	The installation of new energy source in the vicinity of a city is a first step to improve the resilience of the city. In case of a failure in the transmission grid parts of the city could be supplied by the wind farm if appropriate measures for managing the resources are foreseen.
	Name: Adding key buildings Description: The city administration is influenced from social needs as for example the request of complete decarbonisation (replacing PP with a PVG renewable energy source) and the building of a new hospital to manage the health of the citizens. Evolutionary Features introduced: 1	Similar to adding new residential building a new hospital is considered as another but critical load that needs to be supplied.

Scenario Representation	Scenario Description	Smart Features
	Name: Inserting Storages Description: This change is mandatory to start the exploiting of smart functionalities. Two data and energy storages are added and a basic data control center is installed to provide simple DSR and load balancing strategies. Evolutionary Features introduced: 9, 11, 14, 16	This is the first step towards the implementation of the Smart Grid. Demand Side Response (DSR) allows the utility to shift peak loads. Electricity demand can be shifted by automating flexible loads. In order to enable demand response functionality appliances in the household need to be controlled. Thus, an AMI subsystem and a home automation system need to be in place. In order to integrate also energy storage into load balancing additionally a Distributed Energy subsystem is required. DER control allows for balancing active and reactive power in the system.
	Name: Building an industrial district Description: Creation of an industrial district with associate micro grid to optimize consumption, load balancing and optimization mechanisms. New sensors are added to the micro grid area. Evolutionary Features introduced: 10, 14, 15	The operation of a micro grid requires also the introduction of micro grid controllers able to control the different energy sources in the micro grid in order to balance supply and demand, control voltage and frequency in the micro grid. The micro grid controller is part of the distribution grid. To make full use of all benefits it interfaces with the DER subsystem and the industrial and the commercial subsystem. The interaction with the industrial/commercial subsystem enables demand side management features such as load shedding in case of congestion.

Scenario Representation	Scenario Description	Smart Features
	Name: Insertion of SCADA System Description: Replace of the Data Center Analysis with a complete SCADA system. The efficiency of load balancing and data analysis techniques is improved and extended to the entire grid with the addition of new sensors. Evolutionary Features introduced: 9, 11, 13, 14	By introducing a SCADA supervisory and control system the whole distribution gird is affected. SCADA enables the control of the distribution grid and the smart features this includes Distribution Automation and Demand Side Management. Simultaneously the threats associated with cyber-attacks on the distribution grid become effective.
	Name: Installing micro grids Description: Adding other micro grids for islanding and quarantining purposes; improving the ability to control smart components from personal devices. Evolutionary Features introduced: 9, 15	The installation of micro grids requires the implementation of micro grid controllers as mentioned earlier. For operating the micro grid as an island additionally Demand Side Management needs to be introduced in order to be able to balance demand and supply.

Scenario Representation	Scenario Description	Smart Features
	Name: Improving Decarbonisation Description: Decarbonisation improved with encouragement to adopt EVs. A public charging point is inserted in the citizen's area. Evolutionary Features introduced: 4, 6, 8	Plug in Electric Vehicles (PEVs) require the installation of a charging infrastructure. Components for vehicle charging are situated in the customer premises domain. Depending on the capacity of the infrastructure it can also be necessary to introduce Demand Side Management for charging vehicles in order to prevent congestion in the grid.

5 METHODOLOGY AND THREAT ANALYSIS APPROACH

As highlighted before, some useful guidelines come from [2], especially regarding the approach to follow and the main steps to perform with the aim to reach a complete and validated risk assessment process. It should be noted that our approach is currently applied for cyber threats, but it would also be applicable for physical threats (intentional damage) or natural disasters. In such case, obviously, an appropriate threats/disaster list should be provided as input.

Since it is very difficult to link a threat event with a quantitative and reasonable evaluation of its impact and likelihood in such generic context, we will talk of threats but we will not weight them (e.g., we will not define the functions of the degree of harm and related likelihood that is assigned to a threat or a risk in general). Consequently, the guidelines must be integrated and extended to tailor these general directions on the IRENE context, which also focus the attention on the dynamicity of the entire grid. Regarding the threat analysis approach, the focus on dynamicity is well-supported by the asset-oriented approach, that is useful to identify threat events depending on critical or updated assets.

The conduction of threat analysis process is therefore based on the NIST references, but with the following changes:

- **Identify threat sources (profiling attackers)**: this activity is scheduled for T2.2 and consequently it is not debated here;
- **Identify threat events**: no change;
- **Identify vulnerabilities:** starting from the analysis of new assets, the vulnerabilities can be obtained from the information about the components that can expose the grid to the identified events: if a component generates threats with high probability, it is a vulnerability point of the system;
- **Determine the adverse impacts**: difficult to evaluate with reasonable precision due to the generality of the context ;
- **Determine information security risks**: as before, this process needs accurate impact and likelihood evaluations.

5.1 METHODOLOGY

The proposed methodology is intended to operate according to changes in the scenario, focusing the attention on the threats that emerge due to the abovementioned updates, which can be insertion or removal of components/functionalities (here the asset oriented approach proposed by NIST [2] becomes useful). Therefore, the investigated scenario needs to be compliant with this methodology, and must be composed by the different descriptions of:

- an initial situation, that summarize the starting point of the city scenario we want to analyse;
- evolution actions that might be taken from the city's administration in order to improve the smartness of the grid or simply to adapt the scenario to newer requirements;

- a target context, that is obtained from the composition of different evolution steps and that represents a sort of expected status of the city in some years from now.

In addition to this, if the scenario and the related evolutionary features are not very specific (e.g. "adding some smart homes" instead of "add *n* smart homes in this specific location with these characteristics"), the outcomes of the process could be used also in different situations in which the same changes are planned, reusing the already performed work with minimal adjustments.

5.1.1 Main Advantages of this Approach

In a nutshell, the main advantages and the novelty of this methodology are the following:

- observing emerging behaviours becomes simpler: when the scenario is updated with a specific evolutionary step, the new connections established between the added and the existing components are easier to identify;
- the generality of the changing of the scenario make the threat analysis outcomes very reusable in other contexts that have common features and consequently it can be used as a reference;
- it is fully compliant to the NIST 800-30 standard;
- the final threat analysis result is the composition of the conclusions drawn in each analysis process related to a single evolution step, so we could change the definition of the steps without changing the methodology that remains valid independently from the specific evolution way we choose for the context.

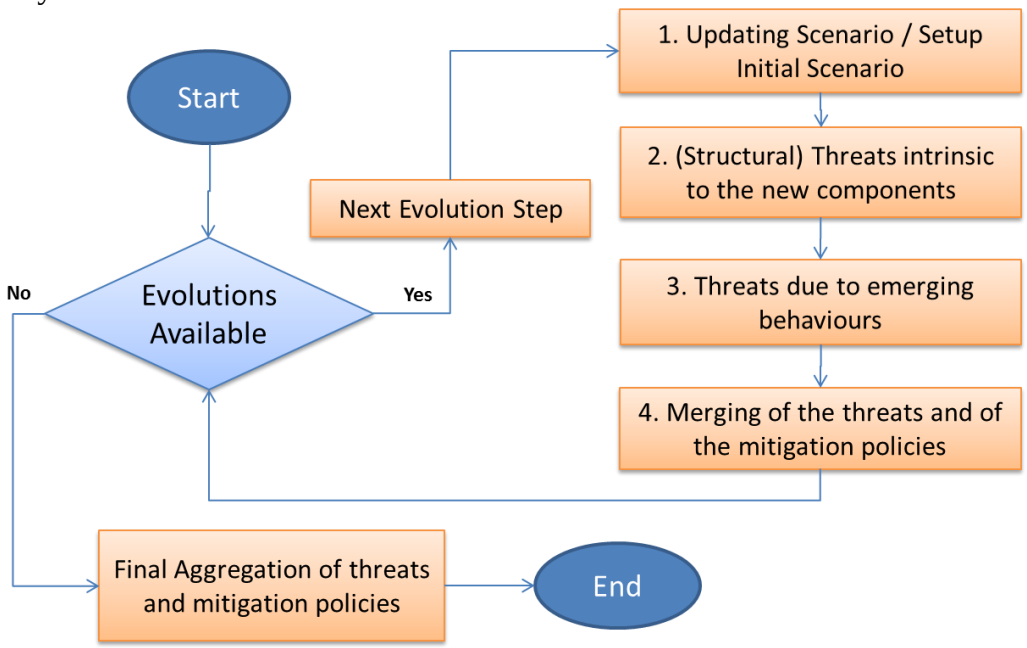


Figure 2: Methodology workflow

5.1.2 Methodology Definition

The methodology is built to perform the same sequence of actions for each evolution steps, including the initial scenario; note that in this case all the components are new (it is the initial scenario). The actions are the following, described also in Figure 2:

1. Evolve the scenario. On the updated scenario we repeat the analysis conducted focusing the attention on the new assets introduced from this evolution (new assets in our examples always results in new components and/or connections).
2. We look to the IRENE threat list to understand if one or more threats are introduced in the scenario with the addition of the new components, without considering the context in which we put that component (threats intrinsic of the components and its interface, referred in this document as "structural" events).
3. Once the structural analysis on the new components and connections is completed, it is mandatory to investigate the interactions established between one newer component and every set of old ones. This process leads us to highlight complex emerging behaviours due to these interactions, which we described in the previous sections as a main target to deepen during the analysis.
4. The results coming both from the structural analysis on new assets and on emerging features are merged and added to the partial results of the process, updating both the threat event list for the scenario and the linked mitigation policies that are directly related to them, as we can see in the following sections.

Once all the evolved scenarios are analysed, all the results coming from each iteration of the process are merged and added to the final list, that contain information about what event is generated from which group of components and if that event is due to emerging or static behaviour.

6 THREAT IDENTIFICATION

Here follows the description of the threat identification process that takes advantage of the structuration of the scenario with different evolution steps. As explained before this approach allows us to understand which are the changes at the threat listing introduced by a specific evolution of the grid scenario, giving a very high relevance to the evolution of the smart grids under investigation.

According to the methodology described in the previous sections, for each of the considered changes of the scenario (point 1 of the methodology) our target is to describe every structural (point 2 of the methodology) or emerging (point 3) threat which is introduced in the grid. The aggregation of these results (point 4), that would lead to the final outcomes of the threat identification process, is not deepened here, but it will be explained in the following sections.

6.1 MORE ABOUT THREAT EVENTS

Some of the events that involve a smart grid are structural (intrinsic of the components), while emerging ones are due to interactions among different components. Both sets need to be investigated to provide a complete analysis about the context, in which these two types of sources can lead to a relevant number of threat events. For example, in a scenario in which a data storage building is installed, you have to be worried about disk errors, which is an error that is not related to the relationships with other components but only to the functionalities of the storage point. As another example, a MiM attack can also be conducted when two or more components share a communication channel, so this threat event is due to multiple entities. Thus, the output of the threat identification process for each scenario can be summarized as

$$Threat\ Event\ Set = Emerging\ Events \cup \bigcup_{\substack{component \in \\ scenario}} Structural\ Component\ Events$$

To facilitate the reader, we put the listing of the structural threat events related to each of the considered components in Annex E, while in the rest of the section we will give a detailed description of the emerging events (due to the interactions between components) in each of the evolution scenarios we considered.

6.2 EMERGING THREATS IN EVOLUTIONARY SCENARIOS

Here follows the detailed analysis of the threat events that can emerge in each scenario depending on the evolutionary features we decide to consider at a specific step. For each evolutionary scenario, we highlighted:

- the main changes with respect to the previous step;
- the list of the events due to the new interactions introduced with the update of the scenario.

6.2.1 Initial Scenario

This is the initial scenario, so all the components are considered as new. The starting point of our analysis represents a small city context with a **power plant**, a **factory**, a **stadium** and some **homes** with a limited set of smart features that are connected to the Internet through a public **access point**.

- ADDED: Power plant (PP), Factory (F), Stadium (S), Smart Homes (SH), Access Point (AP), Power Substation (PS);
- REMOVED: none

Table 8: Emerging threats for "Initial Scenario"

IRENE Index	Involved Components	Description
4	SH, AP	While browsing the Internet from home through the access point, citizens may incur in phishing attacks aimed to steal personal data from the outside of the smart home.
10	AP, PP	Tunnels left opened by citizens can be exploited to conduct any type of attack (to the power plant) through the tunnel
15	SH, AP	Communication between homes and access points may be intercepted by an adversary taking place in the middle of a wireless/cable exchange of data.
21	SH, AP	Communications can be intercepted if an adversary takes place in the middle of a wireless/cable exchange of data between homes and access point
29	SH, AP	Citizens accessing the Internet through an access point may leave critical or sensible information exposed to the network
30	SH, AP	The citizen is usually not aware of security issues so it may leave critical or sensible information exposed to the network
31	S, F	When a match is in progress, a huge amount of energy is requested by the stadium, which competes for the acquisition with the factory. The latter may receive a non-sufficient amount of energy for their purposes.
31	S, SH	When a match is in progress, a huge amount of energy is requested by the stadium, and maybe stolen from other key components. The latter may receive a non-sufficient amount of energy for their purposes.

6.2.2 Discovering Resources

The interest towards the city is growing due to the new discovered resources, so the number of **homes** is growing, but their smartness remains undeveloped. A new **thermal centre** was built just outside the city area and connected to the electric (and not the data) line. The request of electricity grows quickly because of the increasing number of citizens.

- ADDED: Special Building (SB), Smart Homes (SH)
- REMOVED:

Table 9: Emerging threats for "Discovering Resources"

IRENE Index	Involved Components	Description
17	SH, AP	The growing number of citizens that use the access point lead to open more ports, services and protocols that are difficult to control and manage. The adversary, acting from outside the smart home can exploit one of the opened ports.
31	SH, SH	The growing number of citizens can lead to a consequent increasing number of smart homes which compete to get energy resources thus provoking a higher number of unsatisfied requests.
31	SB, SH	The special building (thermal center) needs of a continuous supply of energy, that in some days or weekends can be higher than usual leading to a competition to stole energy against other city buildings.
31	SB, S	When a match is in progress, a huge amount of energy is requested by the stadium, which competes for the acquisition with the special building. The latter may receive a non-sufficient amount of energy for their purposes.

6.2.3 Growing number of People

The growing number of citizens needs building new different **offices** to give people the opportunities to work and to increase the appeal of the city. From the other side, this change calls to a massive request of energy that cannot be provided only by the existing power plant, so a new renewable (**wind farm**) energy source is added to the city. The smartness of the city remains very poor because the authorities in this phase are interested in building new infrastructures and not in improving the existing grid, because for the moment the newer citizens need homes and work instead of advanced smart services.

- ADDED: Office (O), Wind Farm (WF)
- REMOVED: none

Table 10: Emerging threats for "Growing Number of People"

IRENE Index	Involved Components	Description
5	O, SH	Malwares may corrupt personal employers' devices thus leading to detrimental consequences in the offices where employers operate with such devices. This allows the access from attackers which may either stole data or apply denial-of-service attacks. Personal devices of the employers can be corrupted by this type of malware. Its diffusion is facilitated by lack of attention that a common user has with respect to the common communication channels
9	O, SH	An adversary may get an un-authorized access to the office exploiting non-correctly implemented access policies. This may let internal information undisclosed to non-authorized users. The security configurations of each office are dependent from the passwords of the employers, and the permissions may not be always configured in the right way

IRENE Index	Involved Components	Description
11	O, SH	Personal devices of the employers can be corrupted by this type of malware. Its diffusion is facilitated by the lack of attention that a common user has with respect to the common communication channels
15	O, SH	When an employer tries to connect to the office from home an attacker can intercept data such as passwords or other types of key information because the communication may not be secure enough (e.g., missing encryption)
20	O, SH	Taking advantage of information that can be erroneously left available from the employers, the attacker can lead cyber-physical threats directed to the offices.
27	O, O	Adversary can acquire information from different organizations that have offices in the city thus leading to detrimental consequences, namely DoS and privacy attacks.
29	O, SH	The lack of attention that a common user has with respect to the common communication channels can contribute to expose information with unauthorized users.
30	O, SH	The lack of attention that a common user has with respect to the common communication channels can contribute to expose information with unauthorized users.
31	O, S	When a match is in progress, a huge amount of energy is requested by the stadium, which competes for the acquisition with the other key resources
31	O, O	Different offices can fight to obtain the needed energy, stealing it from other offices. This competition lead to detrimental consequences, i.e., some offices may incur in a non-sufficient provision of energy for their purposes.
31	O, SB	The special building (thermal center) needs of a continuous supply of energy, that in some days or weekends can be higher than usual leading to a competition to get energy against other city buildings. The latter may receive a non-sufficient amount of energy for their purposes.

6.2.4 Adding key buildings

Now the increased number of people calls for building structures that are useful to take care of the health of the citizens, so a new **hospital** is built in the city and the power plant in the city's area is replaced with a **photovoltaic** one. This allows the city to reduce the carbon emissions, although PVs do not produce electricity at night, as PP did. The hospital is connected to the data line and some basic data flow control techniques are added only to monitor the energy provided to the hospital.

- ADDED: Hospital (H), Photovoltaic station (PVG)
- REMOVED: Power Plant (PP), Power Substation (PS)

Table 11: Emerging threats for "Adding Key Buildings"

IRENE Index	Involved Components	Description
10	AP, H	If a citizen checks some data related to the hospital or requests some services such as payments, day hospital treatment … some connections may not be closed properly by the user, giving the attacker opportunities to exploit them.
15	AP, H	If a citizen checks some data related to the hospital or requests some services such as payments, day hospital treatment, the attacker can collect the data trying to extract useful information
16	AP, H	The services provided by the hospital can be blocked using wireless jamming techniques from the public access point
18	AP, H	The services provided by the hospital can be blocked by external attackers by using DoS techniques from the public access point
21	AP, H	If a citizen checks some data related to the hospital or requests some services such as payments, day hospital treatment, the attacker can intercept the data trying to extract useful information or compromise the communications.
31	H, S	When a match is in progress, a huge amount of energy is requested by the stadium, which competes for the acquisition with the other key components. The latter may receive a non-sufficient amount of energy for their purposes.
31	H, O	The hospital needs a continuous supply of energy that can generate races to acquire the energy leading to the provision of non-sufficient amount of energy for some components.
31	H, SB	The special building (thermal center) needs of a continuous supply of energy, that in some days or weekends can be higher than usual leading to a competition to get energy against other city buildings. The latter may run out of energy.
31	H, F	The hospital needs a continuous supply of energy that can generate races to acquire the energy. Factories may incur in a non-sufficient provision of energy for their purposes.

6.2.5 Inserting storages

Smart features start to have an important role in the city context. First of all, the authorities decide to insert two **storage** points in the grid, one near to an energy source and the hospital and one near to the other source and to the factory and the offices. These storages placed in key points of the grid should help to improve the resilience of the grid, especially regarding the continuity of energy provided to key buildings as hospital, offices, factory and the stadium when a match is on. A **basic data center** system implements simple load balancing techniques based on the existing (and quite poor) sensor network to take advantage of the new storages.

- ADDED: Data and Energy Storage (DES), Basic Data Center (BDC)
- REMOVED: none

Table 12: Emerging threats for "Inserting Storages"

IRENE Index	Involved Compo-nents	Description
5	AP, BDC	Using the public access point the adversary can try to insert some kind of malware into the data center, (e.g. sending some corrupted data that contains malware), resulting in information leakage and malfunctioning of the Basic Data Center (BDC).
9	AP, BDC	Using the public access point the adversary can exploit poorly configured protocols to get access to key functionalities of the data center control. This may end up to information leakage and malfunctioning of the BDC.
12	AP, BDC	Using the public access point the adversary can try to exploit some vulnerabilities of the new data center that are not detected from the city owners
12	AP, S	Using the public access point the adversary can try to exploit some vulnerabilities due to the recent connection changes that are not detected from the city owners
15	DES, H	The data channel between storages and key buildings can be monitored to intercept key communications (e.g. request of providing more energy in a specific interval of time)
15	DES, F	The data channel between storages and key buildings can be monitored to intercept key communications (e.g. request of providing more energy in a specific interval of time)
15	DES, SB	The data channel between storages and key buildings can be monitored to intercept key communications (e.g. request of providing more energy in a specific interval of time)
15	DES, S	The data channel between storages and key buildings can be monitored to intercept key communications (e.g. request of providing more energy in a specific interval of time)
15	BDC, H	The data channel between data center and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
15	BDC, F	The data channel between data center and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
15	BDC, SB	The data channel between data center and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data com-

IRENE Index	Involved Compo-nents	Description
		ing from building' sensors ...)
15	BDC, S	The data channel between data center and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
15	DES, BDC	The data channel between data center and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
21	DES, H	The data channel between storages and key buildings can be monitored to intercept or counterfeit key communications (e.g. request of providing more energy in a specific interval of time) changing the content of a specific group of packets.
21	DES, F	The data channel between storages and key buildings can be monitored to intercept or counterfeit key communications (e.g. request of providing more energy in a specific interval of time) changing the content of a specific group of packets.
21	DES, SB	The data channel between storages and key buildings can be monitored to intercept or counterfeit key communications (e.g. request of providing more energy in a specific interval of time) changing the content of a specific group of packets.
21	DES, S	The data channel between storages and key buildings can be monitored to intercept or counterfeit key communications (e.g. request of providing more energy in a specific interval of time) changing the content of a specific group of packets.
21	BDC, H	The data channel between data center and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.
21	BDC, F	The data channel between data center and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.
21	BDC, SB	The data channel between data center and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.

IRENE Index	Involved Compo-nents	Description
21	BDC, S	The data channel between data center and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.
21	DES, BDC	The data channel between data center and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.

6.2.6 Building of an industrial center

The city infrastructures (streets, public transports …) are improved and allow the citizens to move quickly from one side of the city to another, so the authorities build an **offices district** in which all the offices are placed. The old ones are removed from their original locations. This center is placed near the factory and close to a primary energy source such as the wind farm to have preferential access to the generated power. To improve the efficiency, a **micro grid** is installed in that area and the data center is uploaded with the insertion of new features that supports load balancing policies for micro grids.

- ADDED: Micro Grid (MG), Offices District (OD)
- REMOVED: Office (O)

Table 13: Emerging threats for "Building an Industrial Center"

IRENE Index	Involved Components	Description
5	OD, AP	Malwares may corrupt personal employers' devices thus leading to detrimental consequences in the offices where employers operate with such devices. This allows the access from attackers which may either stole data or apply denial-of-service attacks.
5	MG, AP	Using the access point the adversary can try to inject malware into other components, especially the new micro grid that controls the activities of buildings that are pillars of the city's economy
9	OD, AP	An adversary, by using the Internet, may get an un-authorized access to the office district exploiting non-correctly implemented access policies. This may let internal information undisclosed to non-authorized users either internal or external through the access point.

IRENE Index	Involved Components	Description
12	OD, AP	The permissions to access data may not be always configured in the right way because of the dynamicity of the offices in which a person can change role, fired, suspended, ...
15	OD, AP	When an employer try to connect to the office from home an attacker can intercept data such as passwords or other types of key information because the communication may be not encrypted
20	OD, AP	Taking advantage of information that can be erroneously left available from the employers, the attacker can lead cyber-physical threats directed to the offices.
24	MG, AP	Using the access point the adversary can try to get privileged access to other components, especially the new micro grid that controls the activities of buildings that are pillars of the city's economy
29	OD, AP, SH	The lack of attention that a common user has with respect to the common communication channels can contribute to expose information with unauthorized users if the employer try to access to working data from home
30	OD, AP, SH	The lack of attention that a common user has with respect to the common communication channels can contribute to expose information with unauthorized users if the employer try to access to working data from home
31	MG, S	When a match is in progress, a huge amount of energy is requested by the stadium, which competes for the acquisition with the micro grid. The latter may receive a non-sufficient amount of energy for their purposes.
31	MG, H	The hospital needs a continuous supply of energy that can generate races to acquire the energy. The latter may incur in a non-sufficient provision of energy leading to detrimental consequences.
31	MG, SB	The special building (thermal center) needs of a continuous supply of energy, that in some days or weekends can be higher than usual leading to a competition to get energy against other city buildings.

6.2.7 Improving Smart services

Due to the new smart components added to the grid, such as storages and micro grids, the basic flow control techniques are not able to manage the whole functionalities, so a **SCADA** system is installed instead of the basic data center to provide advanced load balancing, islanding and demand side response mechanisms.

- ADDED: SCADA
- REMOVED: Basic Data Center (BDC)

Table 14: Emerging threats for "Improving Smart Services"

IRENE Index	Involved Components	Description

IRENE Index	Involved Components	Description
5	AP, SCADA	Using the public access point the adversary can try to insert some kind of malware into the SCADA, (e.g. sending some corrupted data that contains malware)
9	AP, SCADA	Using the public access point the adversary can exploit poorly configured protocols to get access to key functionalities of the SCADA
12	AP, SCADA	Using the public access point the adversary can try to exploit some vulnerabilities of the new SCADA that are not detected from the city owners
12	MG, SCADA	Since the component is new, some interactions could have problems left erroneously (or inserted by an adversary) that can be exploited from an attacker, such as the integration of micro grid policies with the ones defined by authorities for the whole city and implemented in SCADA.
15	SCADA, H	The data channel between SCADA and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
15	SCADA, F	The data channel between SCADA and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
15	SCADA, SB	The data channel between SCADA and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
15	SCADA, S	The data channel between SCADA and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
15	DES, SCADA	The data channel between SCADA and key buildings can be monitored to intercept key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...)
21	SCADA, H	The data channel between SCADA and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.

IRENE Index	Involved Components	Description
21	SCADA, F	The data channel between SCADA and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.
21	SCADA, SB	The data channel between SCADA and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.
21	SCADA, S	The data channel between SCADA and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.
21	DES, SCADA	The data channel between SCADA and key buildings can be monitored to intercept or counterfeit key communications (e.g. load balancing update, changing on permissions regarding the usage of energy, key data coming from building' sensors ...) changing the content of a specific group of packets.

6.2.8 Installing micro grids

The SCADA system is updated with the installation of new features such as the management of the feedbacks and the requests coming from the citizens, which now have new smart features in their houses; further, most of the citizens are now *prosumers*. Their devices are also upgraded to allow the people to send data directly from the mobile devices. New **micro grids** are added, one to the residential zone and one to the services zone, to optimize the power consumption.

- ADDED: Micro Grid (MG)
- REMOVED: none

Table 15: Emerging threats for "Installing Micro Grids"

IRENE Index	Involved Components	Description
9	SH, MG	The improvement of smartness of the grid allowing communications and exchange of data from/to mobile devices can lead to expose the grid to new attacks that take advantage of some lack of permissions or wrong configurations.
10	SH, MG	Tunnels opened from mobile devices in the smart homes can be left opened erroneously from the user and not detected by mobile devices security techniques, which are not currently well developed as the desktop ones.

IRENE Index	Involved Components	Description
11	SH, MG	The improvement of smartness of the grid allowing communications and exchange of data from/to mobile devices can lead to expose the grid to new attacks that take advantage of known mobile vulnerabilities.
12	SH, MG	Communications can now be established between mobile device and the grid, consequently new vulnerabilities are introduced such as the protection of tunnels opened by mobile devices.
15	SH, MG	Communications between smart devices and the grid, as for example specific micro grids, can be intercepted
16	SH, MG	Wireless jamming can now be conducted from mobile devices owned by the citizens against different components of the grid, such as micro grids that own the energy sources, with the target to compromise the supply of energy
17	SH, MG	Some ports can be left opened by different bad coded apps running on the mobile devices and exploited by the attacker through the micro grid connection.
20	SH, MG	The vulnerabilities and the chances to get useful information looking at specific areas of memory in the mobile device can be used to conduct cyber-physical attacks.
21	SH, MG	Communications between smart devices and the grid, as for example specific micro grids, can be corrupted inserting wrong information or blocking the packets
24	SH, MG	The vulnerabilities and the chances to get useful information looking at specific areas of memory in the mobile device can be used to obtain unauthorized access to facilities through the micro grid connection.
29	SH, MG	Mobile users can share any type of information using instant messaging, mail …, giving the observer several opportunities to catch them.
31	MG, MG	Since now several different micro grids are installed in the smart grid, they can fight to acquire all the needed energy. The latter may receive a non-sufficient amount of energy for their purposes.
37	SH, MG	Some of the new vulnerabilities can come from the apps and kernel modules of mobile devices.

6.2.9 Improving decarbonisation

To further advance the decarbonisation process, a public **charging point** is installed in the residential grid to allow the citizens to charge their electric vehicles and reduce carbon emissions due to the usage of the cars.

- ADDED: Public Charging Point (CP)
- REMOVED: none

Table 16: Emerging threats for "Improving Decarbonisation"

IRENE Index	Involved Components	Description
9	CP, MG	If the authentication policies are not strict enough or the permissions for the charging of vehicles have some type of lack, the grid can incur in supply problems due to the CP component.
10	CP, MG	If the process that manages the opening or closing of the channels/ports has some type of lack, the grid can incur in supply problems due to the CP component.
12	CP, MG	The charging point can introduce several new vulnerabilities, such as ones related to authentication.
15	CP, MG	Feedbacks or requests coming from/to the charging point can be intercepted to annoy the correct behaviour of the system.
17	CP, MG	If the permissions are not strict enough or the mechanisms to regulate the opening or closing of the channels/ports have some type of lack, the grid can incur in supply problems due to the CP component.
21	CP, MG	Since this point has a key role regarding the citizen satisfaction or grid efficiency, can be targeted from DoS attacks aimed to corrupt electrical charging behaviour through the micro grid connection.
31	CP, MG	If the supply of energy is not well regulated, an attacker can leech a huge amount of energy from the charging point stealing it to the near homes or other components. The latter may incur a non-sufficient provision of energy for their purposes.

7 MITIGATION STRATEGIES AND OUTPUTS

7.1 MITIGATION STRATEGIES

While the definition of a threat list is mandatory to perform properly the threat identification process, some indications about mitigation policies and strategies are useful to enrich the threat analysis process with key details about possible responses with respect to a specific threat coming from the library. The role of this information can be summarized as follows: it is very important to know the events possibly damaging the system, but it is also very useful to know how we can respond in a crisis situation or how we can avoid a specific danger for the grid. This summarization is depicted in Figure 3.

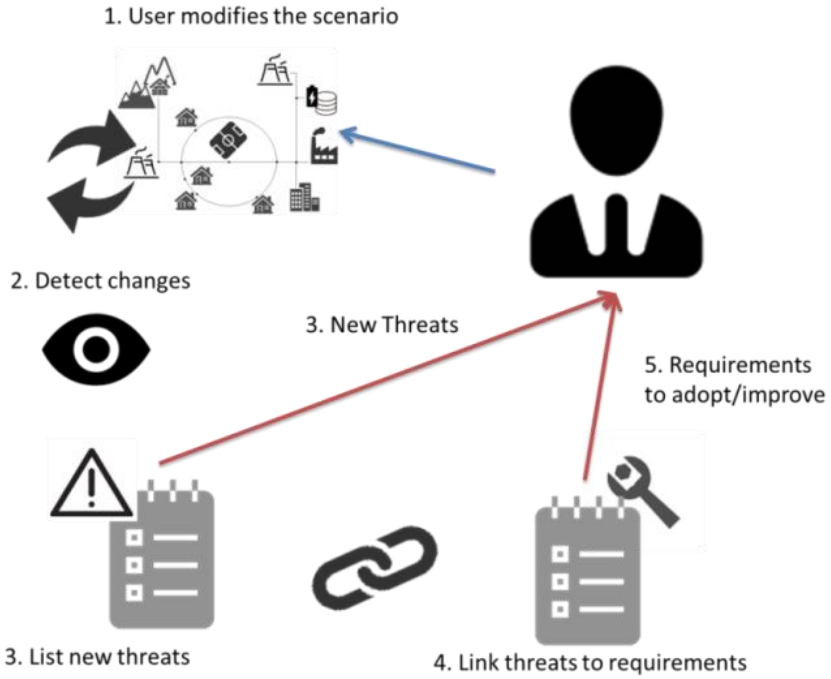


Figure 3: Application of mitigation strategies

In [3] we can observe a detailed list of smart grid security requirements, aimed to avoid classes of threats and actions that can damage the system. These requirements are grouped into categories (reported in Annex C), that are detailed enough for our context: the mitigation policies for each threat event will constitute pointers to categories of security requirements that should be implemented to face and mitigate the upcoming threat. We want to point out that these are only general mitigation guidelines, without quantitative evaluation of the implementation costs and the effectiveness trade-off, that are difficult to calculate in such generic context.

In Annex D we reported the links between IRENE threat events and categories with the abovementioned mitigation strategies. The link is direct, so if a threat or a threat category is present in a scenario, it is immediate to understand the mitigation policies that should be implemented.

7.2 DESCRIPTION OF THE OUTPUT

As already said in the previous sections, we investigated threat events due both to structural and emerging behaviours. At each step, depending on changes to the scenario, new threats can be added or removed from the list depending on newer interactions. As a consequence we enlist the consequent mitigation strategies we can use to avoid these specific threats. Each threat event is linked to a mitigation strategy and, depending on the evolution and on the components, that event can affect the scenario due to intrinsic or emerging reasons.

Finally, the output of the threat analysis is a list of threat events in which selecting a scenario at a defined evolution step and for each of the involved threats we can find information about:

- Type of the threat: structural or emerging
- Details about the threat and its category
- Involved components (only one if the type is structural)
- Motivations described in natural language
- Possible mitigations that can be implemented to limit or avoid the effect of that threat

8 CONCLUSIONS

This document present the threats identification methodology applied in IRENE. The threats have been identified and matched to different scenarios that are considered as reference for the IRENE project.

The analysis has been applied following a methodology intended to be effective in case of an evolutionary behaviour of the scenario, focusing the attention on the threats that emerge due to the connection of previously disconnected grid parts, due to the insertion or removal of components/functionalities. The methodology is fully compliant to the standard NIST 800-30.

Starting from an initial scenario, the methodology is built to perform the same sequence of actions for each evolution of such scenario. The actions are:

- Investigate the IRENE threats list to understand if threats intrinsic of the components and its interface are introduced, and mitigations are defined (new security requirements are introduced).
- Investigate the interactions established between one newer component and every set of old ones and analyse threats due to such interactions, and mitigations are defined (new security requirements are introduced)
- The results lead to an update of the threat events list for the scenario and the linked mitigations.

Once all the evolved scenarios are analysed, all the results coming from each iteration of the process are merged and added to the final list, that contain information about what event is generated from which group of components and if that event is due to emerging or static behaviour.

The threats list presented here and its application will be further applied in the remaining of the project. It is an input to Task 2.2 in order to perform a root causes identification and societal impact analysis of the different threats as well as an input to WP1 to support the identification of the requirements of the collaborative framework. Additionally, the threat analysis will be applied in the remaining of IRENE for the assessment of the collaboration framework, to observe how the actors (stakeholders, DNOs, city planners, regulators) using the collaboration framework will operate to address (a selection of) the identified threats. In particular, emergent threats are expected to require a deeper collaboration of the different actors in order to be predicted and/or mitigated efficiently.

9 REFERENCES

[1] Casey, Timothy. "Threat Agent Library Helps Identify Information Security Risks." Intel White Paper, September (2007).

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

[3] Grid, NIST Smart. "Introduction to NISTIR 7628 guidelines for smart grid cyber security." Guideline, Sep (2010).

[4] Kammerstetter, Markus, et al. "Practical risk assessment using a cumulative smart grid model." 3rd International Conference on Smart Grids and Green IT Systems (SMARTGREENS). 2014.

[5] Uslar, Mathias, Christine Rosinger, and Stefanie Schlegel. "Security by Design for the Smart Grid: Combining the SGAM and NISTIR 7628." Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International. IEEE, 2014.

[6] Smart Grid Coordination Group, CEN-CENELEC-ETSI. Smart grid reference architecture. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf, 2012.

[7] Communication from the Commission on "Critical Information Infrastructure Protection - Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM 149, March 2009.

[8] S.M. Rinaldi, Modeling and simulating critical infrastructures and their interdependencies, 37th Annual Hawaii International Conference on Systems Sciences, pp. 54-61, January 2004.

[9] A. Wenger, V. Mauer, and M. Dunn, Critical information infrastructure protection, International CIIP Handbook 2008, ETH the Swiss Federal Institute of Technology Zurich, 2008, September.

[10] U.S. Department of Energy DoE, FY2008-2013 National SCADA test bed program - multi-year plan, Enhancing Control Systems Security in the Energy Sector, January 2008, http://energy.gov/ [accessed 18 November 2012].

[11] M. Amin, Toward self-healing energy infrastructure systems, IEEE Computer Applications in Power, vol. 14, pp. 20-28, 2001, January.

[12] SMB Smart Grid Strategic Group SG3, IEC Smart Grid Standardization RoadMap, Ed 1.0, June 2010, http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf [last accessed 19 November 2012].

[13] Smart Grid Mandate M/490 EN to European Standardisation Organisations (ESOs) to support European Smart Grid deployment, 2011, http://ec.europa.eu [last accessed 19 November 2012].

[14] 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.

[15] Power Systems Engineering Research Center, Detection, prevention and mitigation of cascading events, Final Report, Part I, Part II, Part III, http://www.pserc.org [last accessed 18 November 2012].

[16] Kopetz, H. A. ―Conceptual Model for the Information Transfer in Systems of Systems‖. Proc. Of ISORC 2014. Reno, Nevada. IEEE Press. 2014.

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

[18] 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.

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

[20] Depuru, Soma Shekara Sreenadh Reddy, Lingfeng Wang, and Vijay Devabhaktuni. "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft." Energy Policy 39.2 (2011): 1007-1015.

[21] ENISA, Smart Grid Threat Landscape and Good Practice Guide, December 2013.

[22] IEC TC57 "IEC 61850: Communication networks and systems for power utility automation." International Electrotechnical Commission Std (2010).

[23] Jovanovic, Philipp, and Samuel Neves. "Dumb Crypto in Smart Grids: Practical Cryptanalysis of the Open Smart Grid Protocol."

A THREAT CATEGORIES

Each IRENE event is described through the following features:

- **Category Index**: a progressive and unique identification number;
- **Type**: defines if the category is related to adversarial or not adversarial threats;
- **Code:** a textual unique code describing the category;
- **Description**: a brief (but more understandable than the Code) description of the category, describing the features of the contained threats;
- **# IRENE events:** number of events that belong to that category.

The considered categories are shown in the table below.

Table 17: IRENE Threat categories

Category Index	Type	Code	Description	# IRENE Events
1	ADV	PRGI	Perform reconnaissance and gather information	3
2	ADV	CCAT	Craft or create attack tools	1
3	ADV	DIIMC	Deliver/insert/install malicious capabilities	3
4	ADV	EC	Exploit and compromise	7
5	ADV	CA	Conduct an attack (e.g., direct/coordinate attack tools or activities)	8
6	ADV	AR	Achieve results (e.g., cause adverse impacts, obtain information)	3
7	ADV	CC	Coordinate a campaign	3
8	NA	ACC	Accidental	3
9	NA	ENV	Environmental	4
10	NA	HI	Hardware or Implementation	3
			Total	**38**

B THREAT EVENTS

Starting from the NIST list of threat events, we reduced the summarization of threats by taking the following actions:

- hold the threat events that are representative also in our context;
- merge similar events into a unique IRENE threat event;
- delete the threat events that are not relevant or not usable in the context due to specific motivations.

The results are shown in the table below. The held NIST events are the ones with no highlighted motivation, the merged events are labelled as "merged" with indications on the linked IRENE event (that is the same for all the similar events merged into the same one) while the deleted NIST events are targeted by a missing value in the corresponding IRENE index.

Table 18: NIST to IRENE threat list

NIST Index	Action	IRENE Index	Motivation
1	Held	1	Represents perimeter scanning aimed to collect data
2	Merged	1	Perimeter scanning that focuses on exposed networks is merged with other perimeter sniffing events
3	Held	2	-
4	Held	3	Represents internal/targeted reconnaissance
5	Merged	3	Internal reconnaissance is merged with reconnaissance of targeted operations to build a "reconnaissance" threat event.
6	Held	4	Represents attacks that aim to obtain sensitive data tricking the user.
7	Merged	4	Type of phishing attack, similar to 6. The aim is still to obtain sensitive data.
8	Deleted	-	Difficult to understand the specificities of information technology environments since we are at higher abstraction levels
9	Merged	4	Attack based on counterfeiting of components that aims to obtain sensitive data
10	Merged	4	Attack based on counterfeiting of components that aims to obtain sensitive data
11	Deleted	-	False front organizations are too specific for our context
12	Held	5	Represents the delivery of malware using different installation or delivering channels / policies
13	Merged	5	Specific type of malware

NIST Index	Action	IRENE Index	Motivation
14	Merged	5	Specific type of malware
15	Merged	5	Specific malware delivering mechanism
16	Merged	5	Specific malware delivering mechanism
17	Merged	5	Specific type of malware
18	Merged	5	Specific malware delivering mechanism
19	Merged	5	Specific type of malware
20	Deleted	-	The compromisation of software components is well defined in the "Exploit and Compromise" category.
21	Held	6	Represents the installation of sniffer and scanning devices inside the targeted system.
22	Merged	6	Specific type of sniffer
23	Merged	6	Specific type of sniffer
24	Held	7	Represents the insertion of subverted individuals into organizations
25	Merged	7	Specific type of individuals
26	Held	8	-
27	Held	9	-
28	Held	10	-
29	Deleted	-	Too many specific conditions for our abstraction level
30	Held	11	-
31	Held	12	-
32	Deleted	-	Too many specific vulnerabilities in such wide and high level context
33	Deleted	-	Too many specific vulnerabilities in such wide and high level context
34	Deleted	-	Too many specific vulnerabilities in such wide and high level context
35	Deleted	-	Too many specific conditions for our abstraction level
36	Deleted	-	Too many specific conditions for our abstraction level
37	Deleted	-	Too many specific physical access: better described in event 50
38	Held	13	Represents information compromisation of specific components and devices
39	Held	14	Represents specific software information compromisation
40	Merged	14	Specific target for compromisation
41	Merged	14	Specific targeted information

NIST Index	Action	IRENE Index	Motivation
42	Merged	13	Compromisation of specific components
43	Held	15	Represents the conduction of communication interception attacks
44	Held	16	-
45	Held	17	-
46	Held	15	Specific interception strategy
47	Held	18	Represents the conduction of DoS attacks
48	Merged	18	Specific type of DoS attack
49	Merged	18	Specific type of DoS attack
50	Held	19	Represents conduction of physical attacks
51	Merged	19	Specific type of targeted resources
52	Held	20	Represents the conduction of cyber-physical attacks
53	Deleted	-	Too many specific type of attacks in a such wide and high level context
54	Merged	20	Specific type of cyber attack
55	Deleted	-	Too many specific type of attacks in a such wide and high level context
56	Merged	20	Specific type of cyber attack
57	Merged	20	Specific type of cyber attack
58	Held	21	Represents conduction of MiM attacks
59	Merged	21	Specific type of MiM attacks
60	Held	22	Represents social engineering attacks also based on user devices
61	Merged	22	Specific type of attack
62	Merged	22	Specific type of attack
63	Deleted	-	Too many specific conditions for our abstraction level
64	Deleted	-	Already considered in events 1-2
65	Deleted	-	Too many specific conditions for our abstraction level
66	Merged	18	Specific targeted services that must be compromised

NIST Index	Action	IRENE Index	Motivation
67	Held	23	Represents the deterioration of critical components that might lead to integrity loss
68	Merged	23	Specific type of damage that causes integrity loss
69	Merged	23	Specific type of damage that causes integrity loss
70	Merged	23	Specific type of damage that causes integrity loss
71	Deleted	-	Too many specific conditions for our abstraction level
72	Deleted	-	Too many specific conditions for our abstraction level
73	Deleted	-	Too many specific conditions for our abstraction level
74	Held	24	-
75	Held	25	Represents the obtainment of sensitive data based on information systems
76	Merged	25	Specific type of data stealing
77	Deleted	-	Too many specific conditions for our abstraction level
78	Deleted	-	Too many specific type of attacks in a such wide and high level context
79	Held	26	Represents campaigns of multi staged attacks
80	Merged	26	Multi attacks: internal and external
81	Held	27	Represents the coordination of campaigns using multiple strategies
82	Held	28	-
83	Merged	27	Specific type of campaign based on changing attacks
84	Merged	26	Multi attacks: outsider, insider, supplier
85	Held	29	-
86	Held	30	-
87	Held	31	-
88	Deleted	-	Too many specific type of attacks in a such wide and high level context
89	Deleted	-	Too many specific type of attacks in a such wide and high level context
90	Held	32	-
91	Held	33	Represents a fire natural disaster
92	Merged	33	Specific type of facility
93	Held	34	Represents a flooding natural disaster

NIST Index	Action	IRENE Index	Motivation
94	Merged	34	Specific type of facility
95	Held	35	Represents an hurricane natural disaster
96	Merged	35	Specific type of facility
97	Held	36	-
98	Held	37	-
99	Held	38	Represents the hardware resource disk error
100	Merged	38	Specific disk error type
101	Merged	35	Similar to Hurricane
102	Merged	35	Similar to Hurricane and specific type of facility

Depending on the distinction reported above, each IRENE event is described through the following features:

- **Event Category**: the code of the category related to the event;
- **NIST reference**: a pointer to the NIST event(s) that constitutes the specified IRENE event. If the event is the result of a merge among different NIST events, the pointers will be more than one;
- **IRENE Index**: a progressive and unique identification number;
- **Threat event name and description**: the same of the NIST reference. For events that are outcomes of the fusion of different NIST ones, these elements are a summarization of the relevant characteristics of each constituent event.

The complete list of IRENE threat events is shown in Table 19

.

Table 19: IRENE threat list

Event Category	NIST Indexes	IRENE Index	Threat Event	Description
PRGI	1,2	1	Perform perimeter (or exposed) network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
PRGI	3	2	Gather information using open source discovery of organizational information.	Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
PRGI	4, 5	3	Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation, malware) over time to examine and assess organizations and ascertain points of vulnerability.
CCAT	6, 7, 9, 10	4	Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, duplicate of legitimate sites or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
DIIMC	12, 13, 14, 15, 16, 17, 18, 19	5	Deliver known/modified malware to internal organizational information systems.	Adversary uses some delivery mechanisms (e.g., email, web traffic, instant messaging, FTP, removable media, downloadable software) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
DIIMC	21, 22, 23	6	Install sniffers or scanning devices on organizational information systems and networks.	Adversary places within internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.

Event Category	NIST Indexes	IRENE Index	Threat Event	Description
DIIMC	24, 25	7	Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.
EC	26	8	Exploit physical access of authorized staff to gain access to organizational facilities.	Adversary follows ("tailgates") authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
EC	27	9	Exploit poorly configured or unauthorized information systems exposed to the Internet.	Adversary gains access through the Internet to information systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
EC	28	10	Exploit split tunnelling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to non-secure remote connections.
EC	30	11	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.

Event Category	NIST Indexes	IRENE Index	Threat Event	Description
EC	31	12	Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.
EC	38, 42	13	Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware) or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected. Adversary can also compromise the design, manufacture, and/or distribution of critical information system components at selected suppliers.
EC	39, 40, 41	14	Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
CA	43, 46	15	Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted, use weak encryption (e.g., encryption containing publically known flaws) or permitted information flows (e.g., email communication, removable storage), to gain access to transmitted information and channels.
CA	44	16	Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
CA	45	17	Conduct attacks using unauthorized ports, protocols and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
CA	47, 48, 49, 66	18	Conduct Denial of Service (DoS) attack.	Adversary attempts to make an Internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.

Event Category	NIST Indexes	IRENE Index	Threat Event	Description
CA	50, 51	19	Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities or infra-structures (e.g., sets a fire, breaks a water main, cuts a power line).
CA	52, 54, 56, 57	20	Conduct cyber-physical attacks on organizational facilities, session hijacking or brute force attempts.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings), takes control of (hijacks) already established with the aim to legitimate information or leads systematic guessing of passwords, possibly supported by password cracking utilities .
CA	58, 59	21	Conduct Man In the Middle attacks.	Adversary, operating outside organizational systems, inter-cepts/eavesdrops on sessions between organizational and external sys-tems. Adversary then relays messages between organizational and exter-nal systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
CA	60, 61, 62	22	Conduct social engineering attacks targeting and com-promising personal devices of critical employees.	Adversary takes actions (e.g., using email, phone) with the intent of per-suading or otherwise tricking individuals within organizations into reveal-ing critical/sensitive information (e.g., personally identifiable infor-mation). The main targets are key organizational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones).

Event Category	NIST Indexes	IRENE Index	Threat Event	Description
AR	67, 68, 69, 70	23	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	Adversary vandalizes organizational websites or data on websites or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Can also implant corrupted or incomplete data in critical one.
AR	74	24	Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.
AR	75, 76	25	Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components. Adversary can also scan or mine information on publically accessible servers and web pages of organizations with the intent of finding sensitive information.
CC	79, 80, 84	26	Coordinate a campaign of multi-staged (e.g., hopping) or multi-typed (e.g. outsider, insider, supplier) attacks.	Adversary combines attacks that require both physical presence within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
CC	81, 83	27	Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
CC	82	28	Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Adversary uses existing presence within organizational systems to extend the adversary's span of control to other organizational systems including organizational infrastructure. Adversary thus is in position to further undermine organizational ability to carry out missions/business functions.

Event Category	NIST Indexes	IRENE Index	Threat Event	Description
ACC	85	29	Spill sensitive information	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
ACC	86	30	Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.
ACC	87	31	Incorrect privilege settings	Authorized privileged user or administrator erroneously sets privilege requirements on a resource too low. This can lead to competition between different consumers aimed to acquire the needed energy, breaking the limits set by the owner.
ENV	90	32	Earthquake at primary facility	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
ENV	91, 92	33	Fire at primary/backup facility	Fire (not due to adversarial activity) at primary/backup facility makes facility inoperable.
ENV	93, 94	34	Flood at primary/backup facility	Flood (not due to adversarial activity) at primary/backup facility makes facility inoperable.
ENV	95, 96, 101,	35	Hurricane at primary/backup facility	Hurricane of organization-defined strength at primary/backup facility makes facility inoperable.

Event Category	NIST Indexes	IRENE Index	Threat Event	Description
	102			
HI	97	36	Resource depletion	Degraded processing performance due to resource depletion.
HI	98	37	Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
HI	99, 100	38	Disk error	Corrupted storage due to a disk error.

C SECURITY REQUIREMENTS (MITIGATIONS)

Here follows a list of security requirement categories coming from [3] that could help to mitigate or avoid some of the threat that will involve the scenario. We reported in the table only the basic information related to each of them: code, name, key characteristics.

Table 20: NIST security requirements

Code	Mitigation Index	Name	Key phrases
AC	1	Access Control	User Access Control
AT	2	Awareness and Training	Training based on roles/responsibilities
AU	3	Audit and Accountability	Compliance with policies/requirements
CA	4	Security Assessment and Authorization	Continuous monitoring, Internal checking, Incident investigation
CM	5	Configuration Management	Change test and management process, Testing of vendor updates
CP	6	Continuity of Operations	Continue/Resume disrupted operations
IA	7	Identification and Authentication	Identification, Authentication
ID	8	Information and Document Management	Protection of digital sensitive data
IR	9	Incident Response	Continue/Resume operations disrupted by an incident
MA	10	Smart Grid Information System Development and Maintenance	Maintenance
MP	11	Media Protection	Limit access to media
PE	12	Physical and Environmental Security	Protect physical assets, Surveillance
PL	13	Planning	Prevent/Recover from interruptions (natural, manmade, equipment)
PM	14	Security Program Management	Implementation of security program
PS	15	Personnel Security	Staff control, Confidentiality agreements
RA	16	Risk Management and Assessment	Identify risks, Identify vulnerabilities
SA	17	Smart Grid Information System and Services Acquisition	Policies for services acquisition

Code	Mitigation Index	Name	Key phrases
SC	18	Smart Grid Information System and Communication Protection	Protect communication links
SI	19	Smart Grid Information System and Information Integrity	Manage system flaws, Malicious code detection

D THREATS AND REQUIREMENTS LINKING

We listed the connections between IRENE event categories (see Annex A) and security requirements (see Annex C). A security requirement is connected to a category if and only if the requirement could help to face all the threat events that belong to the specific category.

Table 21: Mitigations for IRENE categories

Category Index	Mitigation Index	Motivation
1	1	Adversary counterfeits and duplicates of legitimate information: the access of these resources can be regulated through strict access control policies
5	9	Incident response policies are connected to the management of an attack conducted against the grid
5	14	The security program needs to be implemented and tailored to support this type of adversarial attacks, which can damage heavily the entire system.
6	4	Actions that lead to adverse impact can be identified through continuous monitoring and checking of system functionalities
7	16	The effect of an attack campaign can be mitigated if a threat analysis process was run before the happening of the problems due to the adversary
9	9	Ability to resume from disruptions is fundamental in this context because of the violence of natural events
9	10	Maintain the grid can help to face the upcoming natural disaster; a lack of attention regarding one or more component can expose them to huger damages by the event
9	12	When the event is not too wild, the adoption of physical protection techniques can decrease the impact on the grid components
9	13	Planning facilities can help to know the expected effects of the disaster and forecast it when it is possible

Another link we establish is the one between a single IRENE threat event and the requirements that are involved in the process of avoiding, mitigation and facing of that risk. As in the previous table, in each row we report the index of the threat event, the index of the requirement and the motivations related to the connection.

Table 22: Linking IRENE threat events to mitigations

Threat Index	Mitigation Indexes	Motivation

Threat Index	Mitigation Indexes	Motivation
1	11, 12, 18	To limit the amount of information collected by scanning, we can improve media (11), physical (12) and communication (18) protection
2	11	The only way to limit the analysis of open source data is to decrease the amount of sensitive knowledge shared with the community
3	4, 12, 16, 19	When an organization is surveiled, monitoring (4) and risk assessment (16) facilities could help to understand if someone is ready to steal information from you; check the integrity (19) and the physical security (12) is also a way to improve this protection.
4	14, 15, 18	The implementation of a security program is mandatory to limit this type of problems. The user must be aware (15) of this type of attacks, and also the communications (18) need to be protected from middle intrusions.
5	5, 17, 19	Every component need to come from a trusted organization (17) and also need to be tested (5) before inserting it into any organizational process. In this way, we become able also to detect malicious code (19) inserted into the new components.
6	4, 17, 19	Each component needs to come from a trusted organization (17) and checked to detect malicious code (19); in that case, monitoring activities could help to understand if there are some new untrusted streams or actions appeared on the context that execute suspect code.
7	1, 2, 4	It is mandatory to regulate (2) the way personnel access computer programs and applications, and control the access (1) of each of them every time, also using some monitoring (4) facilities.
8	1, 4, 12, 15	The first step is to assume personnel only after a regulated and controlled process (15). Although you have to monitor (4) their activities - also the physical access (12) - to understand if some suspicious actions are performed.
9	1, 2, 7, 10	The exposition is due to a lack of access control (1) (2) and authentication (7) policies. An efficient maintenance process has to be conducted in order to check and update the system configurations.
10	4, 18	All the communications must follow a defined protocol (18) that avoids keeping opened an unused connection. To support this protection technique, checking, investigation and monitoring facilities (4) can be adopted.
11	16, 17, 18	The vulnerabilities need to be assessed (16) in order to discover the weaknesses of the system. Once those vulnerabilities are discovered, the acquisition of new components cannot add new vulnerabilities (17), and the communication links between the system and the devices (18) needs to be protected.
12	8, 10, 13, 16	New vulnerabilities can be due to the lack of maintenance (10), a missing planning (13) process, risk assessment strategy (16) or sensitive data protection (8).

Threat Index	Mitigation Indexes	Motivation
13	5, 17, 19	The reintroduction or the update of software needs to be maintained and checked (17), and some malware detection policies (19), in addition with an adequate management of the configurations (5) need to be implemented.
14	4, 5, 19	If the compromisation could not be avoided with the management of the configurations (5), some monitoring (4) and malware detection policies (19) might be useful.
15	2, 12, 18	People that work on communications need to be aware by this type of attacks to recognize and signal them as soon as they can (and if they can). Cyber-Physical security on the communication links (12) (18) need to be improved to reduce the number of successful attacks.
16	6, 18	The jamming of wireless networks lead to the interruption of the communications, so continuity (6) and protection (18) policies needs to be created.
17	1, 5, 7, 13	Attacks on unauthorized ports can be faced with improved access control (1) and identification (7) policies. The best solution remains the one that, after a complete and accurate planned configuration (5) (13), does not allows the exploiting of that ports.
18	4, 6, 10	Once the attack is detected using control policies (4) or when the service is denied due to the attack, the continuity of the operations (6) need to be guaranteed by a quick maintenance (10) intervention.
19	2, 4, 12	Obviously the physical assets need to be protected (12) and the system (4) and the personnel (2) have to follow some "training courses" to timely detect the attack.
20	4, 6, 10, 12, 16, 19	The wider category of attacks that can be conducted against the system: risk assessment strategies (16) integrity checking (19). Physical assets need some type of protection (12) and in general maintenance (10), monitoring (4), and continuity of operations techniques help to face this type of threats.
21	2, 7, 18	The communication channels should block all the intrusion attempts (18), and also training of the personnel (2) and strong identification policies (7) could help to detect the attack before it damages heavily the whole system.
22	1, 8, 11, 19	Personal devices must also implement some content protection mechanisms (8) (11) and access control policies (1) in addition to malware detection utilities (19).

Threat Index	Mitigation Indexes	Motivation
23	1, 8, 10, 11, 13, 19	The access to public information need to re supported from content protection mechanisms (8) (11) and access control policies (1) in addition to malware detection utilities (19). The integrity loss must be recovered through maintenance (10) operations and a strategic planning (13) to tolerate this type of attacks (e.g. multiple copies of a database).
24	1, 3, 7	The access must be regulated (1) (7) and the actions must be compliant (3) with how expected for this user.
25	12, 14, 17	The theft of components must be avoided by protection policies (12) (17) and the security program management (14) have to support the system for these purposes.
26	4, 9, 10, 12	Different stages and different types of attacks can be very difficult to face, but incident response (9) and maintenance (10) techniques can speed up the recovery process, while monitoring, checking (4) and protection (12) facilities could help to prevent or mitigate the problem.
27	1, 2, 4, 15	The access to organizational data must be regulated (1) and checked (4), and also the personnel (15) must be aware of these risks and prepared (2) to not be tricked and convinced to share sensible data.
28	4, 9	The insider can be recognized also using monitoring techniques (4), and response (9) mechanisms must be implemented because of the high likelihood to do not recognize the threat before it becomes active.
29	2, 8, 15	The information need to be protected (8) and the personnel (15) must be aware of these risks and prepared (2) to not be tricked and convinced to share sensible data.
30	10, 15	Accidental threat that can be less frequent if the user is as affordable as possible (15) and maintenance strategies are activated (10).
31	1, 2, 13	The setup of the privileges might be wrong due to wrong access control (1) policies that are not compliant with the expectations (3) or a wrong planning (13) of some system protocols.
32	-	
33	-	
34	-	
35	-	
36	6, 10, 13	The lack of maintenance (10) or a wrong planning (13) of usage for that resources can expose the system to this type of threats that can also avoided implementing some tips aimed to guarantee the continuity of the operations (6).
37	4, 16, 17, 19	The accidental exposure to new vulnerabilities in response to an update or the acquisition of a new software can be limited by the verification (17) of the update source, and by conducting a risk assessment process (16) that for each update check the software with support given by monitoring (4) and malware detection (19) facilities.

Threat Index	Mitigation Indexes	Motivation
38	9, 10, 14	A hardware error can be mitigated only with maintenance (10) policies with the support of some incident response (9) ones.

E STRUCTURAL THREATS

Here follows the list of the threat events that are strictly related to the components we considered as constituent elements of the evolutionary scenarios. Note that this listing is valid and constant for each of those scenarios, because depends only on the functionalities, the behaviour and the peculiarity of each element.

Some of the events involve all the components that belong to a component category, so we defined a two-step process: first we identify the events that are in common between all the elements of a component category (first table). After that process, we analyse each specific component to understand which specific group of events could depend on it (second table). If a component belongs to a component category (e.g. the *MicroGrid* component belongs to the *Connection* category), the threat events that are related to that component are the merging of the specific (e.g. *MicroGrid*) and the category (e.g. *Connection*) ones.

Table 23: Structural threats of component categories

Category / Group	IRENE Index	Motivation
CON	1	Information shared in networks can be sniffed from connections
CON	3	Connection can be surveiled to get information about vulnerabilities
CON	6	Connection can be sniffed to collect data related to network traffic
CON	15	Communications can be intercepted directly from the link
CON	19	Communications can be broke up by physical attacks aimed to interrupt the exchange of data
EP	3	Since energy providers are key buildings, surveillance could be lead to understand vulnerabilities of the system.
EP	5	Since energy providers can have huge support coming from software systems depending on the functionality, adversary might want to deliver malware into that software
EP	6	Energy Providers need to communicate with the grid to understand useful indications about the generation of energy, so a sniffer activity could reveal lot of information about policies
EP	7	Energy providers works with employers, and subverted individuals can act the part of a simple employer and damage the structure
EP	8	Energy providers works with employers, and the access of authorized staff can be exploited
EP	14	Control software could be targeted especially due to its criticality
EP	19	Since energy providers are physical buildings, physical attacks could be lead with success
EP	22	Energy providers works with employers, and their devices could be compromised with the aim to reveal critical information
EP	26	Due to the complexity and the relevance of the tasks performed by the energy provider, multi - staged attacks can be conducted to defeat protections against attackers

Category / Group	IRENE Index	Motivation
EP	27	Since in the city scenario multiple organizations that provides energy are working simultaneously, the attacker can try to observe different companies to acquire useful data to break defences of target provider
EP	28	When a malicious presence is working in this type of city component, the actions can damage also other component, since the energy is needed in each of the city's services
EP	30	Energy providers works with employers, and users can inadvertently expose information to other people
EP	32	Since this component has a physical state, earthquakes can damage it
EP	33	Since this component has a physical state, fire can damage it
EP	34	Since this component has a physical state, flood can damage it
EP	35	Since this component has a physical state, hurricanes can damage it
BLD	2	Buildings are inserted in a city with specific purposes, that can be publically accessible and available also for adversaries
BLD	3	Each building can have its vulnerabilities, and the adversary wants to discover most of them
BLD	7	Building's employers can be inserted by adversarial organizations to obtain access to critical data
BLD	8	Building's employers have permissions to avoid security checks, that can be exploited from adversary
BLD	12	The physical and organizational evolution of companies that use building can introduce vulnerabilities in the cyber-physical structure
BLD	14	Each building has its software system depending on the functionalities and the adversary wants to insert malware to get data or compromise operations
BLD	19	Buildings are physical components, so is possible to conduct physical attacks aimed to damage them
BLD	26	Due to the complexity and the relevance of some of the tasks performed by the company that owns the building, multi - staged attacks can be conducted to defeat protections against attackers
BLD	28	When a malicious presence is working in this type of city component, the actions can damage also other component, depending on the specificity of that building
BLD	32	Since this component has a physical state, earthquakes can damage it
BLD	33	Since this component has a physical state, fire can damage it
BLD	34	Since this component has a physical state, flood can damage it
BLD	35	Since this component has a physical state, hurricanes can damage it

Category / Group	IRENE Index	Motivation
DAC	5	Data Center control most of the smartness of the grid, so adversary might want to compromise the functionalities with different kind of malwares
DAC	6	Data Center control most of the smartness of the grid and needs lot of data that can be observed during the execution
DAC	9	Data Center can be very complex, and the security configurations must be well-tailored to avoid adversary intrusions
DAC	10	Communications to and from data center need to open tunnels that could be left open by applications that are not well-written
DAC	14	Due to the complexity and the criticality of Data Center actions, the adversary might want to insert malware to get data or compromise operations
DAC	15	Communications to and from data center can be intercepted to limit or damage the effectiveness of techniques managed from this component
DAC	16	Data Centers are exposed to jamming attacks aimed to block or damage the usual traffic on the network
DAC	17	Since data is coming in a huge quantities from different ports or protocols, adversary can try to exploit these wider range of connections to found vulnerabilities
DAC	18	Data Centers are exposed to denial of service attacks aimed to block or damage the usual traffic on the network
DAC	20	Data Centers are key components, so adversaries could want to attack the systems in cyber-physical ways
DAC	23	Integrity of data is a pillar to the correct behaviour of the Data Center, so adversary could try to damage it leading this component to take wrong decisions
DAC	24	Data Centers are exposed to compromisation of policies, permissions, ports and channels also due to violations to authorization controls
DAC	29	Data is coming also from devices, that can be contaminated and prepared to send wrong or malicious data to Data Center
DAC	31	A data center can have specific setups about the permissions and protocols to use, and privileges can be set upped in a wrong way
DAC	36	Data Center are key components with huge support of resources that degrade due to continuous usage
DAC	37	Data Center are key components with huge information support systems (especially for authentication), so software could be affected by bugs that lead to vulnerabilities
DAC	38	Data Centers are key components with huge support of hard drive resources that can fail due to usage, depletion or read write errors.

Table 24: Structural threats of components

Component	IRENE Index	Motivation
EC	-	-
DC	10	It is possible to left open tunnels, that an adversary can exploit
MG	10	It is possible to left open tunnels, that an adversary can exploit
MG	17	A micro grid can have specific setups about the permissions and protocols to use, and an adversary can try to exploit lacks in these components
MG	31	A micro grid can have specific setups about the permissions and protocols to use, and privileges can be set upped in a wrong way
MG	37	When a service specific of micro grid is updated, vulnerabilities can be inserted into that software
CA	-	-
PS	-	-
LRC	-	-
F	5	Factories are key buildings, so adversaries could want to deliver malware to compromise / observe key functionalities
F	13	Factories are key buildings, so adversaries could want to compromise the update process of a component
F	22	Factories are key buildings, so adversaries could want to compromise the devices of the employers, trying to obtain key information
F	23	Factories are key buildings, so adversaries could want to damage key data
F	30	Factories work with employers, that can inadvertently expose critical information
F	36	Factories are key buildings with huge support of resources that degrade due to continuous usage
F	37	Factories are key buildings with huge information support systems, so software could be affected by bugs that lead to vulnerabilities
H	5	Hospitals are key buildings, so adversaries could want to deliver malware to compromise / observe key functionalities
H	23	Hospitals are key buildings, so adversaries could want to damage their key data
H	24	Hospitals are key buildings, so adversaries could want to obtain unauthorized access to key resources
H	25	Hospitals are key buildings, so adversaries could want to obtain data stealing unprotected devices

Component	IRENE Index	Motivation
H	30	Hospitals work with medical employers, that can inadvertently expose critical information
S	-	-
O / OD	4	Offices are key buildings, so adversaries could want to annoy or steal information by the users
O / OD	5	Offices are key buildings, so adversaries could want to deliver malware to compromise / observe key functionalities
O / OD	9	Offices are key buildings with huge support systems, so adversaries could want to exploit lack of configurations related to this system
O / OD	13	Offices are key buildings, so adversaries could want to compromise the update process of a component
O / OD	20	Offices are key buildings, so adversaries could want to attack the systems in cyber-physical ways
O / OD	22	Offices are key buildings, so adversaries could want to compromise the devices of the employers, trying to obtain key information
O / OD	23	Offices are key buildings, so adversaries could want to damage their key data
O / OD	25	Offices are key buildings, so adversaries could want to obtain data stealing unprotected devices (e.g. lost employer device)
O / OD	29	Offices are key buildings, so adversaries could want to try to spill information from employers' devices
O / OD	30	Offices work with employers, that can inadvertently expose critical information
O / OD	37	Offices are key buildings with huge information support systems, so software could be affected by bugs that lead to vulnerabilities
PP	-	-
PVG	-	-
WF	-	-
DES	6	Communications to and from the storages could be observed to collect network traffic
DES	8	Storages are key buildings, so adversaries could want to try to exploit staff access to get access to key functionalities
DES	13	Storages are key buildings, so adversaries could want to compromise the update process of a component
DES	14	Storages are key buildings, so adversaries could want to compromise their information systems
DES	17	Storages can have specific setups about the permissions and protocols to use, and an adversary can try to exploit lacks in these components
DES	19	Storages are key buildings, so adversaries could want to try to lead physical attacks against that facility

Component	IRENE Index	Motivation
DES	23	Storages are key buildings, so adversaries could want to damage key data
DES	24	Storages are key buildings, so adversaries could want to obtain unauthorized access to key resources
DES	32	Since this component has a physical state, earthquakes can damage it
DES	33	Since this component has a physical state, fire can damage it
DES	34	Since this component has a physical state, flood can damage it
DES	35	Since this component has a physical state, hurricanes can damage it
DES	36	Storages are key buildings with huge support of resources that degrade due to continuous usage
DES	38	Storages are key buildings with huge support of hard drive resources that can fail due to usage, depletion or read write errors.
AP	14	Access points are exposed to compromisation of policies, permissions, ports and channels also due to inserted malware
AP	16	Access points are exposed to jamming attacks aimed to block or damage the usual traffic on the network
AP	18	Access points are exposed to denial of service attacks aimed to block or damage the usual traffic on the network
AP	19	Access points are exposed to compromisation of policies, permissions, ports and channels also due to physical attacks
AP	24	Access points are exposed to compromisation of policies, permissions, ports and channels also due to violations to authorization controls
AP	31	Access points are exposed to compromisation of policies, permissions, ports and channels also due to violations to privilege settings
AP	37	Access points are exposed to compromisation of policies, permissions, ports and channels also due to vulnerabilities inserted in component's drivers
SH	4	Some of the vulnerabilities of Smart Homes come from the citizens that use smart services and functionalities. Phishing attacks can be leaded to the user to get sensitive information
SH	9	Some of the vulnerabilities of Smart Homes come from the citizens that use smart services and functionalities. Wrong configurations and permissions can be defined by non-expert users
SH	11	Attacks can be conducted through vulnerabilities left in the devices of the citizens that live in that home

Component	IRENE Index	Motivation
SH	23	Attacks can be conducted with the aim to damage energy usage policies or sensitive data to create problems (e.g. to city load balancing strategies)
SH	24	Attacks can be conducted with the aim to obtain unauthorized access to key components
SH	29	Some of the vulnerabilities of Smart Homes come from the citizens that use smart services and functionalities, and sensitive information can be spilled from devices or network tunnels
SH	30	Some of the vulnerabilities of Smart Homes come from the citizens that use smart services and functionalities,
SH	37	Some information can be inadvertently exposed by the citizens that use smart services and functionalities.
SB	5	Since they are special buildings, adversaries could want to deliver malware to compromise / observe key functionalities
SB	9	Special buildings can have huge support systems, so adversaries could want to exploit lack of configurations related to this system
SB	17	Since they are special buildings, they have specific setups about the permissions and protocols to use, and an adversary can try to exploit lacks in these components
SB	18	Since they are special buildings with key roles in a city's scenario, these components are exposed to denial of service attacks aimed to compromise the correct behaviour
SB	20	Since they are special buildings, adversaries could want to attack the systems in cyber-physical ways
SB	22	Since they are special buildings, adversaries could want to compromise the devices of the employers, trying to obtain key information
SB	25	Since they are special buildings, adversaries could want to obtain data stealing unprotected devices (e.g. lost employer device)
SB	29	Since they are special buildings, adversaries could want to try to spill information from employers' devices
SB	30	Special buildings work with employers, that can inadvertently expose critical information
BDC	-	-
SCADA	11	Due to the advanced capabilities to retrieve data also from mobile devices, adversary can use these connections to lead attacks exploiting vulnerabilities of phones and tablets
SCADA	25	Due to the advanced capabilities to retrieve data also from mobile devices, adversary can use these way to get information or damage operations using unattended devices
CP	5	Charging points are key components, so adversaries could want to deliver malware to compromise / observe key functionalities such as the energy consumption

Component	IRENE Index	Motivation
CP	9	Wrong configurations and permissions can give the attacker the chance to steal energy from city grid
CP	13	Charging points are key components, so adversaries could want to compromise the update process of a component
CP	24	Charging points are key components, so adversaries could want to obtain unauthorized access to energy consumption
CP	32	Since this component has a physical state, earthquakes can damage it
CP	33	Since this component has a physical state, fire can damage it
CP	34	Since this component has a physical state, flood can damage it
CP	35	Since this component has a physical state, hurricanes can damage it
CP	36	Charging points are key components with huge support of resources that degrade due to continuous usage
CP	37	Charging points are key components with huge information support systems (especially for authentication), so software could be affected by bugs that lead to vulnerabilities