



Improving the Robustness of Urban Electricity Networks IRENE

D2.2 — Societal impact of attacks and attack motivations

Document version: 1.0

Document status: Final

Project Document Date: 30/03/2016

Workpackage Contributing to the Project Document: WP2

Dissemination level: Public

Author(s):

Alexandr Vasenev, Lorena Montoya (University of Twente)

Andrea Ceccarelli, Tommaso Zoppi (University of Florence)

Oliver Jung (AIT Austrian Institute of Technology)

Anhtuan Le, Michael Chai, Yue Chen (Queen Mary University of London)

Tony Clarke (Ethos)



TABLE OF CONTENTS

1	Executive Summary.....	1
2	Introduction	2
2.1	Document structure.....	2
2.2	Technical context and objectives.....	2
2.2.1	Relations to Task 2.1.....	2
2.2.2	Relevant research projects in the domain of cybersecurity of smart grids	4
2.2.3	Novelties	5
3	Background: outages, cyber-attacks, and threat taxonomies.....	7
3.1	Brief overview of outages.....	7
3.2	Cyber attacks	9
3.2.1	Examples of attack vectors	9
3.2.2	Cyber-attacks: history and current trends	10
3.3	Approaches to consider threats to smart grids.....	12
3.3.1	Threat categorization by AFTER.....	13
3.3.2	Taxonomy of threats by SESAME.....	13
3.3.3	Taxonomy of threats from IRENE D2.1	14
4	Enhancing IRENE analysis with the FAIR approach.....	16
5	Root-cause analysis of non-malicious threat events.....	19
5.1	Environmental threats.....	20
5.2	Accidental errors and hardware and implementation threats	21
6	Analysis of external malicious threat events	22
6.1	Attackers.....	22
6.1.1	Motivation.....	22
6.1.2	Attacker taxonomies	25
6.1.3	Attack methods	29
6.2	Root-cause analysis of adversarial threats.....	32
6.2.1	Three classes of malicious actors.....	32
6.2.2	Relating classes of attackers to smart grid components.....	37
6.2.3	Analyzing adversarial threats as steps of kill chains.....	39
7	BayesianFAIR: Encoding Flexibility into FAIR Using a Bayesian Network Approach	43
7.1	Bayesian network approach to transform a structural analysis	43
7.2	Bayesian network approach to transform the FAIR framework.....	44
7.3	An exemplary application of the BayesianFAIR.....	46
7.3.1	Input to BayesianFAIR to find LEFs	46
7.3.2	The result of applying BayesianFAIR	47



8	Threat Navigator.....	51
8.1	Calculating LEF of threats for individual buildings.....	51
8.2	Possibilities to apply kill chains for other tasks.....	57
8.2.1	Identifying exposure of the city to adversarial threats and ongoing campaigns.....	57
8.2.2	Updating estimators.....	60
9	New accidental threats.....	61
9.1	Electromagnetic incidents.....	61
9.2	Physical-to-cyber and cyber-to-physical attacks.....	63
9.3	Mapping accidental threats.....	65
10	Disaster scenarios.....	68
10.1	Examples of disaster scenarios.....	68
10.2	An illustrative approach to consider Flood disaster scenarios.....	71
10.2.1	Likelihood of Flood Events.....	72
10.2.2	Flood Height.....	73
10.2.3	Relating water heights to grid components.....	77
10.2.4	Differentiating communication lines as overhead or underground cables.....	78
10.2.5	Illustrative case.....	82
11	Societal impacts.....	88
11.1	Critical Infrastructures to analyze societal impact.....	88
11.2	Infrastructure interdependencies.....	89
11.3	Impact of outages to nodes of other CIs.....	94
11.4	Costs of blackouts.....	102
12	References.....	107
13	Abbreviations.....	114
A	First Appendix. IRENE Threat Analysis.....	115
A.1	IRENE grid components (list from IRENE D2.1).....	115
A.2	IRENE threat events list attributed to threat actors.....	117
B	Second Appendix. IRENE Disaster Scenarios.....	120
B.1	Disaster scenarios based on some pre-selected disaster events.....	120
B.2	Disaster-relevant characteristics of power facilities.....	126
B.3	Disaster-relevant characteristics of care facilities.....	127



LIST OF FIGURES

Figure 1. Average number of power outages that establishments experience in a typical month between 2011 and 2015 [7].	7
Figure 2. Taxonomy of IRENE threat events	14
Figure 3. Adopted mapping of NIST constructs to FAIR threat factors	16
Figure 4. Relation of IRENE threat categories to grid components	19
Figure 5. Hacker Circumplex	24
Figure 6. NIST SP 800-115 attack sequence	30
Figure 7. Kill chain by Dell secureworks (from www.secureworks.com)	31
Figure 8. Components mapping: assigning buildings types to attacker classes based on their <i>Focus</i>	39
Figure 9. Kill chain based on categories of adversarial threats	39
Figure 10. Threat mapping: Assigning IRENE threats to attacker classes based on their <i>Capability</i>	40
Figure 11. Kill chains for different attacker classes	41
Figure 12. An example to concentrate on threats to a grid component	42
Figure 13. Illustration of the cause-effect relation and the parameter for transformation	45
Figure 14. The FAIR model with the factors' weight	48
Figure 15. Evaluation of LEF by Bayesian-FAIR with limited state input of the <i>Action</i> factor	49
Figure 16. Initial stage of the grid	52
Figure 17. Ranking groups of threat events	57
Figure 18. Structure to consider physical results of cyber attacks	65
Figure 19. Overview of impacts of threats from cyber- and physical- domains	66
Figure 20. Exemplary structure of a Hazus report on flood events	74
Figure 21. Hazus Flood model schematics	75
Figure 22. Clustering European countries according to technical characteristics of the network [65]	78
Figure 23. Grid components wrt to ‘flood protection’ and ‘height of the equipment’	81
Figure 24. Activity diagram to identify components of city electricity network that stay operational during a flood	81
Figure 25. A fragment of the Naperville's electricity grid	83
Figure 26. Infrastructure interdependencies [75]	90
Figure 27. Dependencies and influences of interruptions lasting less than two hours [76]	93
Figure 28. Dependencies and influences of interruptions lasting more than one week [76]	93

**LIST OF TABLES**

Table 1. Some characteristics of outages	8
Table 2. Outages with large impact	8
Table 3. Guideline for analysis of <i>Contact</i> factor by FAIR.....	17
Table 4. A look-up table to derive Loss Event Frequency.....	17
Table 5. Dependency of ENV threats based on external/internal grouping.....	20
Table 6. Dependency of HI threats	21
Table 7. Dependency of ACC threats	21
Table 8. Threats to critical infrastructures [31].....	23
Table 9. Cross-comparing different motivation taxonomies	32
Table 10. Grouping malicious actors	34
Table 11. Linking motivation to classes of external malicious actors	35
Table 12. Encoding <i>Focus</i> and <i>Capabilities</i> of C1-C3 actors into FAIR constructs.....	36
Table 13. Relating classes of malicious actors to grid components.....	38
Table 14. Categories of adversarial threats.....	39
Table 15. List of cyber threats to consider a factory within a smart grid evolution step.....	46
Table 16. The individual effect vector for factors in the FAIR model	48
Table 17. Numerical results of the BayesianFAIR to compared to FAIR	48
Table 18. Attacker classes relevant to the factory feature	52
Table 19. Threats relevant to the factory feature	53
Table 20. Threats and mitigations relevant to the factory feature	54
Table 21. Operationalizing threat parameters as FAIR constructs	55
Table 22. Identifying degree of implemented controls as a FAIR construct	55
Table 23. Exposure of the grid to attacks from specific actor classes	59
Table 24. Selected disaster events.....	70
Table 25. Elements of table flElectricPowerFlty [64, pp. F-203].....	76
Table 26. An exemplary disaster scenario for a simple grid in case a flood event.....	85
Table 27. An exemplary disaster scenario in case the grid is highly developed.....	86
Table 28. Disaster scenarios for other grid evolution steps	86
Table 29. Indicative list of critical infrastructure sectors.....	88
Table 30. Critical infrastructure dependencies for interruptions for less than two hours [76]	91
Table 31. Critical infrastructure dependencies for interruptions of more than one week [76]	92
Table 32. Mobile communications.....	94
Table 33. Landline	95
Table 34. Internet	95
Table 35. Data networks	95
Table 36. Water supply	96



Table 37. Sanitation	97
Table 38. Transportation systems	98
Table 39. Refineries	99
Table 40. Petrol stations.....	99
Table 41. Hospitals	100
Table 42. Impact of power outages on the industry.....	101
Table 43. VoLL for households, firms and government in the Netherlands (2001) [81]	104
Table 44. Comparison of WTA and WTP €/kWh estimates by time of outage [83] converted from £/MWh assuming 1 £ = 1,18 €.....	105
Table 45: Estimate of electricity UK VoLL for commercial and industrial users, (based on 2011 data) [83] converted from £/MWh assuming 1 £ = 1,18 €.....	105
Table 46. Outage case studies [84]	106



1 EXECUTIVE SUMMARY

This document is the second report of WP2 “Threat and Risk Analysis”. It describes activities performed within Task 2.2 “Societal impact of attacks and attack motivations” based on the outcome of T2.1 “Threats identification and classification” reported in the [IRENE Deliverable 2.1](#) [1]. Specifically, the T2.2 activities reported herewith included: identifying possible root causes of threats listed in D2.1, profiling attackers in connection to their modus operandi, identifying new accidental threats and cascading effects from natural disasters, and considering the societal impact of blackouts.

The target audience for this deliverable are those interested in analyzing threats to future urban electricity networks. The deliverable is also a useful reference for the wider group of stakeholders who have a vested interest in cybersecurity of cyber-physical systems. Readers with different interests can refer to specific sections of this report.

The deliverable starts with Section 1 that relates T2.2 to other research projects and describes novelties reported in this deliverable. This section can be of interest to readers who want a general understanding of the work conducted in relation to this body of knowledge. Section 3 briefly describes the topic under consideration and lists the state of the art approaches to consider threats to smart grids. Sections 1 and 3 together are relevant to readers interested in the state of the art.

Sections 4 – 9 are fundamental to this deliverable. Section 4 outlines the adopted approach of analysing the NIST-originated list of threats with the help of the FAIR (Factor Analysis of Information Risk) methodology. Then, the report describes the root cause analysis of non-malicious (section 5) and malicious (section 6) threats. Appendix A combines the outcomes of these sections. Section 7 introduces one of the novel contributions of this report: an approach to encode the FAIR constructs and relations into a Bayesian network named *BayesianFAIR*. Section 8 proposes *the Threat Navigator method* to rank and group threats for future urban grids based on their Loss Event Frequencies (LEF). This method constitutes the second contribution of T2.2. Section 9 outlines how new accidental threats to current and future smart grids can be considered.

Sections 10 and 11 concentrate on how threat events can impact the city. Section 10 describes how disaster scenarios can be developed based on specific disaster events, assumptions about the future grid and its context, and possibilities that failures can propagate through the grid. It introduces *a modelling approach for addressing the impact of a flood on the grid* — the third contribution described in this deliverable. This section aims to inform readers interested in infrastructure analysis. Section 11 outlines methods to account for societal impacts of outages and can be relevant to readers concerned with societal impacts.

The research outcomes of T2.2 activities will be integrated into other IRENE work packages.



2 INTRODUCTION

According to the IRENE research proposal, Task 2.2 “will perform an identification of the possible root causes of the identified threats, including the profiling of the potential attackers (motivations, funding, objectives, skills, etc.), possible new accidental threats and potential cascading effects from natural disasters, evaluating the societal impact of the identified attacks/disruptions. This will provide an attack threats’ databases that can be used to support risk assessment activities in smart grids. This includes an in-depth review of literature on modus operandi in general, attacker motivation in particular and in methods to combine expert knowledge when data is either not available or unfeasible to collect given time or financial constraints.”

2.1 DOCUMENT STRUCTURE

This section starts with the background of this research by providing an overview of recent outages and introduces the role of cybersecurity in the light of modern and emerging threats. Approaches to consider threats are briefly outlined next. Afterwards, threat analysis starts by considering non-malicious threat events, such as natural disasters and hardware failures. Analysis of adversarial threats follows. Later, we introduce a way to calculate Loss Event Frequencies (LEFs) for IRENE threat events. We illustrate its application within the Threat Navigator method to group interrelated LEFs for threats relevant to different classes of attackers. Afterwards, we point out several accidental low frequency threats that could lead to high impacts. Finally, we consider how disaster scenarios can unfold within a city and how blackout impacts can be calculated.

This report can be of interest to different readers. Those interested in the state of the art can refer to sections 1 and 3. Specifically, subsections 2.2.2 and 2.2.3 positioning the novel contributions of this report to other research projects. Section 4 outlines the risk taxonomy adopted within the deliverable. Sections 5 – 11 reports on specific T2.2 *activities*. These activities are linked to the report sections as follows:

- *Identification of possible root causes of D2.1 threats* are described in section 5 and 6. *Profiling of attackers* (based on the modus operandi reported in 6.1) is outlined in 6.2;
- Sections 7 and 8 employ outcomes of the previous sections and propose novel technical contributions on how to rank external malicious threats;
- Possible *new accidental threats* are overviewed in section 9;
- *Cascading effects from natural disasters* are illustrated in section 10;
- *Societal impacts* and ways of their calculations are considered in section 11.

2.2 TECHNICAL CONTEXT AND OBJECTIVES

2.2.1 Relations to Task 2.1

Together T2.2 and T2.1 constitute IRENE’s Work Package 2. This aims to “conduct a holistic (physical and cyber) smart grid (ICT & grid) security analysis”. As T2.2 builds on the [T2.1 output](#), this subsection outlines work previously conducted as part of the work package. For adequate threat analysis, D2.2 considers several state of the art threat taxonomies, including NIST 800-30, Octave, and the Open threat taxonomy.



T2.1 activities published within the [IRENE D2.1 deliverable](#) [1] investigated threats as cyber-security vulnerabilities resulting from the interconnection of previously unconnected grid system parts as well as the inclusion of new sensor and actuator devices in the Smart Grids.

In T2.1 we constructed a set of relevant future urban grid components to consider and consequently accounted for different plausible scenarios of future city dynamics (D1.1). Based on this, we envisioned possible future grid scenarios, focusing on a scenario involving a restricted number of grid components represented through an evolution story. In particular, we selected the following set of smart grid components (listed in Tables 5 and 6 in [1]) as functional grid elements relevant for a city-level analysis:

- Connection: Electricity Connection, Data Connection, Micro Grid Connection, Connection Adapter, Power Substation, Long-Range Connector;
- Energy Provider: Power Plant, Photo Voltaic Generator, Wind Farm;
- Building: Factory, Hospital, Stadium, Offices, Office Districts, Smart Home, Smart Building;
- Data Center: Basic Data Center, SCADA.

The relevant threats list built in T2.1 was derived from *NIST Special publication 800-30*. Since NIST SP800-30 aims to guide the conduction of risk assessments of federal information systems and organization, it is suitable for conducting risk assessment and can inform the task of identifying threats relevant to future smart grids. The NIST document outlines 102 threats organizing them depending on the threat source, which can be either “adversarial” or “non-adversarial”. However, some of these threats are too specific for the chosen IRENE abstraction level. For example, it could be difficult to distinguish between the “Conduct simple Denial of Service (DoS) attack” and the “Conduct Distributed Denial of Service (DDoS) attacks” as separate threat events. Therefore, we adapted this list to the chosen level of abstraction, resulting in a list of 38 (instead of NIST’s 102) threat events. In our list, each event belongs to a threat source category as follows:

- Adversarial:
 - a. Perform reconnaissance and gather information;
 - b. Craft or create attack tools;
 - c. Deliver/insert/install malicious capabilities;
 - d. Exploit and compromise;
 - e. Conduct an attack (i.e., direct/coordinate attack tools or activities);
 - f. Achieve results (i.e., cause adverse impacts, obtain information);
 - g. Coordinate a campaign.
- Non Adversarial:
 - a. Environmental;
 - b. Accidental;
 - c. Structural.



Using the scenarios of grid development and the IRENE threats list we conducted a step-by-step analysis of future grids following the NIST SP800-30 guidelines. As mentioned in D2.1, this approach offers several advantages:

- it is fully compliant with the NIST 800.30 standard;
- the generality makes the threat analysis outcomes reusable in other contexts that have common features;
- observing evolution is simpler if new connections between the added and the existing components are considered step-by-step;
- the final threat analysis consists of the conclusions drawn in the analysis of each incremental step in the evolution of the grid where for each step we consider a possible set of changes in the grid (assets added/removed/changed) due to decisions made by authorities or citizens.

We used the scenarios described in D1.1 as input for the threat identification process, which aimed to highlight all the threats that could emerge in a scenario due to several modifications of its connected components. The relevant example could be adding or removing a component, e.g. a hospital, from the grid.

T2.1's outcome (i.e. D2.1) provided several inputs for T2.2. For example, the IRENE threat list constitutes an input for root-cause analysis, while adversarial threat event categories are used for constructing kill-chains of different malicious threat actors based on their capabilities. The scenarios and the components listed in D2.1 link classes of attacker and grid features. Threat events and their mitigations outlined in D2.1 are used to account for Loss Event Frequencies. Multiple other connections can also be identified throughout this document.

In short, T2.1 provided a possible future reference city scenario that could be used in the rest of the project for threat analysis, architectural or behavioral evaluation. The scenario allows reasoning about outages and possible techniques that can be implemented to enhance the resiliency of the city to outages that could affect it, as described in the following sections.

2.2.2 Relevant research projects in the domain of cybersecurity of smart grids

This subsection briefly overviews several projects dealing with topics similar to this deliverable. This introduction aims to position the deliverable within a larger body of literature and highlights the differences.

A number of research projects in the area of smart grids were outlined in deliverable D1.6 of the currently ongoing SPARKS project (smart grid protection against cyber-attacks). In addition to the assessment of trans-national (European) research activities, that deliverable focused on trans-national (EU funded) regional research activities and endeavors. The deliverable listed 14 projects on the topic of smart grids. Within T2.1, we considered the list to identify projects that highlight relevant issues. From the list, the VIKING, SoES, CRISALIS, and AFTER projects were selected. Additionally, we considered research conducted with the SESAME project, which provided an extensive classification of threats to smart grids. These projects are outlined shortly here.



VIKING [2] studied the whole control system from the measurement points over the communication network to the central computer system. Potential targets for cyber-attacks included: workstations for operators, firewalls between SCADA LAN and office LAN, system vendors, substations LAN, stations within office LAN, communication networks between substation LANs and SCADA LAN, and a firewall between office LAN and Internet WAN. Also, the project took a model-based approach to investigate SCADA system vulnerability. The models were employed to assess the effect on SCADA system behavior by cyber-attacks. The four step modeling approach included steps related to attacks, SCADA systems, power networks and societal cost. To calculate the latter, a virtual society simulator was developed. As the project had a more technical focus on the control system, it differs from the IRENE approach that concentrates on islanding.

CRISALIS [3] provides new means to secure critical infrastructure environments from targeted attacks, carried out by resourceful and motivated individuals. The project illustrates a possible attack scenario using a testbed and it focuses on a) detection of vulnerabilities and b) attacks in critical infrastructure environments.

AFTER [4] focusses on the need for vulnerability evaluation and contingency planning of the energy grids and energy plants considering also the relevant ICT systems used in protection and control. Since one of its objectives is to develop a methodology for risk assessment of the interconnected Electrical Power Systems, it shares some topics of interest with IRENE. Later in this deliverable we illustrate how IRENE is aligned with the threat taxonomy of AFTER.

SESAME [5] developed a Decision Support System (DSS) for the protection of the European power transmission, distribution and generation system. SESAME provided a list of prolonged outages and made models to calculate outages on regional levels. The taxonomy of threats for the smart grid introduced in SESAME D1.1 “Analysis of historic outages” (to be outlined later) is particularly relevant for IRENE since the goals of both projects are well aligned: SESAME aims to contribute to developing tools and a regulation framework for the security of the European power grid against natural, accidental and malicious attacks. The IRENE taxonomy of threats could be further elaborated (if needed) by considering the SESAME view on threats, as it has several relevant ramifications.

SOES [6] is also concerned with ICT security in energy smart grids. Deliverable D4 considers a number of threat/attack targets for four use cases (voltage control, photovoltaic generation and storage control, load reduction programs, and smart meter configurations). The project scope overlaps with IRENE in terms of distributed energy resources and interfaces between nodes. It includes threat analysis components, which will be later briefly described in this deliverable together with the list “Best practices in identifying threats” to illustrate how the present deliverable relates to them. However, SOES’ technical focus on different network and communication protocols makes the list of threats less relevant to this deliverable.

2.2.3 Novelties

Novelties reported in this deliverable include suggestions on: (1) how to employ a Bayesian network based on the Factor analysis of information risk (FAIR) methodology for calculating Loss Event Frequencies of malicious threats; (2) how to group and rank malicious threats with respect to smart grid components using kill chains; and (3) how to address a flood disaster scenario. In this way, this



deliverable analyses threat-to-threat and threat-to-component relations for adversarial (section 6) and for non-adversarial (sections 5) threat events.

Specifically, the first contribution is the method named **BayesianFair**: a mechanism to calculate Loss Event Frequencies of malicious threats. This mechanism can combine expert knowledge, even if threat-related parameters (*Contact*, *Action*, *Threat Capability*, and *Control Strength*) are uncertain. The second contribution is the **Threat navigator**: a method to concentrate on specific threats to this deliverable. It builds on threat sequences and employs an outcome of root cause analysis of threat events in relation to modus operandi of malicious actors. The third contribution complements the analysis of malicious threats by addressing how a disaster scenario could develop from a non-adversarial threat event. We describe a **modeling approach for addressing the impact of a flood on the grid**, thus leading to the interruption of the supply of bulk produced electricity to clients. Our approach accounts for interactions between the context and the grid itself and inter-relates some disaster event characteristics and grid topology. Grid nodes properties and connections between nodes are considered with respect to flood height.

3 BACKGROUND: OUTAGES, CYBER-ATTACKS, AND THREAT TAXONOMIES

3.1 BRIEF OVERVIEW OF OUTAGES

Power outages can be experienced virtually everywhere in the world, affect multiple energy consumers, and last for prolonged periods of time. World Bank has extensively covered the topic of how customers in different countries are affected by (re-occurring) blackouts.

Given the crucial role infrastructures play on enterprises, World Bank Group (WBG) aggregated data from surveys of more than 130 000 firms from 135 countries to illustrate the quality of infrastructures worldwide. Figure 1 illustrates that outages are experienced worldwide including in Europe.

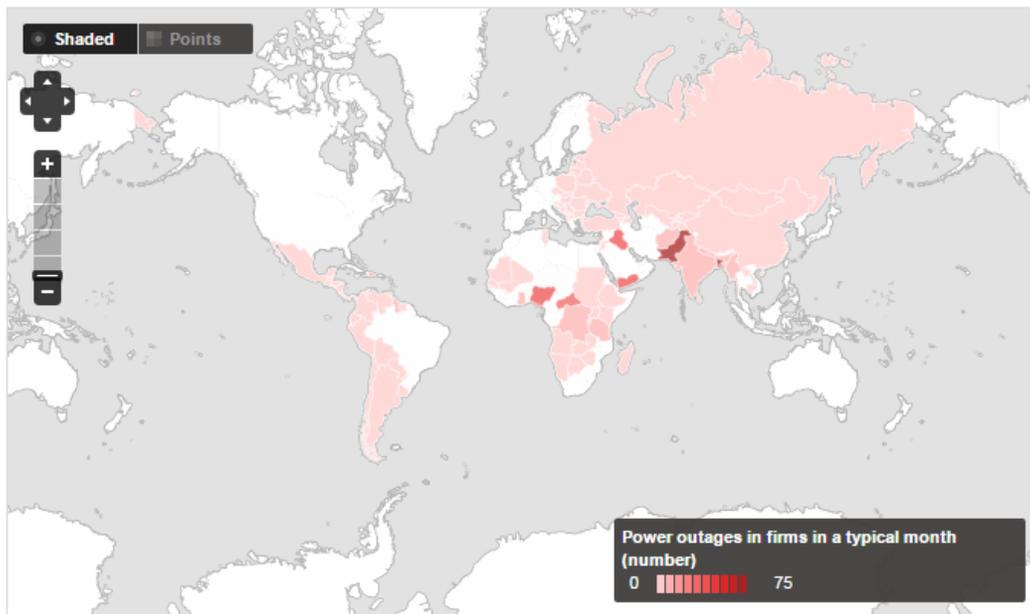


Figure 1. Average number of power outages that establishments experience in a typical month between 2011 and 2015 [7].

The WBG employs thirteen relevant indicators to describe different aspects of outages, including: “Number of electrical outages in a typical month”; “If there were outages, average duration of a typical electrical outage (hours)”; and “Percent of firms owning or sharing a generator”. An excerpt from the WBG database is shown in Figure 1.

Table 1 shows that in some countries the frequency of outages is high (up to 25.4 numbers of outages in a month) or that the outages can be long-lasting (e.g. 9.7 hours for firms in Middle East & North Africa). More indicators, together with their descriptions, can be accessed online [8].



Table 1. Some characteristics of outages

	Number of electrical outages in a typical month	If there were outages, average duration of a typical electrical outage (hours)	Percent of firms owning or sharing a generator
High income: OECD	0.4	2.9	13.1
East Asia & Pacific	4.4	6.4	36.4
Middle East & North Africa	17.6	9.7	41.0
South Asia	25.4	5.3	45.4

It is noticeable that outages in OECD (Organization for Economic Co-operation and Development) countries are not uncommon. For instance in the US the five-year annual average of outages doubled every five years between 2000 and 2013, leading to 130 reported grid outages during the first six months of 2014 [9].

Detailed information on registered outages can be found at the US Department of Energy website (energy.com). Their latest Electric Disturbance Events (OE-417) [10] report lists 18 disturbances in December 2015 alone. The largest one, due to severe weather, affected 168,000 customers. That outage took place on 24 Dec 2015 and lasted from 3 AM until 12 AM. Other blackouts in December 2015 were attributed to system operations, vandalism, and sabotage; similar to others that led to outages during earlier months.

In addition, the scale of prolonged outages may impact millions of people (refer to Table 2).

Table 2. Outages with large impact

Date	Event Description	Impact
26 January 2015	terrorist attacks left 80% of Pakistan without power	some 140 million people
27 March 2015	a technical problem in one of the main power grids in North Holland	1 million households didn't not have power for at least one hour
Jan-Feb 2008	winter storms in China	nearly two-week blackout affected 4.6 million people around the central Chinese city of Chenzhou
14-15 August 2003	Southeast Canada and eight Northeastern U.S. states	50 million people were inconvenienced for up to two days in what turned out to be the biggest blackout in North American history. 11 people died and there was a reported \$6 billion in damages.
2012 (throughout)	US Northeast experienced 10 outages	each outage longer than 175 hours



Outages are therefore not uncommon and since the grid is a critical infrastructure, millions of people can get affected. Novel technologies should be used to reduce the impacts of present and future outages. However, with the increasing utilization of information technologies, the grid becomes not only more resilient, but also more exposed to cyber-threats — a phenomena less observed earlier. Thus, grid evolution needs to be considered in connection with threats to novel technologies. The next section briefly illustrates such.

3.2 CYBER-ATTACKS

Continuous electricity supply is often critical to business operations and services. An accident in a smart grid IT layer can therefore have a significant effect and cause “not only disruption to business operations and services but also potential damage and destruction of equipment, and injury to people” [11]. Given its importance, identifying possible attack vectors for smart grid elements has received considerable attention from both academia and industry.

3.2.1 Examples of attack vectors

Potentially, any connection between smart grid system components, as well as components themselves, can be a target for malicious attack. At a high level, it can be illustrated using Control Theory constructs, where either connections or components can be targets.

According to the Control Theory [12], **Sensor**'s *measured output* is combined with a *reference value*, which results in a *measured error*. A **controller** receives the error value and amplifies it to obtain the *system input*. A **system** (that can be called a plant within control theory terms) processes this value into a *system output*, which then serves as an input to the sensor. Within this structure, sensors, controllers, and systems are components that can be attacked. Connections between them, including measured output, reference value, measured error, system input, and system output can also be targeted.

Because instantiations of connections or constructs of the Control Theory form communication lines and nodes within a smart grid, the control theory view on the grid can be seen as a framework for mapping many different threats to a control system architecture. For example, smart grid elements, including storage and data recall capabilities, can suffer from a multiplicity of attacks that aim to disrupt or degrade the connections. Sensor measurements or reference values can be substituted to provide erroneous measured error to the controller. Finally, if the rate or data exchange between the grid components is reduced, the system can fail to adjust adequately to changes in electricity supply and demand.

Several examples show how attacks on smart grid can render it dysfunctional. For instance, one research described several attacks on a substation control infrastructure [13]. These attacks included a viral infection of the remote control center. Besides, two DoS scenarios have been implemented and analyzed on the CESI RICERCA testbed: one targeting the Substation Web Service and one directed at the VPN connecting the local site to its Remote Control Centre.

Another example [14] describes how a cyber-attack that involve fabricating or tampering with the sensor information can lead to incorrect decision-making for load management. In a simplified case of one generator and two loads, fabricating the sensed data can cause the system to drop both loads or lead



to apparent demand that exceeded generation. The latter could lead to a decrease of generator frequency and a possible trip out.

EU CRISALIS (Securing critical infrastructures) [3] elaborated an opposite case when a system can be led to overloading the grid by producing more electricity than the users demand. When the system is in a safe state, the process control guarantees the correct voltage on the grid. However, the proper feedback may be not functioning as a result of a cyber-attack. By leveraging the lack of an authentication schema an attacker could change input and outputs of the Programmable Logic Controller. As a result, the process control can start asking the power plant for more energy without any new load introduced into the grid. The overall effect of this attack is an overvoltage of the grid.

As well as individual components attacks can target multiple devices at the same time; such as smart meters. The potential for sabotage a significant portion of a grid was demonstrated at the 2009 and 2014 Black Hat conferences. Specifically, manipulating smart meters by exploiting encryption problems in Power-line Communication technologies could result in blackouts [15].

Altogether, the described projects illustrate a number of possible attack vectors that target grid components and aim at disrupting the control feedback loop. Other research further extends this list and highlights how a cyber-attack can physically damage a generator [16] and that a coordinated attack can exhibit itself in both cyber and physical domains [17]. Although these attacks are as yet seldom observed in practice, previous cyber-related incidents suggest that a motivated and capable attacker could exploit these scenarios.

3.2.2 Cyber-attacks: history and current trends

A short overview of cyber incidents showing how the topic of countering cyber-attacks is highly relevant for smart grids, given possible impacts of attacks, ongoing cyber campaigns, and current threat landscapes. The following list briefly outlines possible impacts of cyber-related incidents selected from <http://www.risidata.com/>:

- Siberian Pipeline Explosion in 1982 is possibly the first known cybersecurity incident involving a critical infrastructure. Intruders planted a Trojan in the SCADA system that controls the Siberian Pipeline. This caused an explosion equivalent to 3 kilotons of TNT;
- In Maroochy Shire, Queensland, Australia a disgruntled ex-employee hacked into a water control system in 2000 and flooded the grounds of a hotel and a nearby river with a million liters of sewage. It can be seen as a series of attacks over a prolonged period rather than as an individual attack;
- In 2010 it was discovered that a worm dubbed Stuxnet had struck the Iranian nuclear facility at Natanz. Stuxnet used ‘zero-day vulnerabilities’ (vulnerabilities not known before, so there is no time to develop and distribute patches). The worm employed Siemens’ default passwords to access Windows operating systems that run WinCC and PCS7 programs. The worm hunted down frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland;



- In 2012 one of the two nuclear reactors at the Susquehanna Nuclear Powerplant was shut down because a computer system controlling the reactor's water level was not functioning properly. The reactor was shut down manually by operators when they identified the malfunction;
- In 2012 a virus infection was discovered in a turbine control system at a U. S. power plant. The infection ultimately impacted approximately 10 computers on the control system network. The infection was responsible for downtime for the impacted systems and delayed the plant restart by approximately 3 weeks.

Cyber incidents do not necessarily represent isolated events, but can form continuously ongoing malicious campaigns. Exemplary description of two ongoing campaigns against industrial control systems are provided at US ICS-CERT (Industrial control systems cyber emergency response team) website:

- In 2014 US ICS-CERT alerted about an ICS Focused Malware campaign [18]. The campaign included phishing emails, redirects to compromised web sites, and trojanized update installers on at least 3 industrial control systems (ICS) vendor web sites, which constitute watering hole-style attacks;
- In Feb 2016 US ICS-CERT revised their earlier alert about a sophisticated malware campaign compromising ICS that can be dated back since at least 2011. As reported, this campaign compromised numerous industrial control systems environments using a variant of the BlackEnergy malware [19]. Users of HMI (human-machine interfaces) from various vendors, including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC, have been targeted. Recently, it was suggested by ESET experts that a variant of this software, named BlackEnergy Light led to blackout experienced in Ivano-Frankivsk region in Ukraine [20]. E-ISAC confirmed [21] that a variety of techniques like spear fishing e-mails, BlackEnergy Malware were used to gain access to the SCADA system, disconnect substations, and impede grid recovery leaving 225.00 people without electricity for several hours.

These (and others) malicious campaigns lead to a sharp increase of attacks on smart grids. For example, Dell Security reports that cyber-attacks on supervisory control and data acquisition (SCADA) systems are sharply increasing. Specifically, in 2014, Dell reported a 2X increase in SCADA attacks compared with 2013: worldwide SCADA attacks increased from 91,676 in January 2012 to 163,228 in January 2013, and 675,186 in January 2014 [22]. The majority of these attacks targeted Finland, the United Kingdom, and the United States, as SCADA systems are more common in these regions and more likely to be connected to the Internet. For instance, 202,322 SCADA attacks were witnessed in Finland. In the US, according to US Department of Homeland Security, the energy industry was the most heavily targeted sector of all throughout 2014 (with 32% of attacks targeting this sector compared to others) [23]. Dell highlights that buffer overflow vulnerabilities are the primary attack method (accounting for 25% of the attacks), followed by 'improper input validation' and 'information exposure' (9% each). Among others, 'permission, privileges, and access control' and 'cryptographic issues' were attributed with 7.4% and 5.8% correspondingly.



Analysis of significant recent changes in threat landscape can be seen in the ENISA (European Union Agency for Network and Information Security, www.enisa.europa.eu) report. This report looks at threats to cyber-physical system (CPS) as “engineered systems that interact with computing equipment being seamlessly integrated to control, manage and optimize physical processes in a variety of areas from traditional engineering science”. With a recently identified sophisticated malware that can alter imbedded software, the top ten emerging (and continuing to increase) threats to CPS in 2015 includes [24]:

1. Malware;
2. Cyber-espionage;
3. Physical damage/theft/loss;
4. Insider threat;
5. Web based attacks;
6. Web application attacks;
7. Phishing (as instrument to infect IT and affect CPS);
8. Spam (as instrument to infect IT and affect CPS);
9. Denial of Service;
10. Information leakage.

Applied to smart grids, this list outlines threats that can be part of a larger campaign and, through hampering functionality of the control feedback loop, lead to blackouts.

The list can also constitute as an initial categorization of threats. For example, the top four threats outline different directions of possible attacks by including cyber (threats 1, 2, 4) and physical attacks (threat 3). Internal (threat 4) and external nature of attacks (specifically, threats 1 and 2) provide another dimension. In this way, this list reflects common threat taxonomies useful for analyzing threats. The next subsection outlines such taxonomies in more detail. Later, the report applies them to analyze root causes of threats.

3.3 APPROACHES TO CONSIDER THREATS TO SMART GRIDS

A number of methodologies, such as CORAS, CRAMM, and OCTAVE, can inform the task of threat analysis, because such a relevant component of threat categorization is naturally embedding into all major methodologies. At the same time, some approaches specifically concentrate on threat categorization in general or on threats to smart grids. An example of the first type of approaches can be found in the Threat agent risk assessment (TARA) method described by Intel [25]. This method is applicable to risk assessment of information technologies in general. TARA concentrates on threat agents and their motivations, methods, and objectives, and how they map to existing controls, but do not specifically concern the weak points themselves.

A number of categorization of threats relevant to smart grids can be found in specialized research publications as well (e.g. AFTER and SESAME).



3.3.1 Threat categorization by AFTER

FP7 project AFTER ("A Framework for electrical power systems vulnerability identification, defense and Restoration") categorized threats using a major differentiation between physical and ICT threats followed by further subdividing these classes into External and Internal threats. These threats were projected as either Natural or Man-related threats:

- Physical:
 - a. Natural:
 - External (Lightings, fires, ice/snow storm, solar storms);
 - Internal (Component faults, strained operating conditions);
 - b. Man related:
 - External (Unintentional damage by operating a crane, sabotage, terrorism, outsider errors);
 - Internal (Employee errors, malicious actions by unfaithful employees);
- ICT threats:
 - c. Natural:
 - External (Ice and snow, heavy flood, fire and high temperature, geomagnetic storm);
 - Internal (Operation out of range, internal faults, ageing);
 - d. Man related:
 - External (Hacker, sabotage, malicious outsider);
 - Internal (Employee errors, malicious actions by unfaithful employees, software bugs).

This high level differentiation provides a first step for categorizing adversarial and non-adversarial threats. While this can be useful for some applications, a more advanced approach could be needed to differentiate between different natural disasters and parts of the grid.

3.3.2 Taxonomy of threats by SESAME

A more extensive taxonomy of threats was provided in 2011 within the FP7 SESAME (Securing the European Electricity Supply Against Malicious and Accidental Threats) project. Deliverable D1.1 "Analysis of historic outages" [26] states that SESAME differentiates splits outages into four parts: pre-condition, origin, chain of events and end. The project outlines different aspects of threats, events, effect, and phenomena developed. A chain of events, encoded using abbreviations from these groups can describe major failures in power systems. Threats are classified as follows:

- Natural disasters:
- Geological disasters (avalanches, earthquakes, volcanic eruptions, landslides);
 - a. Hydrological disasters (floods, limnic eruptions, tsunamis);
 - b. Meteorological disasters (blizzards, cyclonic storms, droughts, hailstorms, heat waves, tornadoes, lighting, thunder, rainstorm);
 - c. Fires (wild fires);



- d. Health disasters (epidemics, famines);
- e. Space disasters (impact vents, solar flares, gamma ray burst);
- f. Contamination.
- Accidental threats:
 - a. Operational faults (design error, wrong decision, maintenance accident);
 - b. Equipment failures (technical failure, human and animal interference).
- Malicious threats:
 - a. Physical threats (terrorist attack, war act, sabotage);
 - b. Human threats (insider threats);
 - c. Cyber-threats (malware, terrorist hacking).

These threats can result in undesirable events related to the:

- Generation (e.g. generator trip, backup generator failure, turbine malfunction);
- Transmission (such as short circuit, power tower collapse);
- Transformation (transformer trip, switch malfunction);
- Distribution (underground cable malfunction, distribution line trip);
- Information, communication, and control system (cyber equipment break or cyber system hack).

Such a sophisticated classification covers a threat landscape in great detail. Although it can clearly help in structurally approaching threat analysis, its direct application for this deliverable seems to be less practical. First, due to its high level analysis, IRENE project may lack details to differentiate between hydrological and meteorological disasters and secondly, IRENE's accents on cyber components. As adversarial threats are more complex due to the adapting nature of attackers, it might require analysis of different classes of attackers that pose threats for a given malicious threat category. Therefore, it can be useful to focus on adversarial and non-adversarial threats when considering the high level of the IRENE classification.

3.3.3 Taxonomy of threats from IRENE D2.1

Task 2.1 and [deliverable D2.1](#) of the IRENE project considered the differentiation of threats in line with NIST 800-30. Figure 2 represents the underlying taxonomy of threats.

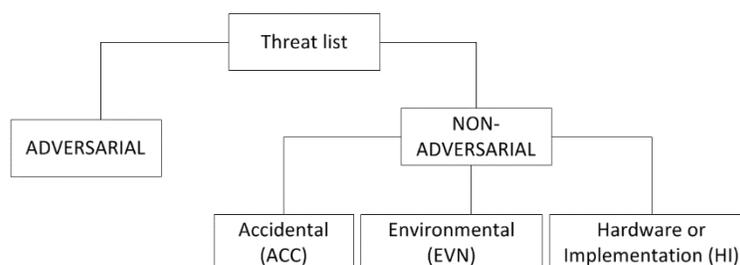


Figure 2. Taxonomy of IRENE threat events



This can be elaborated with the help of the NIST 800-30 document (Appendix D, p. D-2) as follows:

- Adversarial (such as an individual, outsider, insider, trusted Insider, privileged Insider, competitor, supplier, partner, customer, nation state). These sources are characterized by *Capability*, *Intent*, and *Targeting*. The sources seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies);
- Accidental (user or privileged user/administrator). These sources, as well as the rest of the sources in this list, are characterized by a range of effects;
- Structural (including IT Equipment, storage, processing, communications, display, sensor, controller, environmental and temperature/humidity controls, power supply, software, operating system, networking, general- and mission-specific applications). This category is related to failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters;
- Environmental (natural or man-made disaster, fire, flood/tsunami, windstorm/tornado, hurricane, earthquake, bombing, overrun, unusual natural event (e.g., sunspots), infrastructure Failure/Outage, telecommunications, electrical Power). This category concerns natural disasters and failures of critical infrastructures which the organization depends on, but which are outside its control.

The previously mentioned taxonomies share some similarities, while differently categorizing threats in general. While the AFTER taxonomy explicitly considers physical and cyber-threats to the grid on a high level, SESAME looked at natural, accidental, and malicious threats within the first categorization step. In addition, the SESAME taxonomy elaborates well on threats relevant to natural disasters. The IRENE categorization, as stemming from an information security standard, concentrated more on cyber-threats and initially differentiated adversarial and non-adversarial threats.

This interrelation of taxonomies highlights their differences and opportunities for adjustments, if needed. For example, IRENE environmental threat events can be extended using the SESAME's detailed natural disaster list. Similarly, the IRENE list could account for different origins of threats to a smart grid as a cyber-physical system. This opportunity will be highlighted later in Section 9.

The next section outlines constructs of individual threats and describes how they are addressed within this deliverable based on the NIST classification and the FAIR (Factor analysis of information risk) methodology. Later, it analyses non-malicious and external malicious threats.

4 ENHANCING IRENE ANALYSIS WITH THE FAIR APPROACH

This deliverable analyses threats identified from the NIST standard within [D2.1](#) with the help of the FAIR (Factor analysis of information risk) methodology. This approach builds on a property of FAIR, i.e. being complementary to major risk assessments [27]; the key reason it was used. It is to analyze Smart Grid threats, for instance by Bell Labs Advisory Service. This subsection outlines constructs related to threat analysis and maps FAIR risk taxonomy by The Open Group to NIST 800-30.

FAIR provides a taxonomy of the factors that contribute to risk and how they affect each other. The risk is defined as “the probable frequency and probable magnitude of future loss.” For the purpose of threat analysis, this deliverable looks at Loss Event Frequency (LEF). Probable Loss Magnitude is addressed later in the section (i.e. how an outage can impact the city’s population).

Loss Even Frequency is subdivided into Threat Event Frequency and Vulnerability. The first construct includes *Contact* and *Action* factors. Threat event frequencies are thus constructed by relating probabilities of contacts between threat sources and the system (as characterized by *Targeting*), complemented by the attackers’ incentive to engage (*Intent*). Vulnerability deals with *Control Strength* and *Threat Capability*. This approach can be linked to NIST constructs as illustrated in Figure 3.

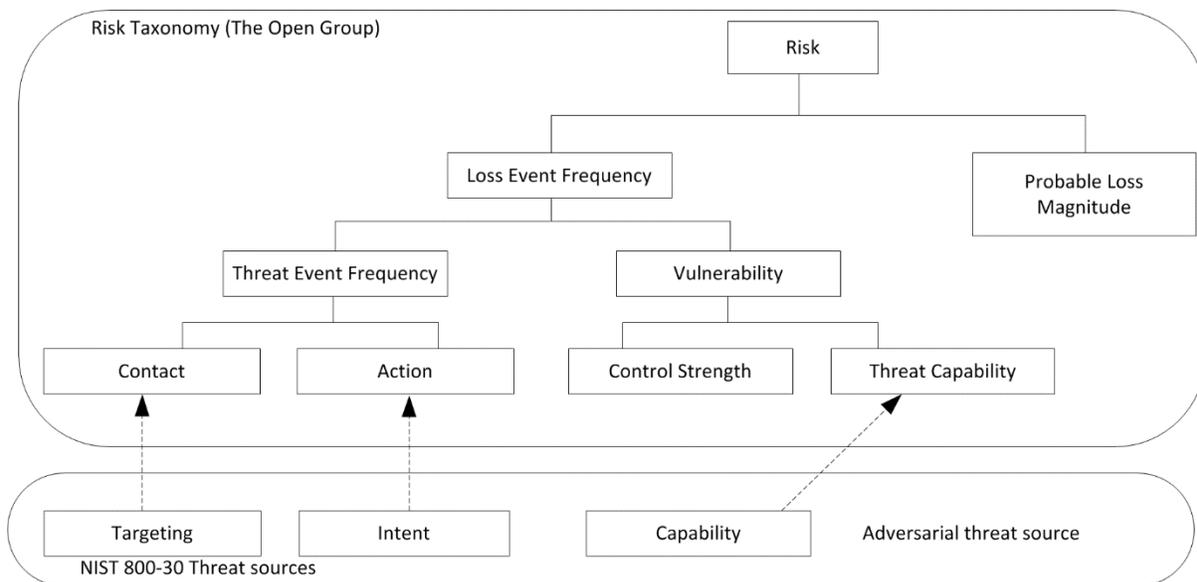


Figure 3. Adopted mapping of NIST constructs to FAIR threat factors

This report sees FAIR threat factors as being related to the NIST constructs. For example, FAIR defines vulnerability as “the probability that threat capability exceeds the ability to resist the threat” and suggests relating relationship with *Control Strength* and *Threat Capability*. NIST, instead, outlines that “A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness.” This definition mentions both threat source and controls in relation to each other.



Threat Event Frequency and *Threat Capability* describe the attackers’ side. They lend themselves well to designate both *malicious* and *non-malicious* threat origins. Natural disasters, such as flooding and hurricanes, can thus be considered in line with other threat events.

The *Threat Capability* construct can be related to natural disasters and malicious threats. For instance, in case of a hurricane the threat capability could be the wind speed and the threat event frequency can be derived from historical data. For malicious attacks the threat capability can describe specific resources available to cyber-attackers.

Control Strength outlines the strength of a control as compared to a baseline measure of force. In case of malicious attempts, the ‘defending’ side responsible for control measures in place is related to the ‘attacking’ side, which attempts to outperform the defenders. In case of natural disasters, *Control Strength* can be attributed to the ability of a structure to withstand strong wind. *Control Strength* can include specific measures that can limit success of malicious attackers’ actions.

FAIR encodes each threat factor by means of a five-point scale (i.e. Very Low, Low, Moderated, High, and Very High). For instance, a FAIR suggestion about how to consider the *Contact* factor is shown in Table 3.

Table 3. Guideline for analysis of *Contact* factor by FAIR

Rating	Description
Very high (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year

With known states of the causes, FAIR employs reasoning tables to look up for the state of the effect. Table 4 illustrates how to derive Loss Event Frequency (LEF) from the Threat Event Frequency (TEF) and the “Vulnerability” factors.

Table 4. A look-up table to derive Loss Event Frequency

		LEF				
TEF	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
		VL	L	M	H	VH
		Vulnerability (V)				



It should be noted that several methodologies and taxonomies account for differences between threat sources and threat actors. While this aspect is less highlighted within some methodologies, others employ it at the beginning of analysis. For example, this is a departure point for HMG Information Assurance Standard No. 1 [28], which is a standard method for assessing ICT systems that manage UK government information. A threat source is a person or organization that desires to breach security. A threat actor is a person who actually performs the attack. A threat source can also be a threat actor. The differentiation is useful because it allows to depict situations in which a person or organization outsources a task to a more skilled person or organization and can thus allow for such interactions.

Threat sources (disaffected or dishonest employees; terrorists; etc.) can be characterized by their capability level (from “very little” to “formidable”) and priority (“indifferent” to “focused”). Threat levels related to threat actors (e.g. a bystander; physical intruder; privileged User) reflect the combination of motivation (from “indifferent” to “focused”) and capability (from “very little” to “formidable”).

This deliverable adopts FAIR factors to account for IRENE threats identified within D2.1 and particularly concentrates on threat actors. Thus, we relate NIST’s *Targeting* concept to FAIR’s *Contact* concept. *Intent* is seen as being related to *Actions*. Together, *Targeting* and *Intent* (or in other words, *Contact* and *Action*) correspond to the *Focus* construct, which depicts a malicious actor(s) aiming at a specific object (e.g. a type of grid element). *Focus* represents an abstraction of Threat Event Frequency as a number. *Focus* is fundamentally different from NIST’s Capability (FAIR’s Threat Capability) of actors. Together, *Focus* and *Threat Capability* describe specific classes of threat actors.

The following sections analyze non-malicious threats (ACC and ENV), threat events caused by external malicious sources, and the societal impact of outages. Each section starts with review of literature on the topic and then analyses threat events outlined in D2.1. Later, the root-cause analysis of external malicious threats is provided.

5 ROOT-CAUSE ANALYSIS OF NON-MALICIOUS THREAT EVENTS

As the grid normally balances the electricity production and demand in real time, the factors that can negatively impact this balance need to be studied and understood. This section has a high level of abstraction and provides a short overview of how environmental (ENV), Accidental (ACC) and Hardware and Implementation (HI) threats identified in [D2.1](#) can depend on each other. This complements the individual view of non-malicious threat events (such as the one outlined within the SESAME taxonomy mentioned above).

Categories of Threats can be related to categories of grid components. For example, CRO Forum [29] illustrated how different blackout causes can be linked to blackouts due to increased demand, failure of transmission and failure of production. It is possible to apply the logic behind the case-effect graph of grid threats outlined in the CRO report to map IRENE threat categories to specific grid components. The result as an IRENE-specific mapping is demonstrated in Figure 4.

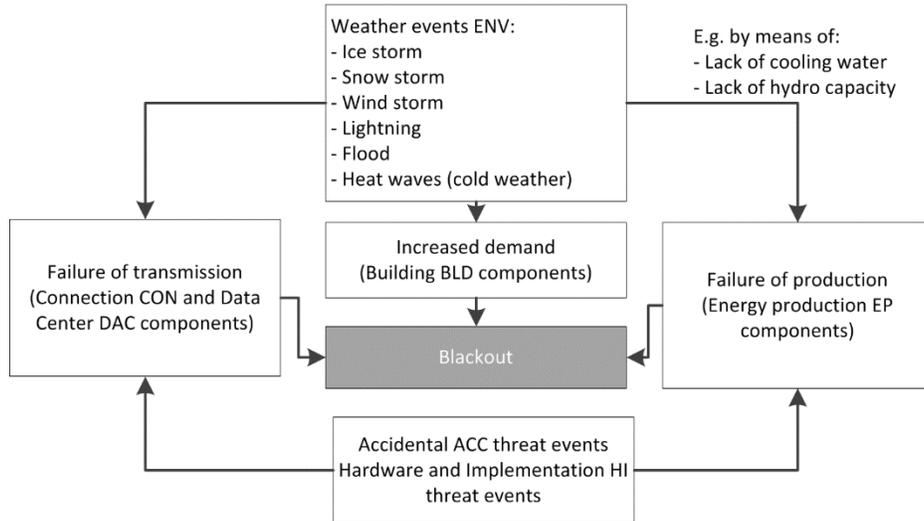


Figure 4. Relation of IRENE threat categories to grid components

Among threat categories, environmental (weather-related) threats can impact all classes of grid components. In unfavorable weather conditions the flexibility of the grid (for instance spared amount of generated reserves) is reduced. The weather can push the grid out of the generating and consumption balance, degrade functionality of components, and can result in the direct destruction of components. For example, weather can lead to a significantly increased demand for energy due to heat waves or cold weather, such as during an ice storm in the winter of 1998 in Montreal. In another example, the electricity production can be hampered due to weather. For instance, lack of water to cool down energy production stations during droughts can lead to a station blackout. Finally, weather can influence the transmission equipment and connections, e.g. sagged electricity lines can trip on contact with vegetation. These connections not only directly map threat categories to grid categories, but also provide initial input on how one event can lead to others.

The following section analyzes how non-malicious threats can be related to each other (threat-to-threat dependency). This is way of linking threats to threats is similar to constructing sequences of malicious



threats, which will be outlined later. Noteworthy, attributing individual threats to grid components (threat-to-component) for non-malicious threats would be essentially different from malicious threats, as natural disasters do not imply selectivity of targets and adaptive origins of threats. Therefore, attributing threats to grid components is a topic to be considered separately.

5.1 ENVIRONMENTAL THREATS

Non-malicious external threats to the grid (e.g. environmental) can lead to threats internal to the grid. In other words, for inner grids require to be addressed in terms of reliability, rather than in terms of resilience.

Consequently, the IRENE environmental threats 32 – 35 (listed in Table 5) can be divided into two groups: threats that are external (with threats 32, 34, and 35 belonging to this category) and threats that can be both internal and external (33). This differentiation is related to whether to account for these as reliability or resilience-related. Both categories of external and internal threats can be attributed to the question of how robust is the grid. External threat events can be interlinked and can cause internal threats, while the opposite is hardly possible.

This reports structures relations between IRENE environmental threats as indicated in Table 5. We consider earthquakes and hurricanes as external individual events that are independent from each other. Fires are internal threats that can be caused by either an earthquake or a hurricane. Although fire could also be triggered by a flood (such as due to short circuits), this link is not elaborated. Flood at a primary or backup facility can be caused by a hurricane, but can also be an individual threat event.

Table 5. Dependency of ENV threats based on external/internal grouping

32	Earthquake at primary facility	ENV	Can lead to threat event 33
33	Fire at primary/backup facility	ENV	-
34	Flood at primary/backup facility	ENV	-
35	Hurricane at primary/backup facility	ENV	Can lead to threat events 33 and 34

As noted, while this table outlines a view on interdependencies of threats, it does not highlight how threats can be related to specific buildings. As opposed to malicious threats, environmental threats can often cover several grid components at once and should be considered therefore separately. We approach this topic from the perspective of cascading effects from natural disasters in more detail later in this report. Section 10 illustrates how threats can be attributed to buildings using a flood as an example and linking parameters of the flood to the grid configuration.



5.2 ACCIDENTAL ERRORS AND HARDWARE AND IMPLEMENTATION THREATS

Hardware and implementation (HI) threats are expected to be relatively random and therefore can hardly be attributed to specific grid components. The only dependency between threats suggested in this report, as shown in Table 6, is that threats 37 (Introduction of vulnerabilities into software products) or 38 (Disk error) can lead to threat 36 (Resource depletion). This can happen where a grid was not designed to ensure resilience. For example, if the grid does not support graceful degradation and not employ parallelization of critical components, resource depletion can be expected.

Table 6. Dependency of HI threats

36	Resource depletion	HI	-
37	Introduction of vulnerabilities into software products	HI	Can lead to threat event 36
38	Disk error	HI	Can lead to threat event 36

IRENE threats 29 – 31 are accidental by definition and hence have no precursors and are not seen as result of malicious actions. However, accidental threats can lead to undesirable complex contingencies (as indicated in Table 7). Within these threats incorrect privilege settings (threat 31) is particularly noticeable, as it can allow malicious actors to achieve their objectives significantly more easily. Similarly, if spill of sensitive information (threat 29) concerns grid configuration, malicious actors can use it as a complementary or a substitution to their actions related to threats 1 – 3 (system recon).

Table 7. Dependency of ACC threats

29	Spill sensitive information	ACC	Can be linked to threat events 1 – 3
30	Mishandling of critical and/or sensitive information by authorized users	ACC	Similarly to threat event 29, it can lead to threat events 1 – 3
31	Incorrect privilege settings	ACC	Incorrect privilege settings can directly lead to multiple other threat events, including events 23 – 25

ACC and HI threats differ from environmental in the sense that they do not commonly pose threats to multiple grid components. Therefore, within IRENE these do not need to be considered as related to individual (small) electricity consumers, as a failure of one consumer will not necessarily leads to a blackout.



6 ANALYSIS OF EXTERNAL MALICIOUS THREAT EVENTS

Cybersecurity is largely concerned with intelligent and adaptive adversaries with the major topic being the analysis of malicious threats. This section differs from the non-adversarial threats, as “Estimating the likelihood of malicious scenarios is considerably different than for other threats/hazards, as these estimates must take into account the determined and adaptive nature of an intelligent adversary” [30].

In this section the deliverable outlines interrelations between motivation, *Capability*, *Intent*, and *Targeting* properties of three classes of malicious actors. This deliverable maps plausible sequences of threat events to these classes according to their *Focus* (seen as *Targeting* and *Intent*) and *Capabilities*. We apply the notation of kill chains derived from a generalization of the Lockheed Martin Intrusion kill chain, Mandiant’s attack lifecycle, and Dell secureworks lifecycle of an advanced persistent threat. The deliverable considers that each next threat class covers threats relevant to the previous class and also includes additional threat events. “First Appendix. IRENE Threat Analysis” at the end of this document provides the outcome of the root cause analysis of different adversarial threat events linked to three attacker classes.

Subsection 6.1 covers the state of the art in the domain, including: attacker motivations (6.1.1), taxonomies of threat actors (6.1.2), and modus operandi of attackers described as kill chains (6.1.3). Next, subsection 6.2 analyses these taxonomies and methods. First, in subsection 6.2.1 we outline three classes of malicious actors that should be considered when analyzing threats to critical infrastructures. In 6.2.2 we relate each of those classes to components of the smart grid infrastructure. These relations can be employed for analyzing malicious external threats using a kill chain notation as described in 6.2.3.

6.1 ATTACKERS

As Intel’s TARA (Threat Agent Risk Assessment) [25] suggests, the objectives or goals of attackers can be defined as the combination of threat agent motivations and capabilities. Motivations, i.e. internal reason why he or she wants to attack, are important because they underpin the action and might change with time. Attack goals can include theft/exposure, data loss (destruction or alteration of data), sabotage, operations impact, defacing. Motivations can be accidental (without a malicious intent), personal financial gain (with the goal to obtain business or technical advantage), emotional gain (for personal recognition or satisfaction; damage or destroy organization), as well as social or moral gain (with the goal to change public opinion or corporate policy). Several taxonomies of motivation can be related to each other as follows.

6.1.1 Motivation

After the widely adopted initial step of differentiating between deliberate or accidental motive of threat actors, further differentiation is less straightforward since the motivations of threat actors can significantly differ even for similar skill level across attacker classes. This subsection highlights the diversity of possible attack motives on a smart grid as a critical asset for modern society. Furthermore, we present several classifications of motivations, illustrate their differences and show how these motivations are linked to different classes of attackers.



One of the earlier reports on the topic of critical infrastructure [31] laid out a number of motives in connection to threats to smart grids as a national asset. Table 8 lists threats related to the private sector, outlines traditional national security concerns, and portrays shared threats. This illustrates the level of complexity between different motives.

Table 8. Threats to critical infrastructures [31]

National Security Treats	Reduce US decision space, strategic advantage, chaos, target damage
	Information for political, military, economic advantage
Shared threats	Visibility, publicity, chaos, political change
	Competitive advantage
	Revenge, retribution, financial gain, institutional change
Local threats	Monetary gain, thrill, challenge, prestige
	Thrill, challenge

A list of motives can be constructed from Table 8 as:

- Reduce decision space of a country (from the perspective of national security);
- Obtaining strategic advantage;
- Chaos;
- Target damage;
- Political advantage;
- Military advantage;
- Economic advantage;
- Visibility;
- Publicity;
- Political change;
- Competitive advantage;
- Revenge;
- Retribution;
- Financial (monetary) gain;
- Institutional change;
- Thrill;
- Challenge;
- Prestige;

Another way of considering motivation can be derived from publications by M. Rogers. Figure 5 (reconstructed from [32]) highlights that even for actors with similar skills, motivations can significantly differ. Information warriors, for instance, can be located in an opposite direction compared to “Old guard hackers”, as well as motivations of cyber-punks being different from petty

thieves and professional criminals. Political activists were noted as having a high skill level with motivation different from other actors of a similar skill. In [33] Rogers outlines a two-dimensional graph of motivations. The motivations are divided into four high order categories:

- Curiosity;
- Revenge;
- Notoriety;
- Financial.

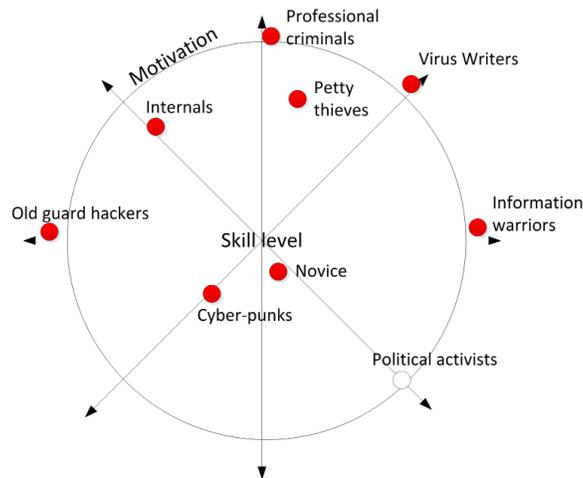


Figure 5. Hacker Circumplex

According to this classification, Novice and old guard hackers were located within the curiosity quadrant; virus writers and internals were placed within the revenge quadrant; cyber-punks and political activists were positioned at the notoriety quadrant. Finally, information warriors, petty thieves, and professional criminals were assigned to the financial quadrant.

In another approach, A. Rege [34] listed seven rationales that can be used to explain hacking:

- Curiosity;
- Spying;
- Thrill and/or challenge;
- Status;
- Political ideologies;
- Revenge;
- Monetary gain.

Another list can be obtained from The HoneyNet Project publications. This project aims to help policymakers decide how best to protect the nation's critical information infrastructure. It outlines [35] six basic motivations for predicting the potential behavior of individuals who gain unauthorized access to their networks. The origins of the six motivations come from an acronym used by the U.S. Federal



Bureau of Investigation's counterintelligence unit to indicate possible motivations of individuals who commit espionage against their country. The original MICE acronym lists Money, Ideology, Compromise, and Ego as four motives. The extended list (i.e. MEECES) includes two more aspects to better reflect the hacker community:

- Money;
- Entertainment;
- Ego;
- Cause (Ideology);
- Entrance to social group;
- Status.

It can be noted that the motivation “Cause”, being the least self-explanatory within this list, points to hacktivism — the use of the Internet to promote a particular political, scientific, social, or other cause. A brief overview of these motivations shows that while some elements of the previous list can be attributed to MEECES (e.g. monetary gain), others cannot. In addition, one of the rationales concerns ‘spying’, which can link to threat sources, rather than to threat actors. These discrepancies are also observable if the list is compared to other motivation taxonomies.

This brief overview introduces a number of views on different attacker motivations. The listed motivations are later cross-compared and analyzed in subsection 6.2.1 of this report. The next one concentrates on attacker taxonomies, which later will be used to outline 3 classes of malicious actors.

6.1.2 Attacker taxonomies

Risk assessment methodologies often link motivations to specific actors. In available classifications, the ways to differentiate actors differ according to the granularity needed for the assessment scope and purposes. This subsection overviews several threat actor taxonomies. We will later use the comparative analysis to outline three classes of malicious actors for analyzing IRENE threat events. Also, by building on the analysis of different taxonomies we provide a link between the IRENE attacker classes to other taxonomies. This ensures the possibility to consistently extend IRENE threat classes, if needed.

According to A. Rege [34], several malicious threats sources can be linked to smart grids as critical infrastructures. These threats include:

- Leisure cyber-criminals (thrill, bragging rights in the cyber-criminal community).
- Industrial spies (to acquire intellectual property);
- Foreign intelligence services, or nation-states, (disrupting supply, communications, and economic infrastructures);
- Terrorists (to disrupt, debilitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence);
- Disgruntled insiders (to cause system damage or steal sensitive information);
- Professional cyber-criminals (to further their criminal pursuits);



- Criminal groups (to attack systems for monetary gain; they may hire or develop cyber-criminal talent to target ICS);
- Phishers (to steal identities or information for monetary gain);
- Spammers (to sell products, conduct phishing schemes, or distribute spyware and malware);
- Spyware/malware authors (attacks against users by producing and disseminating spyware and Malware).

Octave Allegro [36] — a methodology to streamline and optimize the process of assessing information security risks based on existing OCTAVE methods — uses a notation of Threat Trees to differentiate threat sources. Octave does not explicitly provide a list of individual actors. An exemplary list outlined for this methodology found in the literature [37] includes both actors and their motives as follows:

- Nonmalicious employees — people within the organization who accidentally abuse or misuse computer systems and their information;
- Disgruntled employees — people within the organization who deliberately abuse or misuse computer systems and their information;
- Attackers — people who attack computer systems for challenge, status, or thrill;
- Spies — people who attack computer systems for political gain;
- Terrorists — people who attack computer systems to cause fear and for destruction for political gain;
- Competitors — people who attack computer systems for economic gain;
- Criminals — people who attack computer systems for personal financial gain;
- Vandals — people who attack computer systems to cause damage.

The above mentioned taxonomy by Rogers [32] lists the following actors:

- Information warriors;
- Professional criminals;
- Political activists;
- Virus writers;
- Petty thieves;
- Cyber-punks.

Cyber-criminal taxonomy based on technical expertise includes, according to McAfee [38], includes:

- Script kiddy — an amateur attacker who uses codes written by others to exploit the vulnerabilities in computer systems;
- Cyber-punks — motivated by either revenge or a political agenda;
- Hackers — motivated by learning and exploring, while having a strong sense of morals;
- Crackers — with the goal to gain a reputation in the cracker community;
- Cyber-gangs — work in partnership for a criminal organization, driven by the profit,



Spectrum of threat actors outlined in the mentioned earlier Report of the President's Commission on Critical Infrastructure Protection from 1997 [31] relates actors to national, shared, or local threats as follows:

- National Security Treats:
 - a. Information warrior (who aim to reduce US decision space, strategic advantage, chaos, target damage);
 - b. National Intelligence (Information for political, military, economic advantage);
- Shared threats:
 - a. Terrorist (Visibility, publicity, chaos, political change);
 - b. Industrial espionage (Competitive advantage);
 - c. Organized crime (Revenge, retribution, financial gain, institutional change);
- Local threats:
 - a. Institutional hacker (Monetary gain, thrill, challenge, prestige);
 - b. Recreational hacker (Thrill, challenge).

Several other taxonomies provide even more elaborated classifications. ENISA (European Network and Information Security Agency) [24] considers cyber-agents as actors with intent and skills who interact with the system. At the first differentiation step, agents are considered to be either friendly or hostile. The latter group is subdivided by accounting for their high or low capability. A list of cyber-agents forms the following structure:

- Friendly (Unintentional): researchers, ethical hacker, security agent, law enforcement agent, cyber-soldier, employee, end-user/customer;
- Hostile (Intentional):
 - a. Low tech/low-medium expertise:
 - Script Kiddies (young, unskilled);
 - Online Social hacker (soft skilled);
 - Insider/Employee (internal, low-medium-skilled):
 1. Current;
 2. Former;
 3. Internal;
 4. External (Contractor, Provider);
 - b. Hi tech/High expertise:
 - Provider/developer/operator (infrastructure deliver);
 - Tools User/deployer (infrastructure use):
 1. State or Corporation espionage;
 2. Hactivist (socially motivated citizens);
 3. Cyber-terrorist (ideologically motivated);
 4. Cyber-criminal (profit oriented);
 5. Cyber-fighter (nationally motivated citizens).



Several roles in this structure can be concurrent. The examples include Insider/Employee and Corporation espionage; Cyber-fighter and Cyber-terrorist; Cybercriminal and Cyber-terrorist; Cyber-fighter and State espionage; and Provider/developer operator and either Cyber-terrorist or Cyber-criminal.

TAL (Threat Agent Library) [39] developed by Intel is an example of a sophisticated list of threat agents. According to the authors, its application reduced the time required for a risk assessment by about 30 percent. This library was constructed by a cross-functional team of security specialists with expertise in corporate IT security, government security agencies, product security, law enforcement, and physical security. It enables to differentiate among different agents commonly described as ‘hackers’. A list of corresponding agents includes: Cyber-Vandal, Data Miner, Internal Spy, Mobster, Government Spy, and Government Cyber-warrior.

TAL describes 21 standardized archetypes of threat agents. These archetypes are defined using a simple taxonomy of the following eight attributes:

- Intent (Hostile, Non-Hostile);
- Access (Internal, External);
- Outcome (Acquisition/Theft, Business Advantage, Damage, Embarrassment, Technical Advantage);
- Limits (Code of Conduct, Legal, Extra-legal minor, Extra-legal major);
- Resources — this defines the organizational level at which an agent typically works (Individual, Club, Contest, Team, Organization, Government). This attribute is linked to the Skill level attribute — a specific organizational level implies that the agent has access to at least a specific skill level;
- Skill Level (None, Minimal, Operational, Adept);
- Objective (Copy, Destroy, Injure, Take, Don’t care);
- Visibility (Overt, Covert, Clandestine, Don’t care).

For instance, the first differentiation suggests the assignment of the attribute ‘non-hostile’ to: Reckless Employee, Untrained Employee, and Information partner. All of them are considered as insiders. Other insiders include Disgruntled Employee, Government Spy, Internal Spy, Thief, and Vendor. The complete list of actors includes: Employee Reckless, Employee Untrained, Info Partner, Anarchist, Civil Activist, Competitor, Corrupt Government Official, Data Miner, Employee Disgruntled, Government Cyber-warrior, Government Spy, Internal Spy, Irrational Individual, Legal Adversary, Mobster, Radical Activist, Sensationalist, Terrorist, Thief, Vandal, and Vendor.

Altogether these attacker taxonomies extensively cover the topic of differentiating actors at different levels of granularity, including actor taxonomies seen from the perspective of critical infrastructures. These taxonomies can be cross-related to identify several classes of attackers, as shown in subsection 6.2.1.



6.1.3 Attack methods

The patterns of attacks differ significantly by type of motive and actor. Methods by which an attack may occur might depend on the combination of threat agent objectives and threat agent operating methods.

Attacker's methods may limit possible actions, as well as reinforce persistence in using others. This is illustrated by the view adopted by Intel within the Methods and Objectives (MOL) Library that considers Limits and Acts relevant to malicious actors. For instance, MOL limits include “Code of conduct”, “legal”, “crimes against property”, and “crime against people”. At the same time, Acts on target can take several forms. MOL includes actions of “copy, expose”, “deny, withhold, ransom”, “destroy, delete, render unavailable”, “damage, alter”, and “take, remove”. Another way of structuring actions is outlined in the US information operations doctrine as: detect, deny, disrupt, degrade, deceive, and destroy. FAIR actions against an asset include: access, misuse, disclose, modify, and deny access. Octave lists outcomes of actions as “disclosure”, “modification”, “loss, destruction”, and “interruptions”. Similarly to limits, individual actions can be attributed to specific actor profiles. Although considering actions can clearly assist in assessing the impact, they can be hard to predict and hence, often these are used mainly in attack or fault tree methodologies. Instead, another approach could be to concentrate not on final actions, but rather on structuring the sequence leading to the success of an attack. The Kill Chain notation can be useful to this effect.

The Kill Chain, a conceptual model used by US Military, structures (sequential) steps of attacks an attacker necessarily goes through in the course of their goal. These resemble the ‘crime script’ which is the criminology method for structuring modus operandi. While kill chains are most relevant for advanced persistent threats with intent to compromise data for economic or military advancement, this approach is also used to structurally map threats to specific actors, as well as to relate sequence specific threats with respect to others.

Probably, the most widely known kill chain model in information security was developed by Lockheed Martin for intrusion detection purposes. The model includes 7 phases:

1. Reconnaissance — research on targets, such as search for mailing lists, social relationships, or information on specific technologies;
2. Weaponization — e.g. coupling a remote access trojan with an exploit into a deliverable payload;
3. Delivery — transmission of the weapon to the targeted environment;
4. Exploitation — the triggered code targets an application or operating system vulnerability;
5. Installations — a remote access Trojan or backdoor allows to maintain persistence inside the environment;
6. C2 (commands & control) — a compromised host reaches an external server to establish a channel;
7. Actions — for instance, data exfiltration, violations of data integrity and availability.

Another example of an APT's attack lifecycle was presented in the Mandiant publication [40]. The steps include:

1. Initial Recon;
2. Initial compromise — methods used to penetrate an organization’s network. The most common method is spear phishing. For instance, e-mails or messages in social networks can include malicious attachments or a link to a malicious website;
3. Establish foothold — when an attacker can access and control a computer within the targeted organization. The communication, established through a backdoor connection, is often established as an outbound connection from the organization network;
4. Escalate privileges (can be repeated after a set of three steps “Internal recon”, “Move laterally”, and “Maintain presence”) — corresponds to the access to more resources within the organization’s network. Next to obtaining usernames and passwords, it may include access to VPN software or privileged computers. This stage can initiate several loop of “Internal recon”, “Move laterally”, and “Maintain presence”. These steps correspond to collecting additional information, gaining access to additional computers, and ensuring control over key systems correspondingly;
5. Complete mission — can include stealing data or achieving other actions on target.

These steps are similar to those of the Lockheed Martin kill chain, but highlight that some actions are needed to manage access level (escalate privileges) and points out that this process can be iterative. Besides, “Maintain presence” is seen as a separate action.

CRISALIS (Securing critical infrastructures) in its deliverable “D5.1 Security Testing Methodology” [41] describes another attack sequence. This structure outlines an attack example structure similar to a kill chain by considering NIST SP 800-115 “Technical Guide to Information Security Testing and Assessment”. Two phases with several steps within the attack phase are shown in Figure 6.

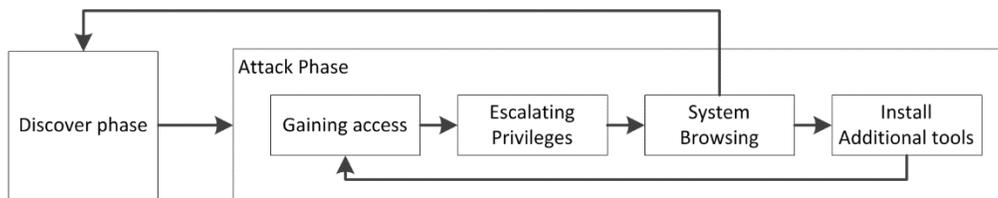


Figure 6. NIST SP 800-115 attack sequence

The steps corresponds to the following:

- Gaining access — starts after enough data has been gathered in the discovery phase to make an informed attempt to access the target;
- Escalating privileges — an attacker will seek to gain full control of the system, if only user-level access was obtained;
- System browsing — gathering new information;
- Install additional tools — new tools are installed to gain additional information and/or access.

Compared to the kill chains, this approach distinguishes between information and access. Additionally, it demonstrates that feedback loops can be both within the Attack phase and in-between the Discovery and Attack phases.

Dell secureworks (www.secureworks.com) describes another highly elaborated kill chain structure (Figure 7).



Figure 7. Kill chain by Dell secureworks (from www.secureworks.com)

By relating steps to actors, this kill chain shows some steps being expected from every actor: “Build or acquire tools”, “Deployment”, “Initial intrusion”, “Outbound connection initiated”, and “Exfiltrate data”. Advanced Persistent Threats (APT) are seen as iterative in their nature and pose every threat listed in Figure 7. Sets of threats relevant to other actors are subsets of the APT list of threats.

The chains described in this subsection allow to structurally approaching the diversity of attacks conducted by different actors. In their format, they stay close to ‘crime scripts’ in criminology that dissects steps in the commission of a crime. As indicated, kill chains highlight important aspects of attacks relevant to consider: the iterative nature of attacks, lateral movements and the need to maintain presence in the system, the differentiation between information and access, and how some types of attackers can be related to specific attack steps. These elements of kill chains can be encoded and exchanged among experts by using, for instance, the STIX¹ XML scheme and TAXII² set of specifications.

¹ Structured Threat Information eXpression as described at <https://stix.mitre.org/language/version1.2/xsddocs/XMLSchema/ttp/1.2/ttp.html>

² The Trusted Automated eXchange of Indicator Information from <https://taxiiproject.github.io/>



This deliverable adopts a kill chain approach to analyze root causes of threats. As later described, it relates kill chain steps to different classes of threat actors. This approach is shown next.

6.2 ROOT-CAUSE ANALYSIS OF ADVERSARIAL THREATS

This subsection analyses adversarial threats and makes interrelations between threats and threat categories. First, three classes of malicious actors (C1, C2, and C3) are outlined according to their *Focus* and *Capability*. Next, the categories of grid components described in [D2.1](#) (and listed in Appendix A of this deliverable) are linked to *Focus* of malicious actors. This results in lists of components relevant to each class representing threat-to-component relations. Finally, threats are related to *Capabilities* of attackers to identify expected kill chains. This corresponds to threat-to-threat relations. Together, lists of relevant components and expected kill chains provide adequate guidance to identify threats relevant to a particular grid component or feature (several components). Later, they are used to calculate Loss Event Frequencies of specific threats.

6.2.1 Three classes of malicious actors

This subsection identifies different types of motivations and then outlines three classes of attackers analyzing interrelations between attacker taxonomies on attacker motivation taxonomies.

The taxonomies mentioned in subsection 6.1.1 were mapped to identify overlaps and deficits. Table 9 illustrates a possible outcome of this task. Within the table the “Financial” and “Money” categories are seen as direct benefits, not comparable to obtaining “Competitive” or “Economic” advantage. In addition, several motivations can be grouped to obtain categories “Political & Institutional change”, “Obtaining Strategic & Political & Military advantage” and similar.

Table 9. Cross-comparing different motivation taxonomies

	US CI protection	Rogers	Rege	MEECES	
1	Reduce decision space of a country				
2	Political & Institutional change		Political ideologies	Cause (Ideology)	
3	Target damage				
4	Chaos				
5	Obtaining Strategic & Political & Military advantage		Spying		
6	Competitive advantage				
7	Economic advantage				
8	Revenge & Retribution	Revenge	Revenge		
9	Financial & monetary gain	Financial	monetary gain	Money	
10	Visibility	Notoriety	Status	Status	Entrance to social group
11	Publicity				
12	Prestige				
13	Thrill & Challenge		Thrill and/or challenge	Ego	
14		Curiosity		Entertainment	

This table highlights several aspects of motivations relevant to smart grid attacks:



- Three motivation categories of threat sources can be outlined: national, organizational, and individual. The motivations can be grouped based on the role that a critical infrastructure plays as a national asset at country level (motivations 1 – 5), adversarial interest related to an organization level (6 – 7), and individual-based motivations (8 – 14). The colors within the table illustrate these groups of motivations. Some motivations can, however, be attributed partially to either individual or organizational motivations. For example, a disgruntled employee (as an individual) or a competing organization can have a motivation to damage or destroy an organization (motivation 3). This points out that motivation can be a driving force for different actors;
- Not every taxonomy can be used to account for the essential role of critical infrastructures on a country- and organizational level. For example, the taxonomy by Rogers concentrates more on individual interests;
- All classifications can be extended by adopting at least one motivation from other taxonomies. For instance, “Curiosity” or “Entertainment” can be seen as different to “Thrill & Challenge”; “Reduce decision space of a country” can be incorporated into other classifications, if they aim to account for strategic goals of hampering critical infrastructures, etc;
- Motivation 8 – 14 appear in most of listed classifications and hence are widely accepted. At the same time, because the mentioned classifications concentrate less on some motivations (1, 5 – 7), it can be argued that these motivations are less relevant to individual actors and can be more related to threat sources;
- By differentiating between motivations for threat sources and threat actors, some motivations can be seen as interfaces between threat sources and actors. In other words, threat sources with motivations 1 – 14, by means of these interfaces (namely, motivations 2 – 4 and 8 – 14), can foster threat actors to perform malicious activities. Arguably, the degree to which a source can employ the interfaces, such as those related to financial aspects, can be related to the degree of motivation of the sources themselves. Types of instantiations of these interfaces can be further classified. For instance, as related to threat source-sponsored, threat source-sanctioned, or threat source-directed malicious activities.

Actors from the taxonomies outlined in subsection 6.1.2 can be individually assigned to three classes as Table 10 shows (“Hi” and “Low” shows whether high or low capabilities of these actors were explicitly mentioned in the corresponding documents).



Table 10. Grouping malicious actors

	PCCIP	Octave	Rogers	McAfee	ENISA	TAL
C3 (APT)	National Intelligence	Spies	Information warriors (Hi)		State or Corporation espionage (with national or corporate mission) (Hi tech)	Government Cyber-warrior, Government Spy
	Terrorist	Terrorists			Cyber-terrorist (ideologically motivated) (Hi)	Terrorist
	Information warrior					
C2 (organizations)	Industrial espionage	Competitors	Professional criminals (Hi)	Cyber-gangs (Hi)	Provider/developer/operator (infrastructure deliver) (Hi tech)	Internal Spy
	Institutional hacker	Criminals	Political activists (Hi)	Crackers (Mid)	Cyber-criminal (profit oriented) (Hi)	Vendor
	Organized crime	Attackers	Virus writers (Hi)		Cyber-fighter (nationally motivated citizens) (Hi)	Legal Adversary
					Hactivist (socially motivated citizens) (Hi)	Competitor
						Corrupt Government Official
C1 (mostly individuals)	Recreational hacker	Vandals	Petty thieves (mid)	Cyber-punks (lo)	Script Kiddies (Low)	Vandal
			Cyber-punks (Low)	Script kiddy (lo)	Online Social hacker (Low)	Anarchist
			Novice (low)			Irrational Individual
						Thief
						Sensationalist
						Civil Activist
						Data Miner
						Mobster
						Radical Activist
Malicious Insider:		Disgruntled employees	Internal (mid)		Insider/Employee (Low)	Disgruntled employee
Non-intentional insider		Non-malicious employees	Old guard hackers (hi)	Hackers	Friendly (Unintentional), including researchers, ethical hacker, etc.	Reckless employee, Untrained employee, Info Partner

The table groups attackers into three classes: commodity actors (C1), targeted actors (C2), and actors that pose advanced persistent threats (C3). The classes are characterized based on their *Focus* (as *Targeting* together with *Intent* (in other words, *Contact* together with *Action*) and *Capabilities*:

- C1 class: opportunistic actors that pose commodity threats. The actors from this class possess low *Focus* and *Capabilities*;
- C2: targeted actors. These actors are more devoted to attacks due to organizational support. This support provides more *Capabilities*;



- C3 highlights Advanced Persistent Treats. These highly motivated actors possess the highest level of *Focus* and *Capabilities*.

The top layer of the table lists examples of actors from the C3 class for different taxonomies. This grouping is in line with the Dell Securework classification that includes nation-state actors, organized criminal actors, corporate espionage actors, and terrorists as APT actors. These actors can be attributed to government-level and other highly capable organizations. By interesting capabilities of these threat sources, the corresponding actors can be seen as both highly focused and capable. Actors from the second class (C2) have less capabilities and lack focus compared to C3. Still, this class can make use of organization-level features. For instance, virus writers, criminals, and crackers can be part of larger organizations. Finally, class C1 includes mainly individual actors not largely involved in collaborations and organized attacks. For example, a recreational hacker located in this class can perform individual attacks driven by thrill and curiosity, while an anarchist or a cyber-punk act because of different personal reasons.

In line with most taxonomies, Malicious Insider and Non- intentional insider, are left out of the outlined C1 – C3 classes as they already have some limited access to the system. Malicious Insiders as actors can span over the whole C1 – C3 spectrum of attackers depending on their access. Similarly, Non-intentional insiders are limited by the degree the system can be protected from mistakes made by such personnel due, for instance, lack of training or misinterpretation of data. Old guard hackers and ethical hackers are classed as non-intentional actors because these can accidentally damage the system during pen-testing. The interplay between the current extent of access of non-intentional insiders and their goal thus becomes the focal point, rather than considering their capability to attack the system.

Table 9 and Table 10 were mapped to outline the *Focus* of malicious actors as shown in Table 11. This implies that higher classes of actors can be fostered to actions by threat sources, which in turn may have different motivations. In other words, motivation of high-level threat sources implies possibilities to direct focus of attacks due to potentially high degree of organizational support.

Table 11. Linking motivation to classes of external malicious actors

	Motivation mainly linked to high degree threat sources	Organization-level motivations	Individual motivations
C3	X	X	X
C2		X	X
C1			X

Therefore, the C1 class can be driven by individual motivations, C2 by organization-level and individual motivations whilst C3 to both individual-, organization-, and state-level motivations (through targeted disposition of threat source resources).

Such C1 – C3 motivation logic implies that the C3 class results from advanced support due to the motivation of highly organized threat sources. C3 actors could therefore stay more focused and capable than C2, whose *Focus* and *Capabilities* in turn would exceed those of C1 attackers. We employ this



logic to assign values to FAIR’s constructs of *Contact*, *Action*, and *Treat Capabilities* to describe these classes as shown in Table 12.

Table 12. Encoding *Focus* and *Capabilities* of C1 – C3 actors into FAIR constructs

	Contact	Action	Threat Capability
C3	High	High	High
C2	Medium	Medium	Medium
C1	Low	Low	Low

In this table, the employed ‘Low’, ‘Medium’, and ‘High’ qualitative values are originated from the 5 step scale [Very Low, Low, Medium, High, Very High] outlined in Section 4. Assigning similar levels to *Contact* and *Action* for each class is motivated by our intention to provide a high level overview of the highly diverse population of relevant threat actors.

The C1 – C3 classification of threat origins can be linked to three attack types with different organization principles, which is in line with other research projects e.g. SOES. However, it significantly differs from SOES in terms of scope, method, and goal. First, the C1 – C3 classification outlines different motivations that can be related to particular threat sources or actors (Table 9). Next, it illustrates the landscape of different actors taking into account their capabilities (Table 10). The relation between motivations and actors provided in Table 11 supports flexible assignment of different *Focus* to different actor classes. Finally, Table 12 forms the input for future FAIR analysis to group threats based on their Loss Event Frequencies.

Thus, this approach is more structured, integrated, and flexible compared to similar existing high level classifications. A more structured overview is provided by comparing different taxonomies. Besides, the motivation of malicious agents described in 5.1.1 is linked to attacker classes using an organization-related lens. The integration is supported by connecting actors to LEF calculations using the FAIR method. Finally, the outlined approach provides noticeable opportunities for further ramifications of the three tier form.

With relation to the provided flexibility, the mapping can be further adjusted for the needs of a specific analysis. If another level of granularity is needed, further breakdown of specific classes might be employed by following one of the taxonomies listed above. For instance, a breakdown can introduce class C2.2 that includes actors who benefit from being a part of an organization, but have individual motivations for attacks. An example can be an ex-employee that couples with organized crime for the purpose of individual revenge. This and other similar breakdowns can benefit from the outlined taxonomies and can result in specific tables similar to Table 11. They might have the same structure, but be filled in with different content. An even further ramification of threat actors can be to re-assign *Contact*, *Action*, and *Capabilities* characteristics of attackers to specific threats. For instance, ex-employees mentioned above as a possible C2.2 class can be subdivide into C2.2a and C2.2b using a table similar to Table 12. The first of the two sub-classes may have higher *Focus* (i.e. *Contact* and *Action* can be Medium for C2.2a compared to Low for C2.2). The reason could be that actors form



C2.2a compared to C2.2b can possess a unique expertise and wide knowledge of the system components are located.

Actor classes can be related to different attacks according to their *Focus* and *Capability*. This implies considering what targets the actors could choose, as well what specific threats can be expected from the actors. The next subsection concentrates on the first of these two aspects.

6.2.2 Relating classes of attackers to smart grid components

This subsection illustrates how classes of attackers can be related to the IRENE list of grid components. We relate List of Components from D2.1 to our threat classes C1 – C3 based on their *Focus* characteristic (*Intent* and *Targeting* according to NIST or *Contact* and *Action* in FAIR terms). The degree of probable physical and cyber contacts of attackers with grid assets and their intention to start attacks have a stake in this matter.

Table 13 links classes of malicious actors to specific grid components in terms of the Threat Event Frequency (TEF) concept from the FAIR taxonomy.

Table 13 incorporates the idea that some types of grid components may be less relevant for specific classes than others. For instance, an attack on a Factory grid component implies that adversarial *Focus* would exceed the properties of the C1 class. Therefore, the event can be more frequently attributed to either C2 or C3 classes. Data connections stay more available to contact for malicious actors than micro grid connections. Only two elements in this table — Power Plant and SCADA — are linked exclusively to class C3. This is because they stay significantly less available to insufficiently organized actors.

Table 13 is built around the idea of a minimum needed *Focus*. If a component can be within *Focus* of a lower class of malicious actors, actors from higher classes may focus on it according to their advanced organizational structure. Thus, if *Focus* of C1 actors is sufficient for considering this mapping, other classes (that have higher *Focus*) should also be linked to the component. In another example, as a Basic Data Center is linked to the *Focus* of C2, its TEF with respect to C3 should also be considered. We employ the term ‘Equalizer’ to highlight this idea by illustrating the implied continuity, when the next level includes characteristics of the previous. Graphically, the outlined relations between specific grid components and threat classes can be represented as in Figure 8.

Table 13. Relating classes of malicious actors to grid components

N	Component name	C1	C2	C3
Connections				
1	Electricity Connection	X	X	X
2	Data Connection	X	X	X
3	Micro Grid Connection	-	X	X
4	Connection Adapter	-	X	X
5	Connection Adapter with Energy Transformer	-	X	X
6	Long-Range Connector	-	X	X
Energy Provider				
7	Power Plant	-	- ³	X
8	Photo Voltaic Energy Generator	-	X	X
9	Wind Farm	-	X	X
Buildings				
10	Factory	-	X	X
11	Stadium	X	X	X
12	Hospital	X	X	X
13	Offices	X	X	X
14	Offices District	X	X	X
15	Smart Home	X	X	X ⁴
16	Generic Special Building	X	X	X
Data Center				
17	Basic Data Center	-	X	X
18	SCADA	-	- ⁵	X
Others				
19	Data and Electricity Storage	-	X	X
20	EVs Charging Point	X	X	X
21	Access Point	X	X	X

³ Because power plants are not easily accessible, the amount of contacts of adversaries for this component is limited

⁴ The settings where smart homes can be highly targeted include situations when DNO employees work outside of the DNO premises

⁵ Due to the need of advanced knowledge about control systems

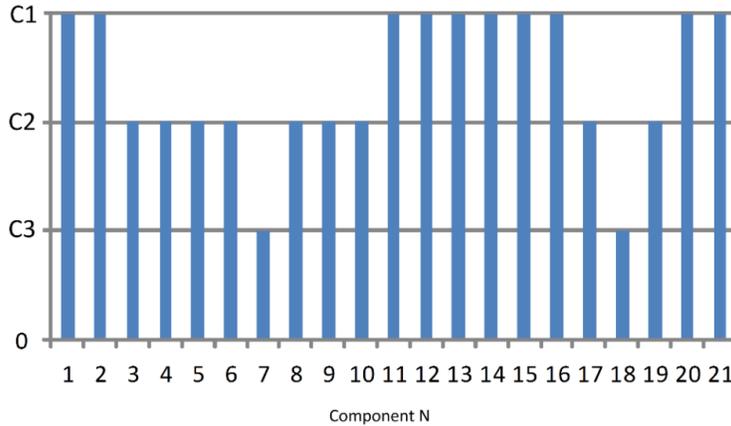


Figure 8. Components mapping: assigning buildings types to attacker classes based on their *Focus*

6.2.3 Analyzing adversarial threats as steps of kill chains

The IRENE threat event inherits NIST 800-30 categories of threats. For adversarial actors the list of categories is as shown in Table 14

Table 14. Categories of adversarial threats

Tag	Category
PRGI	Perform reconnaissance and gather information
CCAT	Craft or create attack tools
DIIMC	Deliver/insert/install malicious capabilities
EC	Exploit and compromise
CA	Conduct an attack (i.e., direct/coordinate attack tools or activities)
AR	Achieve results (i.e., cause adverse impacts, obtain information)
CC	Coordinate a campaign

This list aligns well with the kill chain notation and reflects steps of kill chains described above. It suggests that NIST threat categories cover different stages of an attack in a structured manner. The similarity between kill chains and the IRENE categories allows us to construct a sequence of categories that highlights an attack as a sequence of kill chain steps (Figure 9).

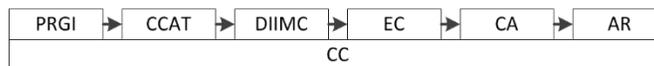


Figure 9. Kill chain based on categories of adversarial threats

Deliberate actions of external malicious actors leading to ‘Achieve Results’ categories can be mapped to this kill chain according to their *Capability*. **Appendix A “IRENE threat events list attributed to**



threat “lists the mapping. The adopted mapping enables to structurally consider cyber-threats that remain relevant to specific classes. Graphically, the threat sequences can be illustrated as shown in Figure 10.

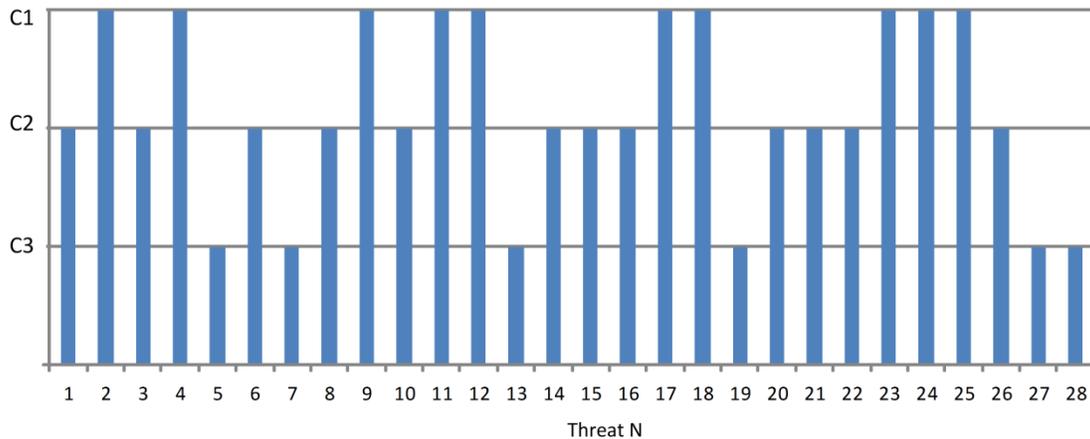


Figure 10. Threat mapping: Assigning IRENE threats to attacker classes based on their *Capability*

The format of an equalizer illustrates that threats relevant to the next attacker class include threats related to the previous one. This table illustrates the continuity of the threat landscape. Due to the continuity of increasing threat *Capability*, threats relevant to C2 include all threats from C1. The C3 (APT class) — the most sophisticated adversaries due to their *Capabilities* — can be related to each of the IRENE threats events. Noticeably, highly capable actors need not to employ all their resources as they might aim to spend only the least amount needed to succeed. For example, in some situations C3 could potentially exploit a zero-day vulnerability, but might prefer to follow other (cheaper) ways to achieve their goal.

Considering threats relevant to individual actors based on their *Capabilities* enables projecting threats to IRENE categories as kill chains. The generic kill chain can be populated for classes C1 – C3 of malicious external actors as follows (Figure 11).

The clustering of threats makes it possible to consider subsets of threats for individual malicious classes as well as highlight sequences relevant to individual classes. These kill chains can be useful for relating *Capabilities* of actors to the list of types of IRENE components outlined earlier based on *Focus* of different attackers.

These sequences represent threat-to-threat connections. They include interrelations between individual threats, between individual threats and threat categories, and in-between categories of threats. In kill chain C1, for example, threat number 9 is parallel to threats 11 and 12, stays connected to threats 17 and 18 of the next step (CA threat category) and can be related to threat 4 of the CCAT category. Connections to classes DIIMC and CC are absent due to *Capabilities* of attackers.

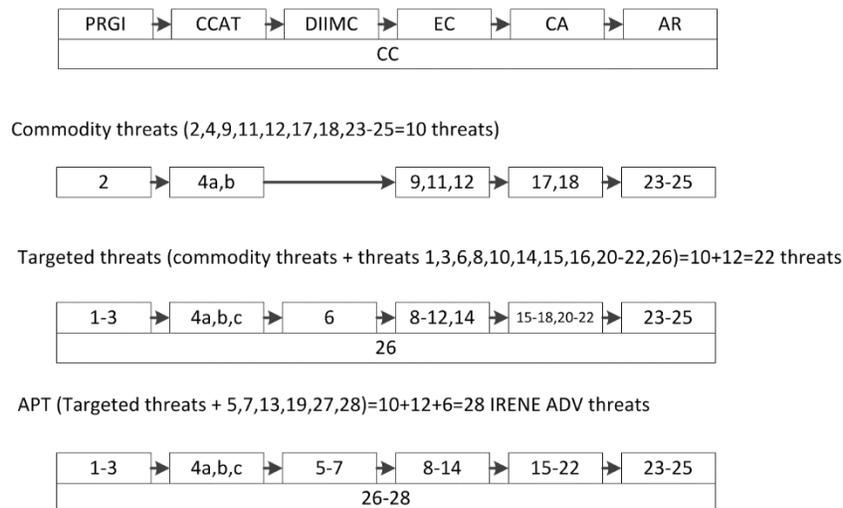


Figure 11. Kill chains for different attacker classes

Combining the outlined components-to-classes and threats-to-classes mappings allows to relate building types to specific threats according to *Focus* and *Capabilities* of actors. Each building type within a grid can be related to C3 attackers due to their advanced focus, thus suggesting that all threats are applicable to each buildings for this class. The buildings related to *Focus* of at least C2 (the types of buildings include 1 – 6, 8 – 17, 19 – 21) have several threats that repeat twice (1 – 3, 4, 6, 8 –12, 14, 15 – 18, 20 – 22, 23 – 25). Finally, the buildings related to at least class C1 (1, 2, 11 –16, 20, 21) are exposed to threats that are repeated in connection to other classes. Threats that repeat twice include those of C2 (1 – 3, 4, 6, 8 –12, 14, 15 – 18, 20 –22, 23 – 25). Some other threats are repeated three times and stay relevant for all classes (2, 4, 9, 11, 12, 17, 18, 23 – 25).

The two-step process described allows for the concentration on threats relevant to specific types of buildings (or building categories) by accounting for a particular class of attackers. Thus, it allows for the elimination of sets of threats for a specific grid component in a traceable and repeatable way. By removing less relevant actor classes stakeholders can concentrate on more relevant kill chains that include several groups of threats aligned in a sequence. This represents threat-to-component connections.

An application of the described approach can be illustrated with respect to the 5th grid component Connection Adapter with Energy Transformer, CAT as shown in Figure 12. Given the component type, the *Focus* characteristic of attackers to initiate a threat event to CAT should be at least on the C2 level. It makes the shortest kill chain less relevant. Eliminating the C1 kill chain allows to concentrate on other two.

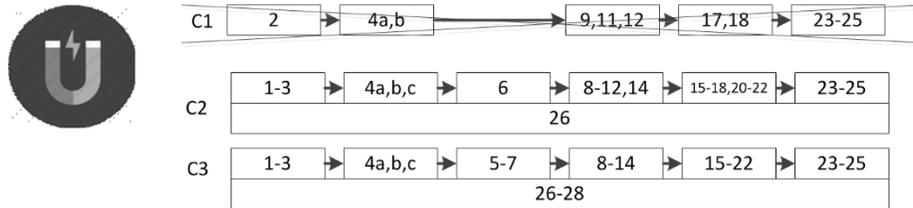


Figure 12. An example to concentrate on threats to a grid component

Based on lists of threats relevant to specific components, a decision maker could concentrate on strength of controls relevant to those threat events, resulting in the calculation of Loss Event Frequencies for specific threats. Because a number of threats share mitigation measures, implementation of one measure could increase the *Control Strength* for several threats at once. This increase can be different for some threats. For example, one threat could demand four mitigation strategies, while another requires three. The implementation of a mitigation strategy will thus lead to an increase in *Control Strength* for the first threat by $1/4=25\%$ and for the second $1/3=33\%$. These changes in *Control Strength* will influence Loss Event Frequency for different threats, suggesting that the first one can be expected more frequently.

In a more realistic case, the changes in *Control Strength* might not be linear and even stay fuzzy. It can be reasonable to expect that, given the complexity of the task, expert opinion may have difficulty in unequivocally assigning *Control Strength* as ‘high’, ‘average’, or ‘low’ element on a scale that describes a specific threat factor. Similarly, the description of other threat factors (*Contact*, *Action*, *Threat Capability*) can be designated as in-between ‘high’ and average, especially if classes of threats actors would be extended using the information provided on actor taxonomies and motivations.

Therefore, to find LEF for specific threats a suitable structure should be employed. Although FAIR provides a structure to calculate LEF based on threat factors, it might be extended to calculate LEF under the described assumptions. Specifically, there is a need to account for possible variations in threat factors, which can hardly be mapped to the FAIR five point scale. The next section illustrates how FAIR can be enhanced with a Bayesian approach.



7 BAYESIANFAIR: ENCODING FLEXIBILITY INTO FAIR USING A BAYESIAN NETWORK APPROACH⁶

In this section, we propose a method to construct a Bayesian network model based on the FAIR approach to LEF and look-up table. The Bayesian approach is consistent with FAIR's look-up tables. However, the difference between the two is that our model provides a quantitative output.

Our method offers several advantages due to its design, as it:

- Supports ranking threats in the same group. By providing a numerical output for system managers we aim to support their perception of threat LEF with respect to other threats in the group. Managers can thus be able to make better decisions regarding security countermeasures and mitigation plans;
- Identifies the most influential factor which, if lowered, can decrease the overall LEF more quickly than others;
- Allows answers to be obtained even with fuzzy inputs, for instance when experts did not fully agree on specific threat parameters;
- Illustrates how changes in the input data propagate through the network and contribute to the output.

In the next subsection we introduce our FAIR framework to the Bayesian network model transformation. Next, we present experiment results and discussions.

It should be noted that this section provides a method of calculating LEFs using BayesianFAIR; the examples used being merely illustrative. The more relevant application within the Threat Navigator method are presented in the next section.

7.1 BAYESIAN NETWORK APPROACH TO TRANSFORM A STRUCTURAL ANALYSIS

We apply the method proposed in [42], which provides the way to construct the Bayesian Conditional Probability Table (CPT) of an effect based on the fuzzy relations of the causes. The transformed model is as follows: given a Bayesian reasoning structure with n causes that lead to an effect. The causes and the effect all can have m states, which represented as state $1, 2, \dots, m$. Each cause i affect to the effect through the individual effect vector $[r_{i1} \ r_{i2} \ \dots \ r_{im}]$, which mean, if the state of cause i is j , then it will contribute r_{ij} percent to the event that the effect has the highest state (state m). On the other hand, the relationships between the causes and the effect are represented through the weights a_1, a_2, \dots, a_n , which means state of cause i will contribute a_i percent to the state of the effect. The weight vector $[a_1, a_2, \dots, a_n]$ and the individual effect vectors for each cause are standardized, in a way that the sum of all the vector members is 1.

⁶ This chapter was published as: Le, A., Chen, Y., Chai, M., Vasenev, A., Montoya, L: Assessing Loss Event Frequencies of Smart Grid Cyber Threats: Encoding Flexibility into FAIR Using Bayesian Network Approach, SmartGifts conference on smart grid inspired future technologies, 2016.

With this model, the method in [42] allows the generation of the effect's Conditional Probability Table (CPT) from the individual effect vectors and the weights through the following formula:

$$P(E = j \mid C_1 = j_1, C_2 = j_2, \dots, C_n = j_n) = \sum_{i=1}^n a_i r_{i\sigma(j_i - j, j)} \quad (1)$$

in which $P(E = j \mid C_1 = j_1, C_2 = j_2, \dots, C_n = j_n)$ is the conditional probability of the event in which the effect E has state j , while its causes C_1, C_2, \dots, C_n has state of j_1, j_2, \dots, j_n respectively; and $\sigma(j_i - j, j)$ is calculated as:

$$\sigma(j_i - j, j) = \begin{cases} j_i - j, & j_i - j \geq 0 \\ j, & j_i - j < 0 \end{cases}$$

$I(C_i)$, the influence of C_i to the effect, can also be calculated by formula (2). In the formula, $P(E=m|C_i=k)$ is the conditional probability when Effect E has state m (highest) and cause C_i has state k . By comparing the I value for each of the factors, we will know which element is the most important.

$$I(C_i) = \frac{\left| \frac{\sum_{k=1}^{m-1} P(C_i = k)}{\sum_{j=1}^{m-1} P(C_i = j)} P(E = m | P(C_i = k)) - P(E = m | C_i = m) \right|}{P(E = m)} \quad (2)$$

7.2 BAYESIAN NETWORK APPROACH TO TRANSFORM THE FAIR FRAMEWORK

We consider the FAIR structure as a Bayesian network which consist of three pairs of cause-effect relations, including [cause: C, A; effect: TEF], [cause: Tcap, CS; effect: V], and [cause: TEF, V; effect: LEF]. In order to calculate with this Bayesian model, the CPTs at the three nodes TEF, V, and LEF need to be identified. After these CPTs are formed, the Bayesian model can give statistical output for the LEF query, which later needs to be transformed into a numerical output. We propose a method to identify the CPTs, let's say between effect E and cause C1, C2, given their corresponding FAIR look-up table [eij \in {VL, L, M, H, VH}, i=1..5, j=1..5], as can be seen in Figure 13, through the following steps.

Step 1. Calculating the weight of the factors: Noteworthy, the FAIR tables are formed with the assumption that the states of the two causes create direct impacts to the state of the effect. Therefore, if we transform the state data to numerical data, there should be a strong correlation between the causes and effect data in most of the cases. In the simplest form, we can assume the relation is linear and translate the node state into number by defining VL=1; L=2; M=3; H=4; VH=5. We then have numerical data for the causes and effect, which we can use to run a regression to test the linear model between the causes and effect, $E = \alpha C_1 + \beta C_2 + \gamma$. The coefficients α, β are then standardized with $\alpha' = |\alpha|/(|\alpha| + |\beta|)$ and $\beta' = |\beta|/(|\alpha| + |\beta|)$. We choose α' and β' as the weights of the causes toward the effect (see Figure 13).

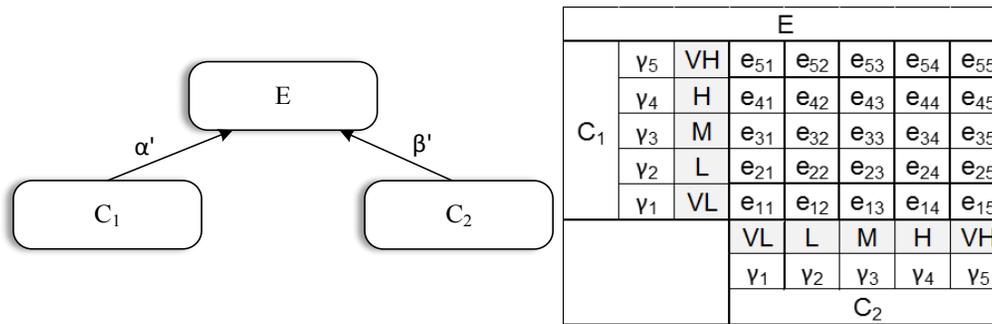


Figure 13. Illustration of the cause-effect relation and the parameter for transformation

Step 2. Calculating the individual effect vector: In order to sharpen the difference between the levels of the state, we convert further state e_{ij} to n_{ij} in which $n_{ij} = k^{e_{ij}}$, $k > 0$. So we have $n(VL) = k$, $n(L) = k^2$, $n(M) = k^3$, $n(H) = k^4$, and $n(VH) = k^5$. We also set the weights for the state of the cause (VL, L, M, H, VH) as $(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5)$ to further differentiate the effect of the state from the other cause (see Figure 13). For each cause, we derive its individual effect vector $r = [r(VL), r(L), r(M), r(H), r(VH)]$ by calculating the individual effect value of each state s_i as:

$$r(s_i) = \frac{\sum_{j=1}^5 \gamma_i n_{ij}}{\sum_{k=1}^5 \sum_{j=1}^5 \gamma_k n_{kj}}, i = 1..5$$

For each of the relations, after obtaining the weight of the factors and the relevant individual effect vectors, we can generate the Bayesian CPT in each of the effect node. Having the 3 CPTs from the 3 FAIR look-up tables is enough to form the overall Bayesian network for calculating the LEF output given the input states of the causes.

Step 3. Generating numerical output: The output of the Bayesian will be a vector of the probability of the state evaluations for the LEF, for example, $[p_1, p_2, p_3, p_4, p_5]$, in which p_1 is the probability that LEF has state VL, p_2 is the probability that LEF has state L and so on. We use the grade vector $[1, 2, 4, 8, 16]$ to derive the final numerical result, in detail, the assessment for LEF is equal to $p_1 + 2 * p_2 + 4 * p_3 + 8 * p_4 + 16 * p_5$. This grade will later be used to compare and rank the threat, according to their LEF.

Step 4. Adjusting Bayesian model for FAIR consistency: Sometimes there may have some inconsistencies between the FAIR and Bayesian model due to the weak correlation of the values in the FAIR table. For example, with the same input state, FAIR output gives a “Low” state, but Bayesian gives a not low numerical output. In such cases, we provide fixed by adjusting the corresponding CPT entry of the Bayesian model based on the upper/lower bound grade according to the FAIR state. In detail, we group 25 FAIR outputs for LEF into 5 categories $[VL, L, M, H, VH]$. In each category, we will replace the FAIR output by the corresponding Bayesian grade (with the same input). We then obtain the value range for each category. If there is no intersection between the value ranges, the Bayesian model is fully consistent with the FAIR assessment. In case there are intersections, we will decrease the upper bound (for instance, decrease to the same value with the second highest upper bound in the same category) or increase the lower bound of the relevant categories accordingly to eliminate all the intersections. We then update all the CPT entries that related to the adjustments. After this stage, we can ensure the consistent assessments with all the 25 inputs that FAIR can provide.



Once produced, our Bayesian model can give the numerical output for the fuzzy inputs that FAIR cannot evaluate, reflecting the assessment trend obtained from the FAIR table, and point out the most influential element. To illustrate the method, we applied it to a list of plausible threats to the smart grids in the next section.

7.3 AN EXEMPLARY APPLICATION OF THE BAYESIANFAIR

The following example highlights the diversity of inputs that our solution can process. As mentioned, more specific examples that are in line with the Threat Navigator are provided in the next sections.

7.3.1 Input to BayesianFAIR to find LEFs

Assume system managers are tasked to consider LEF of 14 threats (Table 15), which were selected from the IRENE list of threats relevant to Smart City components and connections [1].

Table 15. List of cyber-threats to consider a factory within a smart grid evolution step

ID	Threat	ID	Threat
1	Perimeter network scanning	8	Exploit physical access
2	Information gathering	9	Exploit unauthorized access
3	Reconnaissance	10	Exploit split tunneling
4	Craft phishing attacks	11	Exploit mobile systems
5	Create and operate false front organizations	12	Exploit recently vulnerabilities
6	Sniffers/Scanning	13	Compromise design, manufacture, and/or distribution of information system components
7	Insert subverted individuals	14	Compromise software of organizational critical information systems.

This example assumes that experts agreed that some threat factors can be defined in-between some states (not as 100% Medium, High, or other). For instance, one of agreed fuzzy states can be described as [40%M, 60%H], which means that there is a 40% believe that the factor has ‘M’ state and 60% believe of having an H state. Another example is [20%VL, 20%L, 20%M, 20%H, 20%VH] which implies that no information about a specific factor can be defined: all states have equal probabilities. Therefore, the input should support such structure.

It is worth noting that the latest example is here to illustrate the flexibility of the method, which can be misleading if experts possess no proper understanding of the mechanics behind calculating LEF from input data. Importantly, experts should be aware of their responsibility for the accurateness of the input states of the FAIR factors. In case the users use a (considerably) fuzzy input, they should be conscious



that the accuracy of the evaluation will be lowered. Still, this example shows that the suggested method can still provide them an idea of how severe the threat can be, which cannot be achieved when using FAIR.

Let us therefore assume that experts derived input for the 14 threats for which the input was decided clearly for all except for the threats “Exploit unauthorized access” (ID:9) and threat “Physical compromise” (ID:13). In the first case, the experts were not able to assign either the “Medium” or “High” state for the “Threat Capability” factor, while for threat 13 the experts were not sure about the state of the *Action* factor.

Although classical FAIR look-up tables do not support threat assessments such as this one, our method enables applying the FAIR approach even with such type of input. The details of how to apply the method to the LEF element of the FAIR taxonomy and propagating the data to obtain output values are described next.

7.3.2 The result of applying BayesianFAIR

The first step of our method transforms the FAIR tables into the factor weights as can be seen in Figure 14. The individual effect vectors of the TEF, Vulnerability, *Contact*, *Action*, *TCap* (*Threat capability*), and *Control Strength* is given in Table 16. We form the Bayesian network from these input and the formula presented above.

We use this Bayesian model to assess the threats according to the input given by the expert. In case of fuzzy input, we give probability for each state of the factors according to the experts’ opinions. For example, we assign the input of ID:9 to be 40% L and 60% M. If there is no expert opinion available, we will give an equal probability for each state, for instance, the input of ID:13 can be set up to assign 20% for each State. The comparison results of the FAIR and the Bayesian-FAIR for assessing the threats is presented in Table 17.

The BayesianFAIR also allows users to see the impact of the change of a fuzzy input in the overall assessment. By assessing the change of such input, we obtain the upper and lower bounds of the evaluation, as well as see its trend when changing the probability of the input. We illustrate this idea by assessing the threat 13, when the *Action*’s input state cannot be identified, while the other three factors [*Contact*, *Tcap*, *Control Strength*] are set to [VL, L, VL]. We calculate different evaluation grades when changing the fuzzy input of *Contact*, from [100%VL] to [20%VL 20%L 20%M 20%H 20%VH], [40%VL 15% L 15%M 15%H 15%VH], [60%VL 10%L 10%M 10%H 10%VH, ..., and [100%VH]. The lower bound of the calculated value is 264.49 where factor *Action* is at its lowest state “VL”, while its higher bound is 531.3 for an input at its highest state “VH”. A number of LEFs calculated by Bayesian-FAIR using different inputs is shown in Figure 15.

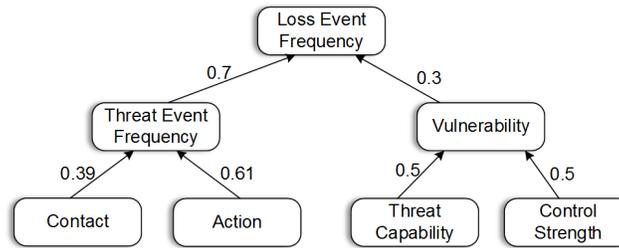


Figure 14. The FAIR model with the factors' weight

Table 16. The individual effect vector for factors in the FAIR model

Factor	Individual effect vector
TEF	[0.62, 0.25, 0.09, 0.03, 0.01]
V	[0.37, 0.3, 0.23, 0.08, 0.02]
Contact	[0.42, 0.34, 0.18, 0.05, 0.01]
Action	[0.5, 0.34, 0.13, 0.03, 0.01]
Tcap	[0.49, 0.3, 0.15, 0.05, 0.01]
Control	[0.01, 0.05, 0.15, 0.3, 0.49]

Table 17. Numerical results of the BayesianFAIR to compared to FAIR

ID	Input state [Contact, Action, Tcap, Control Strength]	FAIR	B-FAIR	Grade	Log2(G/100)	Rank	MF(**)
1	[M, H, M, M]	H	[12.7, 16.9, 25.3, 39.9, 5.2]	889.5	3.15	7	C
2	[VH, H, M, H]	H	[10.6, 12.7, 16.9, 21.7, 38.1]	1016.9	3.35	4	C
3	[M, M, VL, L]	L	[16.9, 25.3, 43.5, 9.1, 5.2]	571.7	2.52	10	A
4	[H, H, VH, H]	H	[10.6, 12.7, 16.9, 21.7, 38.1]	1130.3	3.5	3	A
5	[M, VH, H, VL]	VH	[5.2, 9.1, 16.9, 25.3, 43.5]	1147.1	3.52	1	A
6	[M, H, H, M]	H	[9.1, 16.9, 25.3, 43.5, 5.2]	923.1	3.21	6	C
7	[M, H, H, VL]	H	[7.3, 13.3, 25.3, 43.5, 10.6]	939.9	3.23	5	CS
8	[L, M, L, H]	VL	[25.3, 43.5, 16.9, 9.1, 5.2]	342.9	1.78	13	A
9	[H, M, 40%M-60%H, VH]	n/a	[11.8, 14.3, 25.3, 27.1, 21.5]	290.33	1.54	14	A
10	[L, H, H, M]	M	[13.3, 25.3, 43.5, 12.7, 5.2]	685.1	2.78	9	C
11	[VH, H, VH, H]	VH	[7, 12.7, 16.9, 25.3, 38.1]	1147.1	3.52	1	C
12	[H, M, H, VH]	M	[12.7, 16.9, 25.3, 39.9, 5.2]	809.7	3.02	8	A
13	[VL, E(*), L, VL]	n/a	[39.9, 25.3, 16.9, 12.7, 5.2]	343	1.78	12	A
14	[M, L, H, M]	VL	[39.9, 25.3, 16.9, 12.7, 5.2]	397.4	1.99	11	A

(*): State E indicates the equal probability of 20%VL – 20%L – 20%M – 20%H – 20%VH (**): MF: Most influential factor

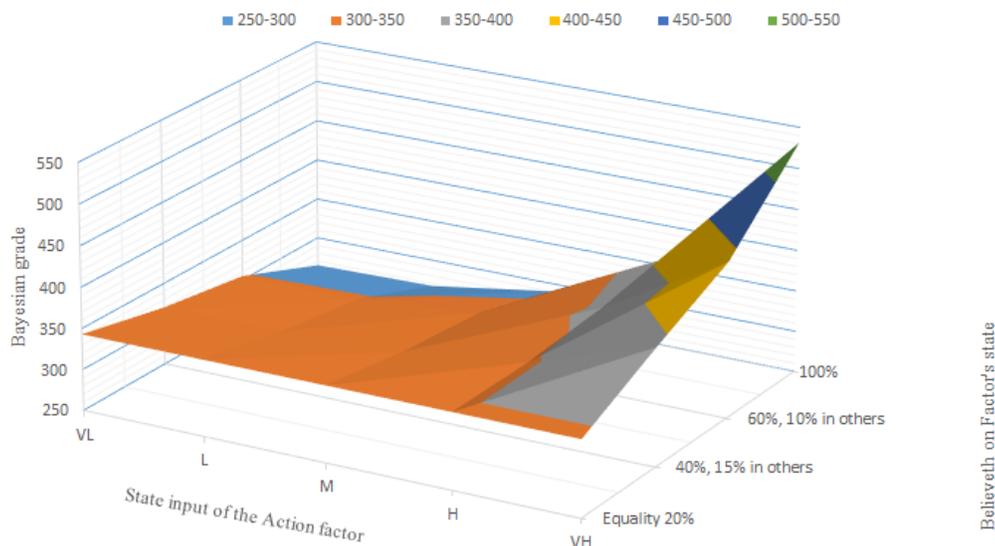


Figure 15. Evaluation of LEF by Bayesian-FAIR with limited state input of the *Action* factor

Table 17 shows that a Bayesian network constructed using the proposed method, generates an assessment consistent with the FAIR framework. Moreover, our approach can differentiate further threats in the same category. For example, threat 6 and 7 are in the same “High” category, according to FAIR, but having the grade of 923.1 and 939.9 respectively according to our approach. From the table, we can see that 6 and 7 have the same assessments for the three inputs [C, A, and Tcap], the only difference being the evaluation of factor “CS”. Threat 7 has “VL” state compared to “M” of threat 6, so LEF of 7 should be higher than LEF of 6. This difference cannot be shown by FAIR as both of the threats are in the ”H” category, but it can be seen clearly from our Bayesian model.

In addition to providing a repeatable and traceable way to reach conclusions, even in case of uncertainties, we supply a clear mechanism for integrating a threat threshold. Having the threat grades, we can simply define the cut out point to reduce the list of threats to consider. For example, a cut out point of 900 means threats are only considered when their grade is higher or equal to 900, which will reduce the list of threats to {2, 4, 5, 6, 7, 11}.

Our model also has the capacity to produce output even with fuzzy input. For example, in case of threats 9 and 13, we can give the assessment grades of 290.33 and 343 respectively, while the FAIR model cannot provide the exact state. This is helpful when there is a lack of expert opinions for assessing the threats, or experts have conflicted assessments of the threats.

Another advantage is that our approach can point out the most influential factor for each of the threats to assess. These outputs then can be combined to show which factor should be improved to lower the threat impact. For example, considering the 14 threats in Table 15, we see that the “A” factor is the one that affects the most, with 8/14 of the threats. This suggests to the system managers that they should implement countermeasures to lower the *Action*, for example, by creating policies that increase punishment on the attackers that initiating such threats, so as to lower the motivation of attacking. Such



countermeasures will lower significantly the impacts of 8 threats in the list, hence, effectively improving the security system with the least effort considering the 14 threats.

All in all, the ability to assess cyber-threats is becoming more and more important for stakeholders, given their rise in smart grid. In this section, we proposed a method to transform the FAIR look-up tables to the Bayesian network model to provide numerical threat LEF assessment. We showed that our method gives a consistent assessment with FAIR, while providing some advantages, such as differentiating threats with the same FAIR inputs; giving more granular output; allowing flexible fuzzy inputs; and having the capability to highlight the most influential cause of particular threats. We believe that this FAIR-based model can help the system manager in planning more effectively the security countermeasures to lower the smart grid threats' impact.



8 THREAT NAVIGATOR⁷

This section builds on the outlined kill chains and BayesianFAIR. Herewith we propose a method, named Threat Navigator, to cluster adversarial threats in connection to specific classes of attackers and position them next to each other.

The method takes as input the list of threats from [D2.1](#) [1]. This list is compiled by considering specifics of a grid structure in three steps:

1. Identifying threats relevant to individual grid components (or features). This task concerns selecting threats from the list of structural threats assigned to each building
2. Accounting for threats to categories of buildings, as each building inherits threats specific to its category. These category-specific structural threats extend the outcome of step 1.
3. Complementing the list with emerging threats (caused by interactions of components).

The Threat Navigator:

1. Assigns a generic threat list to kill chains for different classes of malicious actors. These chains are used as a ‘sifting structure’ to remove threats less relevant to specific classes of attackers based on attackers’ *Capabilities* and *Focus*. Thus, instantiated kill chains per grid feature or component are constructed.
2. Accounts for implemented mitigations;
3. Calculates Loss Event Frequencies to threats from each kill chain using BayesianFAIR. The output of this step provides threat events grouped by LEF for each attacker class.

This section illustrates mechanics of applying the Threat Navigator to a simplified case.

8.1 CALCULATING LEF OF THREATS FOR INDIVIDUAL BUILDINGS

This subsection takes a simple example to illustrate how the Threat Navigator can be used to consider LEF of threats in relation to each other. For this, we illustrate how to calculate LEFs of threats relevant to a Factory feature within the initial stage of an urban smart grid (Figure 16). This feature includes both the Factory and the Long-Range Connector needed to connect the factory to the grid. A number of threats relevant to this feature can be identified according to D2.1 as: FFactory (factory with Long-Range Connector) connection: {5, 13, 22, 23, 30, 36, 37, 2, 3, 7, 8, 12, 14, 19, 26, 28, 32, 33, 34, 35, 1, 3, 6, 15}.

⁷ This chapter was published as: Vasenev, A., Montoya, L., Ceccarelli, A., Le, A., Ionita, D.: Threat navigator: grouping and ranking malicious external threats to current and future urban smart grids, SmartGifts conference on smart grid inspired future technologies, 2016.

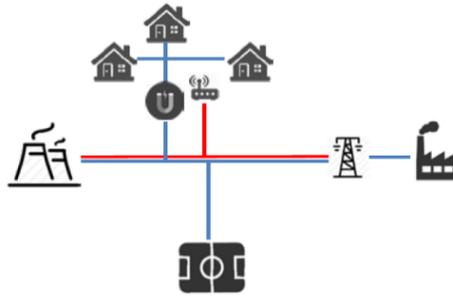


Figure 16. Initial stage of the grid

According to the *Focus* property we can highlight which classes of attackers should be considered for this feature. The excerpt of the table shown in Table 18 indicates that both Factory and the Long-Range connector are linked to classes C2 and C3 of attackers.

Table 18. Attacker classes relevant to the factory feature

N	Component name	C1	C2	C3
6	Long-Range Connector	-	X	X
10	Factory	-	X	X

Applying the filtering based on the *Capability* of threat actors from “IRENE threat events list attributed to threat actors”, we can filter FFactory threats with respect to attacker classes C2, and C3. Table 19 illustrates threats:

- To be considered for a particular attacker class (denoted as “X” in the following table);
- Not attributed to a specific class (marked as “|”);
- Absent in the list of threats of this feature (“-”), although should be considered in principle given the *Capability* of threat actors.



Table 19. Threats relevant to the factory feature

Steps of kill chain	Considered threats (highlighted)	Relevance to Class C1	Relevance to Class C2	Relevance to Class C3
PRGI	1		X	X
	2		X	X
	3		X	X
CCAT	4	-	-	-
DIIMC	5			X
	6		X	X
	7			X
EC	8		X	X
	9	-	-	-
	10	-	-	-
	11	-	-	-
	12	X	X	X
	13			X
	14		X	X
CA	15		X	X
	16		X	X
	17	-	-	-
	18	-	-	-
	19			X
	20		-	-
	21		-	-
AR	22		X	X
	23	X	X	X
	24	-	-	-
CC	25	-	-	-
	26			-
	27			-
	28			X

Thus, the list of relevant threats to the feature includes:

- For C2: C2_Factory_feature_threats= {1, 2, 3, 6, 8, 12, 14, 15, 22, 23, 26};



- For C3: $C3_Factory_feature_threats = C3_Factory_feature_threats + \Delta_{C2-C3}$, where Δ_{C2-C3} corresponds to threats to be considered relevant to C3 but less to C2. For the factory feature this list includes threats {5, 7, 13, 19, 28}.

Mitigations to each threat (taken from D2.1) can be grouped according to C2 or C3 (Table 20).

Table 20. Threats and mitigations relevant to the factory feature

	Threat	Relevant mitigations
C2 threats	1	11, 12, 18
	2	11
	3	4, 12, 16, 19
	6	4, 17, 19
	8	1, 4, 12, 15
	12	8, 10, 13, 16
	14	4, 5, 19
	15	2, 12, 18
	22	1, 8, 11, 19
	23	1, 8, 10, 11, 13, 19
	26	4, 9, 10, 12
Δ_{C2-C3} threats	5	5, 17, 19
	7	1, 2, 4
	13	5, 17, 19
	19	2, 4, 12
	28	4, 9

The result of analyzing which actors can pose threats to specific grid features provides us with:

- A list of threats relevant to C2 actors for the grid feature, including threats that should be considered if a more advanced class should be taken into account;
- A list of mitigations relevant to these lists of threats. This provides us with a checklist of mitigations that can be implemented to make the feature more robust to attacks related to a specific class.

To rank threats for a specific building we calculate LEFs (Loss Event Frequencies) using the BayesianFAIR. Four parameters should be accounted, namely [*Contact*, *Action*, *Threat Capability*, *Control Strength*]. While the first three are known by profiling the attackers, the last one is derived based on what measures are in place. The LEF value for each threat can be found by calculating BayesianFAIR value based on Table 21.

**Table 21. Operationalizing threat parameters as FAIR constructs**

	Contact (FAIR concept)	Action (FAIR concept)	Threat Capability	Control Strength
C1	Low	Low	Low	% of implemented controls
C2	Medium	Medium	Medium	
C3	High	High	High	

Thus, if no mitigations are in place, LEF can be calculated by providing four inputs to the BayesianFAIR:

- C2 threats {1, 2, 3, 6, 8, 12, 14, 15, 22, 23, 26} calculations take values [Medium, Medium, Medium, Very Low] as an input vector;
- C3 threats (C2 threats + {5,7,13, 19, 28}) are calculated by taking the vector [High, High, High, Very Low].

The input vectors for calculating LEF would be different if some mitigations were implemented. As one mitigation measure improves controls to several threats at once, the threat ranking will be updated. Essentially, as interrelations between the threats and mitigations are intricate, implementing one mitigation can result in changes of input vectors to several threats.

Table 22. Identifying degree of implemented controls as a FAIR construct

	Threat number	Relevant mitigations	% of mitigations implemented	Qualitative characterization of controls
C2 threats	1	11, 12, 18	0%	Very Low
	2	11	0%	Very Low
	3	<u>4</u> , 12, 16, 19	25%	Low
	6	<u>4</u> , 17, 19	33%	Medium
	8	1, <u>4</u> , 12, 15	25%	Low
	12	8, 10, 13, 16	0%	Very Low
	14	<u>4</u> , 5, 19	33%	Medium
	15	2, 12, 18	0%	Very Low
	22	1, 8, 11, 19	0%	Very Low
	23	1, 8, 10, 11, 13, 19	0%	Very Low
	26	<u>4</u> , 9, 10, 12	25%	Low
Δ_{C2-C3} threats	5	5, 17, 19	0	Very Low
	7	1, 2, <u>4</u>	25%	Low
	13	5, 17, 19	0	Very Low
	19	2, <u>4</u> , 12	25%	Low
	28	<u>4</u> , 9	25%	Low



In this example we assume that a mitigation number 4 (Security Assessment and Authorization) was implemented wrt to the list of threats relevant to the Factory feature. The update on control to threats concern threats {3, 6, 8, 14, 26} for class C2 (Table 22). Similarly, we can find the change in controls to threat {7, 19, 28} relevant to the transition from C2 to C3.

Thus, controls for several threats {3, 8, 26, 7, 19, 28} are improved from 0 to 25%, while for others controls increase up to 33% {6, 14}. With the change of controls the LEF of each threat changes. We can re-calculate LEF for the listed threats. For instance, with controls increased up to 25% for class C2 domain experts can suggest to calculate LEF using the input vector described as [Medium, Medium, Medium, Low] and as [Medium, Medium, Medium, Medium] to calculate LEF for threats with more relevant mitigations implemented. Thus, calculations of LEFs for C2 class can be conducted using BayesianFAIR as follows:

- For threats without mitigations implemented {1, 2, 12, 15, 22, 23, 26} input data corresponds to [Medium, Medium, Medium, Very Low]. The obtained probability of the LEF vector [Very Low; Low; Medium; High; Very High] using the BayesianFair approach described above is [0.013; 0.045; 0.503; 0.265; 0.174]. The value of Loss Event Frequency is 701.9;
- For threats with 25% mitigations covered {3, 6, 8, 14, 26} input is [Medium, Medium, Medium, Low]. The LEF vector is [0.013; 0.045; 0.503; 0.286; 0.153] with LEF value 685.1;
- For threats with 33% increase in mitigations {6, 14}, input for calculations is [Medium, Medium, Medium, Medium]. The LEF probability vector is [0.013; 0.045; 0.545; 0.265; 0.132] with LEF= 651.5.

Analysis of output vectors for C2 threats and their LEF values suggests that the LEF value decreases non-linearly. The decrease in LEF for threats with only one mitigation implemented is found to be 17. Two mitigations implemented provided LEF with a decrease of 50. With increase in the amount of mitigations, the contribution of the Medium element of the vector to the LEF value is increasing, while the contributions of the Very Low and Low elements of the vector stay the same. At the same time, the contributions by the Very High vector element to LEF is decreasing. This dynamic is in line with the intuition that for ‘Medium’ events the LEF calculated using FAIR tables is expected to stay medium.

Threat groups relevant to C3 obtain the following LEF value:

- For threats without mitigations implemented {1, 2, 5, 12, 13, 15, 22, 23, 26} the input vector is [High, High, High, Very Low]. Results are [0.013; 0.0502; 0.1396; 0.2746; 0.5226] and LEF = 1123.02;
- For threats with 25% mitigations covered {3, 6, 7, 8, 14, 19, 26, 28} input [High, High, High, Low] leads to [0.013; 0.0694; 0.1421; 0.3306; 0.4449] with LEF = 1048.34;
- For threats with 33% mitigations covered {6, 14} — [High, High, High, Medium] — the output LEF vector is [0.013; 0.082; 0.1443; 0.3265; 0.4342] and LEF= 1031.34.

Similarly to C2 threats, the LEF value decreases. With one implemented measure it lowers by 75 and with two mitigations in place it decreases by 92. The contribution of the High element of the LEF probability vector increases. Figure 17 shows changes in the LEF values of provided threats. Some



LEF values can potentially be cut-off targets and stakeholders might wish to introduce sufficient mitigations to obtain LEF values less than these thresholds.

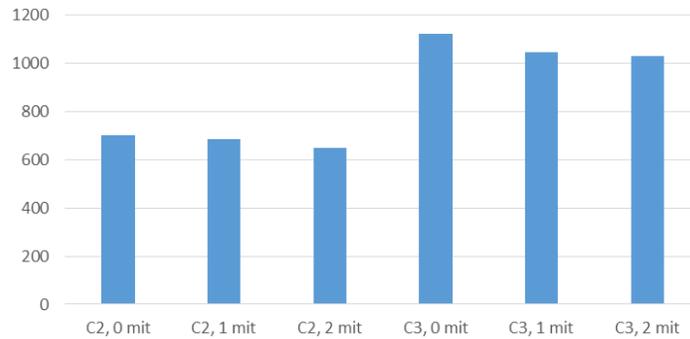


Figure 17. Ranking groups of threat events

This simplified example illustrates mechanics of calculating LEF values for groups of threats using the Threat Navigator. Clearly, individual threats can hardly be grouped in reality. Also, a non-linearity increase of *Control Strength* value could be expected due to the degree that specific mitigations counter particular threats non-linearly. Thus, LEF for each threat should be accounted for separately. In a more realistic scenario, the increase of controls might be assigned by experts. The Threat Navigator allows for such functionality and provides experts with a structured way to do so.

Clearly, due to variety of possible mitigations implemented and sets of threats to specific grid components or features, it is not possible to provide a comprehensive table for all possible variations. However, as this section illustrates, the Threat Navigator can help in ranking threats and can be easily implemented in software to rank threats. It is the flexibility embedded into the BayesianFAIR method that assists in defining input vectors (including the parameter characterizing *Control Strength*) with significant flexibility.

Ultimately, this approach can suggest which countermeasures should be implemented to increase controls to multiple threats at once. In this way, it can assist in answering the question of what are the most cost-efficient mitigation strategies to implement.

8.2 POSSIBILITIES TO APPLY KILL CHAINS FOR OTHER TASKS

Kill chains of threats imbedded into the Threat Navigator could be integrated into other methodologies to assess risks to critical infrastructures. For instance, the RASTER (Risk Assessment by Stepwise Refinement) method [43] that concentrates on telecommunication services can elaborate classes of possible attackers to consider more relevant threats to services and infrastructures. Some other examples of using kill chains are presented next.

8.2.1 Identifying exposure of the city to adversarial threats and ongoing campaigns

It is possible to categorize all threats to the urban grid to indicate how many grid components are exposed to similar threats. For this, it is needed to project all threats relevant to a specific grid configuration on kill chains of different actors. This mapping for an exemplary scenario (an initial grid configuration) can be as follows.



For the configuration of the grid from the previous example all threats for the features include the following sets:

- F1. Household feature {2, 3, 7, 8, 12, 14, 19, 26, 28, 32, 33, 34, 35};
- F2. FInternet feature {3, 5, 6, 7, 8, 14, 19, 22, 26, 27, 28, 30, 32, 33, 34, 35};
- F3. Factory feature {4, 9, 11, 23, 24, 29, 30, 37, 1, 3, 6, 15, 33};
- F4. Stadium feature {4, 9, 11, 23, 24, 29, 30, 37, 33, 14, 16, 18, 19, 31, 37};
- F5. CarbonProd feature {5, 13, 22, 23, 30, 36, 37, 2, 3, 7, 8, 12, 14, 19, 26, 28, 32, 33, 34, 35, 1, 3, 6, 15}.

These threats can be related to threat categories as shown in Table 23 (Legend for the table: “X” — identified threat, “|” - not considered for this malicious class, “-” - no threats of this type).

This way of mapping shows how many grid components are susceptible to the same either adversarial or non-adversarial threat. For adversarial threats, it also represents the number of threats relevant to a specific kill chain element. A decision maker, on the basis of the table, can consider several ways to reduce exposure of the grid to re-occurring threats. Relevant aims include:

- Reducing often re-occurring threats. Because of intricate connections between threats and mitigations, several of such threats can be potentially addressed by a single mitigation measure. This approach concerns selecting relevant mitigations on the scale of the city and complements the previously described application of the Threat Navigator to individual grid components;
- Full threat mitigation of one or more adversarial categories. This could assist in breaking a kill chain of a malicious actor. A result can be reduction of exposure to campaigns for specific actors. For instance, if a specific step of the C2 kill chain is fully covered by mitigations measures, more advanced actors (C3) might be needed to conduct large scale attacks against the grid.

In addition to supporting the decision maker in selecting mitigation measures, the mapping described in this subsection can potentially assist in identifying ongoing attacks against the grid. This suggestion departs from assumptions that: (1) kill chains can adequately describe sequences of steps within an attack that an attacker should complete, and (2) NIST 800-30 has a kill chain structure in its core. These assumptions suggest that the hereby outlined kill chains, due to the inherent NIST-complied structure, can be used to account for campaigns against an urban smart grid. Therefore, if several malicious events identified within the city can be linked to different steps of the kill chain, it can be assumed that there is an ongoing attack against the city grid.



Table 23. Exposure of the grid to attacks from specific actor classes

Threat type	N	Threats per feature					Grid exposure to threats		
		F1	F2	F3	F4	F5	exposure to C1 kill chain	exposure to C2 kill chain	exposure to C3 kill chain
PRGI	1			X		X		XX	XX
	2	X				X	XX	XX	XX
	3	X	X	X		X		XXXX	XXXX
CCAT	4			X	X		XX	XX	XX
DIIMC	5		X			X			XX
	6		X	X		X		XXX	XXX
	7	X	X			X			XXX
EC	8	X	X			X		XXX	XXX
	9			X	X		XX	XX	XX
	10							-	-
	11			X	X		XX	XX	XX
	12	X				X	XX	XX	XX
	13					X			X
	14	X	X		X	X		XXXX	XXXX
CA	15			X		X		XX	XX
	16				X			X	X
	17						-	-	-
	18				X		X	X	X
	19	X	X		X	X			XXXX
	20							-	-
	21							-	-
	22		X			X		XX	XX
AR	23			X	X	X	XXX	XXX	XXX
	24			X	X		XX	XX	XX
	25						-	-	-
CC	26	X	X			X		XXX	XXX
	27		X						X
	28	X	X			X			XXX
ACC	29			X	X		XX		
	30		X	X	X	X	XXXX		
	31				X		X		
ENV	32	X	X			X	XXX		
	33	X	X	X	X	X	XXXXX		
	34	X	X			X	XXX		
	35	X	X			X	XXX		
HI	36					X	X		
	37			X	X	X	XXX		
	38						-		



8.2.2 Updating estimators

Kill chains can also provide a foundation for performing consistent updates to risk assessment. Interrelations between threats outlined above can be used to re-calculate LEFs of threat events if some of the linked events are observed.

Conducting an update using kill chains might be also necessary once new information relevant to history/intent of threat sources is available. Such information, as [44] suggest, can be of different types:

- Historic interest: there is documented evidence or speculation that the adversarial group has shown interest in this type of facility of this specific facility;
- Historic attacks: there is documented evidence or speculation that the adversarial group conducted similar attacks in the past at this facility of this type of facility;
- Current interest in facility;
- Current surveillance: if intelligence documents surveillance at specific facility or other similar facilities in the region;
- Documented threats: if the facility has received documented threats from this (or similar) adversarial group.

In summary, the presented Threat Navigator approach can assist in calculating LEFs of threat events using root-cause analysis of adversarial threats described in section 6 and BayesianFAIR presented in section 7 of this deliverable.

The Threat Navigator can be extended. New relevant threats can be considered in addition to IRENE threats from D2.1. The next section briefly overviews what new accidental threats can be relevant to consider during assessment of future urban smart grids.



9 NEW ACCIDENTAL THREATS

Smart grids, similar with other critical infrastructures, operate in complex environments. To account for accidental threats not previously considered it is necessary to look at how the grid interacts with the environment as a human-supervised cyber-physical system.

NERC (North American Electric Reliability Corporation) together with US Department of energy listed some HILF (High-Impact, Low-Frequency) risks for future grids that look beyond commonly considered events. These risks include coordinated cyber, physical, and blended attacks, the high-altitude detonation of a nuclear weapon, and major natural disasters like earthquakes, tsunamis, large hurricanes, pandemics, and geomagnetic disturbances caused by solar weather [17]. Looking at HILF threats can assist in identifying new accidental threats for future urban grids.

Among HILF threats electromagnetic threats are particularly relevant to cyber-physical systems. These HILF threats can be linked to IT components of the grid, which provide communications and control functionality, or to electrical equipment. Both these layers are susceptible to influences from both cyber and physical domains. Although the IRENE threat event list accounts for threat events related to physical or cyber-physical aspects of the grid already (threat events 19 and 20), further structural analysis of interrelations between cyber and physical domains would be useful to identify new accidental threats and future.

This sections considers possible new accidental threats not covered in [D2.1](#). In this attempt, we adopt a differentiation between IT and electric components of the grid and consider cyber and physical aspects of relevant threats. Firstly, we concentrate on electromagnetic threats. Next, we illustrate how attacks from either cyber or physical domain can result in both domains. Finally, we summarize what threats can be considered in addition to the IRENE threat list from D2.1.

9.1 ELECTROMAGNETIC INCIDENTS

Both electricity and control layers of smart grid are susceptible to disturbance in the electromagnetic spectrum. These disturbances can be related to malicious and non-malicious threats. This subsection outlines the role of electromagnetic spectrum in smart grids and looks at related threats and their potential impacts. Three types of electromagnetic incidents — geo storms, high-altitude electromagnetic impulse, and intentional electromagnetic interference — are briefly covered.

Electromagnetic spectrum is widely accepted as being an important and pervasive element to multiple interconnected systems including smart grids. Corresponding disturbances can upset or even destroy not only IT grid components, but also electrical components of the grid. HILF threats related to electromagnetic spectrum can stem from natural (solar storms) and human-originated (nuclear weapons or intentional electromagnetic activities) events.

An example of undesirable electromagnetic disturbances are geomagnetic storms. This *non-malicious* threat is linked to rapid changes in the configuration of Earth's magnetic field caused by intense solar activity, particularly large solar flares. These storms develop rapidly and result in widespread impact to many points of the system by inducing currents into the grid. As a result of this impact, multiple transformers may be damaged due to the unusual mode of operation. For example, in 13 – 14 March 1989 a geomagnetic storm led to the collapse of the Hydro Quebec system. It took nine hours to return



power to 83 percent of the affected Quebec customers. Two large step-up transformers were damaged because of overvoltage conditions. In England, the March 1989 storm is suspected to have caused damage to two 400 kV transformers [17, p. 64].

As widely acknowledged, *malicious* disturbances in the electromagnetic spectrum can have a large scale effect as well. For example, the importance to account for cyber-electromagnetic activities (CEMA) was highlighted in US Army Doctrine Publication (ADP 3-0), Unified Land Operations, and ADP 6-0, Mission Command. The corresponding activities cover both cyberspace and electromagnetic spectrums and include cyberspace operations, electronic warfare, and spectrum management operations. Electromagnetic spectrum is pervasive and therefore concerns all five traditional military domains (space, air, land, maritime, and cyberspace) [45].

A nuclear detonation that leads to an electromagnetic pulse (EMP) is an example of a malicious attack. Several types of EMP can be differentiated, including source-region EMP (EMP is considered next to radiation), system generated EMP (e.g. when x-rays strike a satellite), and high-altitude EMP (HEMP). The latter category includes detonation at altitudes above 30 km and is commonly seen as a high-impact, low-frequency threat event for the grid.

HEMP, as well as other EMP types, can heavily impact the grid in a number of ways. Main areas of concern with respect to HEMP include: HV substation controls and communications; power generation and control room computers and communications; distribution line insulators; and distribution transformers. Three types of HEMP can be differentiated (E1, E2, E3 — early, intermediate, and late time) with different energy levels and various generation mechanisms. On their impact to the grid they can be compared to an electrostatic discharge, a lightning ground return stroke, and a geomagnetic storm correspondingly. Due to their specific properties, the three waveforms impact the grid differently. E1 couples efficiently to short lines (up to dozen meters), including overhead power lines. This waveform can induce large voltages and currents to connected equipment, including low-voltage sensor and control lines between transformers and controls. This coupling pose the major threat to commercial-level equipment, including programmable logic controllers and computer controls at power generation facilities and control centers. Pole-mounted distribution transformers may also be damaged, as many of the E1 HEMP transients are expected to be from 200 to 300 kV. Contrary to E1, E2 and E3 waveforms are of concerns for systems that employ long lines (from hundreds of meters to hundreds of kilometers). They can lead to outages of long communication lines, including both buried and above-ground. Because E3 is preceded by E1 and E2, the compound effect of HEMP can exceed the effect of its individual elements. A plausible scenario is when E1 HEMP causes solid-state relays to fail to operate in the first instance, while E3 will damage transformers as the grid collapses without relay protection.

Another malicious EMI threat is Intentional Electromagnetic Interference (IEMI) that corresponds to intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems. IEMI is produced by a high-power repeatable (non-explosive) generator. IEMI threats can employ two mechanisms: either through radio jamming and by means of cables. A radar hampering SCADA operations, as occurred in 1999 [46], is an example of the first mechanism. In another case, IEMI coupled with a cable can not only upset, but also destroy a grid component. Relevant research suggested that a pulse current of 20 kA in a grounding circuit of a substation can



cause the failure of the power supply to a medium city [47]. The STRUCTURES project provides some relevant examples in its D2.2 “Review of possible IEMI threats”.

IEMI threats should be seen as being different from HEMP. Compared to E1 HEMP, IEMI environments are a local threat with the range typically less than 1 km. Besides, it is less effective than E1 in coupling to lines longer than 10 meters as the environments tend to decrease as $1/r$ from the EM weapon source. The maximum induced voltage of IEMI is about 10 kV. As a result, IEMI pose lesser threat to distribution line insulators and transformers. Therefore, the interference are mainly relevant to consider with respect their impacts to programmable logic controllers and computers than to electrical equipment.

It is worth noting that IEMI threats are more relevant to consider for future urban grids (compared to HEMP) as threat actors require a lower level of organization to acquire and operate them. Such systems can range in size from a 40’ container (77 m³) to a portable case (e.g. 0.05 m³) and differ in their mobility, technological challenge and threat level [48]. For instance, large 80 m³ Swedish Microwave Test Facility (MTF) that can be transported by a truck. This highly sophisticated system can be constructed with knowledge of engineering spiciest and require advanced radar system. At the same time, IEMI systems can be very mobile, such as DIEHL DS 110. With medium technical complexity and moderate cost, DS 110-level system can be constructed by a trained technician supported with open literature.

Located in a suitcase, a mobile IMEI system can be brought to a desktop computer or a similar target to the range of less than 1 m. This leads to the need to account how facilities are protected against IEMI threats. Susceptibility, consequence, and accessibility of the facility can be used to account for specific IEMI threats [49]. A more advanced analysis might involve accessing electromagnetic topology of the buildings together with fault tree of the system, e.g. with the help of probabilistic techniques [50].

In the context of IRENE, it appears to be relevant to consider IEMI threat events as they can directly influence IT components of the grid even though the attack starts in the physical domain. The following subsection illustrates this and other threats that have the similar property.

9.2 PHYSICAL-TO-CYBER AND CYBER-TO-PHYSICAL ATTACKS

As a future urban electricity network is a cyber-physical system, cyber or physical attacks can be conducted in both domains and can result in consequences in either cyber or physical worlds. For instance, threats originated from the cyber-world can take control over an IT component and lead to some physical damage. The opposite is relevant to the introduced above IEMI (Intentional Electromagnetic Interference) threat events. This subsection considers the interrelations between the way of conducting an attack and its consequences by approaching how physical threats can impact the cyber domain and vice versa.

An extensive description on physical threats to the information infrastructure is provided in Chapter 22 of the Computer Security Handbook [51]. The taxonomy outlines several types of threats:

- General threats:



- a. Natural Hazards: Atmospheric (severe weather events, extreme cold or hot weather), Geologic, Hydrologic (riverine flooding, dam failure, and prolonged drought), Seismic hazards, Major volcanic eruptions, Wildfire, Blight or infestation, Sunspot activity (including magnetic storms);
 - b. Health threats (pandemics, e.g. West Nile virus);
 - c. Man-made threats (such as deliberate actions, wiring runs and exposed wire, intrusions);
 - d. Wiretaps (intrusion to copy data);
 - e. High-Energy Radio-Frequency Threats;
- Workplace violence and terrorism;
 - Other threats (leaks, temperature, and humidity, off-hour visitors, cleaning and maintenance threats, storage-room threats (flammable materials), medical emergencies, Illicit workstations);
 - Local threats (utility disruptions; civil, political, and economic disruptions; and coordinated attacks);

This categorization reflects as well as complements the IRENE threat list. Specifically,

- Natural hazards include a more comprehensive list of *weather events* than the one explicitly mentioned within the IRENE classification. Thus, the IRENE list can be extended with additional elements, such as volcanic eruption, blight, sunspot activities, and severe weather events;
- Health threats and ‘other’ threats from the classification above can be grouped as *control room threats*, as they are mostly concerned with humans and directly access to IT control equipment;
- ‘Local’ threats depend on the context in which the cyber-physical system operates and can be referred to as *situational threats*.

For threats acting in the opposite case — when cyber-originated threats result in physical effects — only some high level mechanisms were described in the literature. It can be explained by the need to consider specific configuration of a system and its functionality to account for possible damages. Particularly, two high level classifications are relevant to consider cyber-to-physical threats:

- Differentiation based on the order of damage [52]: 1st order damage describes what can be done *to actuators*; while 2nd order concerns what can be done *with actuators*. In the latter case, by leveraging forces of the environmental in which the actuators operate, a malicious actor could for instance change the direction and strength of forces under control of the actuators. The resulting events, e.g. ‘water hammers’, could lead to equipment degradation, compromising products, catastrophic destructions, or mass casualties. Such outcomes can be illustrated by the targeted damage of Stuxnet. Other examples may include release of toxic gas from production facilities or untreated sewage into rivers;
- Differentiation based on the potential impacts either to the system or to its environment. For instance, in an example of a quad-rotor UAV as a cyber-physical system [53], cyber-attacks can impact the physical domain in terms of :



- a. the system itself, e.g. related to position, orientation, movement direction, movement speed, angular velocities, motor thrust, physical component life time, physical component structural integrity;
- b. the environment (i.e., ground, buildings, trees; cars, airplanes; people, animals) — safety, structural Integrity. Such impacts should particularly be considered if, for instance a cyber-physical system handles hazardous materials, e.g. chemical or biological substances.

As the second classification complements the first one, results of cyber-attacks can be considered using a simple structure shown in Figure 18.

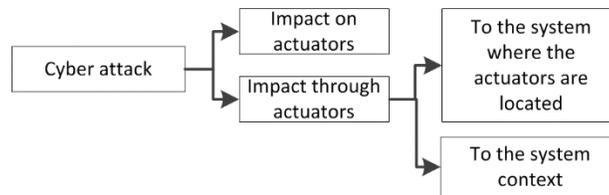


Figure 18. Structure to consider physical results of cyber-attacks

Examples of physical-to-cyber and cyber-to-physical attacks describe in this and the previous subsections can be mapped to cyber-physical systems as shown next.

9.3 MAPPING ACCIDENTAL THREATS

Figure 19 attempts to depict the multiplicity of threats to smart grid as a cyber-physical system, as well as positioning the IRENE event threat list within it. In this way, we highlight new accidental threats that can be considered to complement the IRENE threat event list from D2.1.

Figure 19 illustrates that cyber-attacks can not only pose threats to information security, but also damage the IT layer of the smart grid, which includes information components together with sensors and actuators. Moreover, cyber-attacks can also impede functionality of the grid electrical equipment as a second order impact.

An example of second order impact attacks was demonstrated during the Aurora experiment [54]. During this attack a breaker was opened and closed out of synchronism. The resulting mechanical and electrical stress caused damage to the equipment. Such an attack can damage generators, motors, transformers, and adjustable frequency drives, if they are not adequately protected [55].

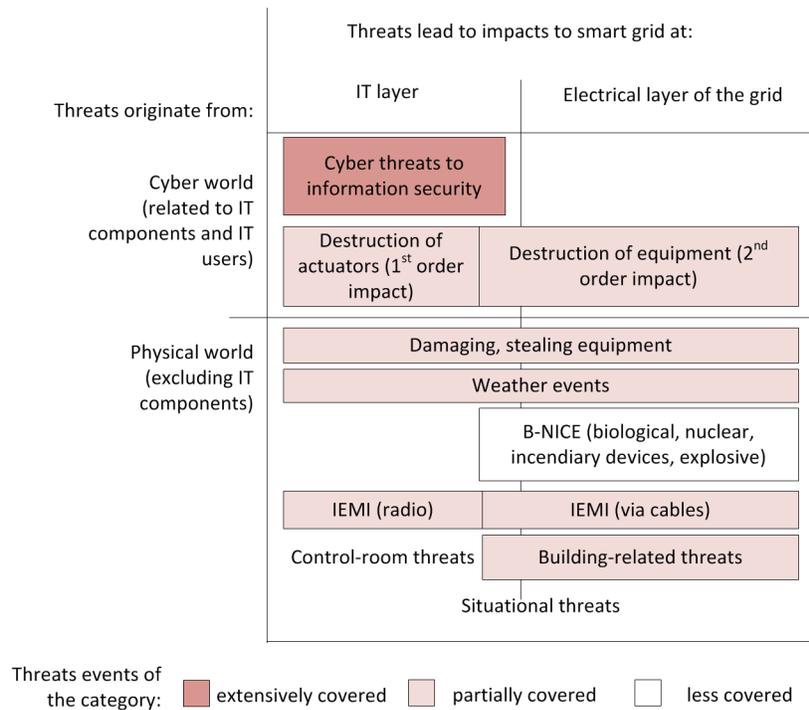


Figure 19. Overview of impacts of threats from cyber and physical domains

Attacks from the physical world can also concern both IT and electrical layers. These attacks can impact unsupervised field equipment (e.g. transformers) of the electric network, as well as equipment located in control rooms. IEMI threats pose a specific example of threats that originate from the physical-world and can lead to impacts in both cyber and physical domains.

The analysis of this mapping can be related to identifying new accidental threats for the future smart grid in the scope of the IRENE project as follows:

- Intentional IEMI attacks appear to be a plausible vector to destruct a physical element of the network or deny its functionality (e.g. to degrade it due to jamming). Therefore, IEMI threats could be considered within the IRENE threat list in more detail. This is particularly relevant for targeted and capable attackers. While conducting cyber-physical attacks is already considered in threat event 20, the preparation of such attacks was not yet seen as a threat event. Specifically, threat 4 that refer to crafting or acquiring tools can be subdivided into: 4a. preparing cyber-attack means (including phishing); 4b. preparing physical attacks; and 4c. preparing attacks with IEMI devices;
- Although the list of natural disasters could be extended with geomagnetic disturbances, this report does not include this threat as being less relevant to urban-scale grids. A more complete risk assessment might include geomagnetic disturbances into the threat list as a subtype of natural disasters;
- Although HEMP events should be considered for a comprehensive risk analysis, this report is not accounting for them due to the scope of the project. Such threats, as well as others related to



biological, nuclear / radiological, incendiary, chemical, and explosive agents (B-NICE), are considered being related to acts of wars, which is out of the scope of this deliverable. A more complete risk assessment might include HEMP threats together with other listed agent;

- Coordinated attacks is a special case of HILF threats. They can be formed by combinations of threats either originated from or resulted to cyber or physical domains. Although a more complete risk assessment can benefit from considering them, it can be an entangled task. Adopting scenario analysis approaches can be suggested to consider such threats. This section provided a solid ground for developing such scenarios by considering interrelations between cyber and physical originated threats.

In connection to new accidental threats it is important to consider not only the grid by itself, but also the context in which the urban electricity networks operate. For example, the grid could operate under stress because of high power demand or high power plant utilization or because of rapid changes or continuously increasing demand can be a pre-condition for a blackout. Therefore, new threat events (alternatively framed as predisposing conditions) could be introduced to consider operations under extreme weather or load conditions.

In summary, threats to future grids cannot be easily listed. We approach considering relevant cyber-to-physical and physical-to-cyber threats as shown in Figure 19. The figure includes an (incomplete) listing of the multiplicity of different threats, including those relevant to human grid operators. It highlights directions for introducing new (and further elaborating existing) IRENE threat events. At the same time, although the described approach to consider accidental threats is helpful to highlight threats related to settings in which cyber-physical systems operate, the number of other threats related to the grid context and acts of war were not considered in this list in detail. Moreover, the list can be potentially extended by accounting for yet-to-be-observed ‘black swans’ or ‘perfect storms’, when simultaneous grid interruption is cause due to a number of accidental events (lines trip on contact with trees, excavation damage, cars crashes into substations, etc.). However, the outlined categorizations provide traceable and relevant connections to a number of domains. These connections can be leveraged in order to extend the list of new accidental threats.



10 DISASTER SCENARIOS

The section provides a description of possible scenarios that could happen in a city following a disaster event. For the needs of this section, a disaster event is characterized as in NIST 800.13: “A disaster event is the multiple severe or catastrophic adverse effect of a threat on organizational operations, organizational assets, individuals, other organizations, or the Nation”. Noticeably, Disaster events can be interrelated. This implies that under undesirable conditions one disaster event can lead to others. Some examples of possible chains are provided in the list of disasters.

Without the aim to be complete, the identification of the events is based on the results of WP2 activities (especially [T2.1](#)), in order to link threats of the IRENE threat list to each disaster event we consider. Completeness in describing all possible disaster events is avoided because it is not feasible to adequately define a generic future city.

This document suggests (and employs for illustrative purposes) the following structure of actions as guidelines to account for specific disasters events:

1. A set of future scenarios feasible for the analysis scope is identified. In this document, we selected a subset of scenarios from T2.1. These scenarios represent the use case smart grids where the disaster events will be defined. The scenarios could be matched, if deemed necessary, to the four elements of the [D1.1](#) matrix (regulated/free, low smart/high smart);
2. A disaster event (or events) should be identified. Guided by the IRENE threat events, we selected such a set of Disaster Events;
3. A number of assumptions should be adopted to describe the future grid and its context. These assumptions are linked to the event likelihood;
4. The disaster events are considered with respect to propagation of the effect through the grid. For this purpose, characteristics of a disaster event should be related to grid specifics (including components that form the grid and the grid topology). As an illustration, we associated likelihoods of disaster scenarios based on disaster events and grid specifics. Noticeable, in the examples below we outline possible likelihood based on personal expectations. To highlight a way of reasoning how to relate grid characteristics to a disaster event we elaborated the considerations for a flood as a case of disaster event.

The rest of this section illustrates the way to consider disaster scenarios in more details.

10.1 EXAMPLES OF DISASTER SCENARIOS

According to the first of the listed steps, we selected several grid configurations from IRENE D2.1:

- Initial configuration (step 1): 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.



- Adding key buildings (step 4): The city administration is influenced from social needs as for example the request of complete decarbonisation and the building of a new hospital to manage the health of the citizens.
- Inserting Storages (step 5): To start the exploiting of smart functionalities storage capabilities were introduced into the grid. Two data and energy storages are added and a basic data control center is installed to provide simple DSR and load balancing strategies.
- Insertion of SCADA System (step 8): Earlier existing Data Center Analysis is replaced by 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.
- Improving decarbonisation (step 10): the city adopts decarbonisation strategy and encourages to take on electric vehicles. A public charging point is inserted in the citizen's area.

Within the second step of the method we chose 7 different disaster events that originate disaster scenarios. Each disaster event is to be described in connection to the mentioned grid configurations.

The disasters can be described as follows:

- **Bomb attack on key connection** — Communications can be broke up by physical attacks aimed to interrupt the exchange of electricity and/or data;
- **Critical functionalities compromised** — Building's employers can be inserted by adversarial organizations to obtain access to critical data or functionalities;
- **Data compromised** — 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;
- **Earthquake impacts on a key building** — Since this component has a physical state, earthquakes can damage it;
- **Theft of energy between components** — If the supply of energy is not well regulated, an attacker can steal energy from the charging point;
- **Substation fire** — A failing circuit breaker can cause a short circuit leading to fire in the substation that destroys substation equipment;
- **Flood** - We look at floods as relatively isolated events that do not cause chain events directly. Although floods can cause wires to short circuit and ultimately lead to a fire, the effect is assumed to be relatively small.

Some disasters (1, 2, and 3) are the results of the occurrence of adversarial threat events, while the others are due to non-adversarial ones (natural disasters, unintentional damages). It is also possible to find disasters due both to structural and emerging threat events, and that involve particular components of the grid.



Table 24. Selected disaster events

Disaster Detail	IRENE Index	Threat Name	Source Type	Threat Type	Involved Components	Potential chain event
Bomb attack on key connection	19	Conduct physical attacks on organizational facilities	ADV	Structural	EC/ DC / MG	substation fire
Critical functionalities compromised	7	Insert subverted individuals into organizations	ADV	Structural	PP / S / H / ...	Data compromised, theft of energy between components
Data compromised	21	Conduct Man in the middle attacks	ADV	Emerging	BDC/SCADA, H	Critical functionalities compromised
Earthquake on key building	32	Earthquake at primary Facility	NA	Structural	PP / PV	Substation fire, Flood (if a dam or dike is damaged)
Theft of energy between components	31	Incorrect privilege settings	NA	Emerging	CP, MG	-
Substation fire	33	Electrical component failure	NA	Structural	CAT	-
Flood	34	Grid component failure	NA	Structural	CA / CAT / SCADA / EC /DC/ MG	-

Next, we adopt several assumptions about the political and geographical localization of the city. Their level of detail suits the need to consider a high level likelihood estimation of the occurrence of the disaster events. These assumptions include:

- The city has an important strategic relevance and is consequently *exposed to terrorism*;
- Due to the terrorism risk, the permissions and the policies for the utilization of resources are strict with the aim to mitigate possible malicious actions;
- The city is NOT in a seismic zone.

Finally, we can consider jointly the grid configurations, disaster events, and assumptions on the grid context. Table 1 in the Appendix B provides likelihoods of disaster scenarios related to disaster events 1 – 6 together with short disaster descriptions. The provided descriptions indicate that grid components and topology are linked to specifics of scenario events.



To illustrate a way how grid specifics can be cross-related to characteristics of a disaster event, the next section illustrates how a specific event (flood) can be considered in more detail. This example complements the earlier analysis on adversarial threats with a case of a non-adversarial threat to a city.

10.2 AN ILLUSTRATIVE APPROACH TO CONSIDER FLOOD DISASTER SCENARIOS

This section suggests how likelihood of natural disaster events and consequent disaster scenarios can be considered. Taking a flood event as a representation of the natural disaster events class, we first illustrate how assumptions about the city under consideration are related to the likelihood of disaster events. The considerations are aligned with the actions described in four-step list earlier. In particular, this document concentrates on (1) a flood likelihood of floods and (2) how a disaster scenario unravel

Noticeably, this approach does not strive to provide either a comprehensive analysis or outline a sophisticated methodology for assessing flood likelihoods. The interested reader may consult one of many research papers on flood events that constitute a comprehensive field populated by more specialized research projects. For instance, input from the FLOODsite project is relevant for conducting an elaborated flood risk assessment. FLOODsite was a large scale Integrated Project in the Global Change and Ecosystems priority of the Sixth Framework Programme of the European Commission. The project ran from 2004 to 2009 and included 37 of Europe's leading institutes and universities. A number of publications that describe multiple diverse methodologies are available for download at <http://www.floodsite.net/default.htm>.

This section illustrates interrelations between natural disaster and possible scenarios as follows:

- We concentrate on flood height as an essential flood-specific parameter. This emphasis is adopted based on our analysis of a sophisticated flood modelling methodology Hazus (<https://www.fema.gov/hazus>). This state of the art GIS-based solution to model natural hazards was recently developed by the US Federal Emergency Management Agency (FEMA). By considering flood height as a Hazus specified flood property, we are ensured that (1) the chosen parameter is particularly relevant for the flood event and (2) it remains possible to couple the outlined method with the Hazus methodology and simulation capabilities of its implementations. We are aware of other parameters which play a role in flood damage (e.g. flood speed), but we concentrate on flood height as it is widely acknowledged to be the key parameter;
- We map grid components to flood height to assess them. We specifically look at parameters of substations (height of equipment), and of communication lines (height is differentiated into under- and above-ground categories). Specific disasters scenarios can be constructed from anticipating which components can fail in upholding their functionality during flood events.

The way to anticipate outage scenarios is significantly different from being merely a formalization of the Hazus methodology. First, Hazus does not concentrate on assessing the availability of electricity supply during natural disasters based on grid components. We used the Hazus flood characteristics as a first step to concentrate on relevant factors that should be accounted for in assessing flood hazards. Second, we target a specific topic — how to anticipate disruptions in electricity supply in a city as an



object of analysis. Finally, instead of considering costs of grid components as a loss function, we concentrate on the function of electricity delivery that the assets provide to the city. Concentrating on this function, or in other words on specific asset value, for such an assessment was suggested earlier in flood-related research. In particular, FLOODsite pointed out that to account for indirect effects of flooding on electricity systems it is “not ... the asset at risk that is important here but the value of that asset to maintaining the system provided by the infrastructure” [56]. This highlights that ultimately, it is not the risk what matters but its translation into impact.

The rest of this section is organized as follows; the next subsection highlights how the likelihood of flood events can be described in relation to their scale; following that the document then describes how Hazus as a state of the art solution accounts for flood properties of buildings that represent city components; and finally, grid components are mapped to flood height together with the description of how underground and overhead electricity lines could function during floods.

10.2.1 Likelihood of Flood Events

According to Planning and Flood Risk Policy Statements prepared by the UK Department of the Environment [57], the likelihood of a flood typically indicates possible frequency of return. For instance, a flood event may be expected to happen only once in 100 years. It can be described as having a 1% probability of being equaled or exceeded in any one year. A 1 in 200 year event may therefore be expressed as having a 0.5% probability of being equaled or exceeded in any one year. While the number indicates possible return period, it concentrates on the scale and not on the time period. In other words, a ‘one in one hundred years flood’ can happen in two consecutive years.

A scale of flood events can help to describe flood-prone areas. For instance, this scale can be similar to the one adopted by Environment Agency in the UK (<http://maps.environment-agency.gov.uk/>). For a UK map provided by this agency, three Flood Zone definitions are employed that were set out in the National Planning Policy Guidance:

- Flood Zone 1 — land assessed as having a less than 1 in 1,000 annual probability of river or sea flooding (<0.1%);
- Flood Zone 2 — land assessed as having between a 1 in 100 and 1 in 1,000 annual probability of river flooding (1% – 0.1%), or between a 1 in 200 and 1 in 1,000 annual probability of sea flooding (0.5% – 0.1%) in any year;
- Flood Zone 3 — land assessed as having a 1 in 100 or greater annual probability of river flooding (>1%), or a 1 in 200 or greater annual probability of flooding from the sea (>0.5%) in any year.

It can be also helpful to link flood probabilities to a qualitative flood scale. An example of explicitly linking the flood likelihood to the qualitative scale can be seen, for instance, in how Moreton Bay region council refers to likelihood of flood events [58]. This council, located at the eastern coast of Australia, specifies that “The terms ‘high’, ‘medium’ and ‘low’ likelihood are intended to give an appreciation of the relative size and likelihood, over a long period of time”. In their three-step scale, high likelihood refer to 5% of annual chance of a flood, which corresponds to a ‘Small’ flood. ‘Medium’ likelihood describes 1% Annual chance of a ‘Large’ flood. A ‘Very large’ flood is an unlikely event — it is specified as 0.1% annual chance and ‘Low’ likelihood.



This document adopts a five-step likelihood classification similar to the Moreton Bay classification. The annual flood chances are differentiated into five values: in addition to ‘high’, ‘medium’, and ‘low’ likelihood of the range we also include ‘very low’ and ‘very high’ likelihood to comply with the five-step scale described earlier. It should be noted that in our classification we do not differentiate between specifics of floods (e.g. we do not specifically account for river or sea floods; neither for their cause, such as rainstorm, ice-jam, or snowmelt floods). Also, we do not argue in favor of a specific scale, but rather illustrate the differentiation of different flood likelihoods. In addition, we are aware of the importance of the flood duration as a function of asset damage (see for instance [59]), but this aspect is left for future considerations.

The scale of the likelihood can be derived from experience of floods at a specific area or based on simulation models. For the first case, multiple sources of information can assist in determining flood likelihoods. FEMA (Federal Emergency Management Agency) highlights several such sources of information for determining flood risks [60], relevant to consider likelihood:

- Site-specific data such as stream gaging records;
- Rainfall records;
- Historic information, e.g. flood marks on buildings and other structures, areas flooded;
- Newspaper accounts, diaries;
- Marking of flood levels after an event;
- Botanical evidence such as scars on trees;
- Physical and geomorphic techniques, e.g., look at water transported debris along walls of canyons;
- Regional information, i.e., look at flood occurrences along similar streams in the area.

Recently, several sophisticated methodologies were developed that consider flood events (and their likelihoods) in great detail. These methodologies allow for flood simulation with respect to the abundant amount of geo-information available for cities.

The next subsection briefly outlines Hazus (<https://www.fema.gov/hazus/>) as a state of the art methodology to simulate flood events. Based on the Hazus specifications, we concentrate on flood height as a flood parameter that can lead to city-scale blackouts.

10.2.2 Flood Height

To meaningfully relate grid properties to disaster events it is necessary to identify properties of the event that can impact the grid. This subsection illustrates how the Hazus methodology — a state of the art approach to consider impacts of natural hazards — approach flood modeling. It is indicated that flood height is one of the most important characteristics for this task.

10.2.2.1 Introduction to the Hazus Methodology

Hazus is developed and freely distributed by the Federal Emergency Management Agency (FEMA) as a solution to model natural hazards. The most recent version of this geographic information system (GIS) — The Hazus®-MH (Multi-hazard) — accounts for four types of hazards: flooding, hurricanes,

coastal surge, and earthquakes. Hazus is freely available by itself, but requires users to have ArcGIS software due to its heavy reliance on GIS component. The GIS aspect stays in the center of the system and assists the software user in providing input and better understanding the output of the methodology application.

As a first step, Hazus models the exposure for a selected area to calculate risks. After modelling the exposure, Hazus-MH characterizes the level or intensity of the hazard, and calculates the potential losses based on the characteristics of the area and the hazard. For this, it builds on geo-referencing of all building mapped by values of latitude and longitude. Among the mentioned four hazard types, in this document we concentrate on how Hazus accounts for flood events.

Hazus accounts that Flood hazard and Inventory of all buildings provide input for all future calculations. Figure 20 shows that these interrelations build on Inventory (buildings, infrastructure, population, and agriculture information) and Flood hazard (such as depth and velocity) parameters.

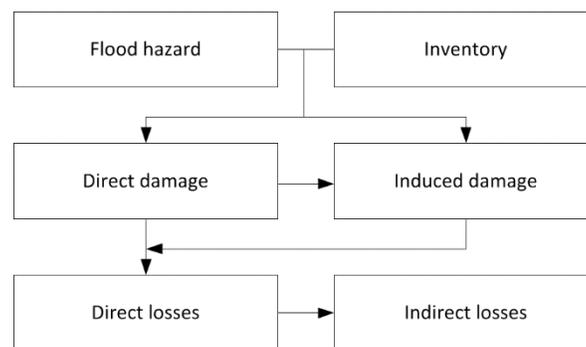


Figure 20. Exemplary structure of a Hazus report on flood events

While Inventory appears to be a rather broad category that contributes to every calculation step, Hazus details what particular elements constitute infrastructures. Essential facilities and general stock buildings are separated. General buildings stock provides input for considerations that account for debris, shelters, and direct economic impact. The latter is used to account for indirect economic losses. Lifeline systems are subdividing into transportation and utilities. Figure 21 shows the relations between these components. A detailed description of the methodology can be found in the Natural Hazards journal [61], [62]. Also, a step-by-step manual on flood modelling named “Multi-hazard Loss Estimation Methodology Flood Model Hazus® -MH User Manual” is available at the FEMA website [63].

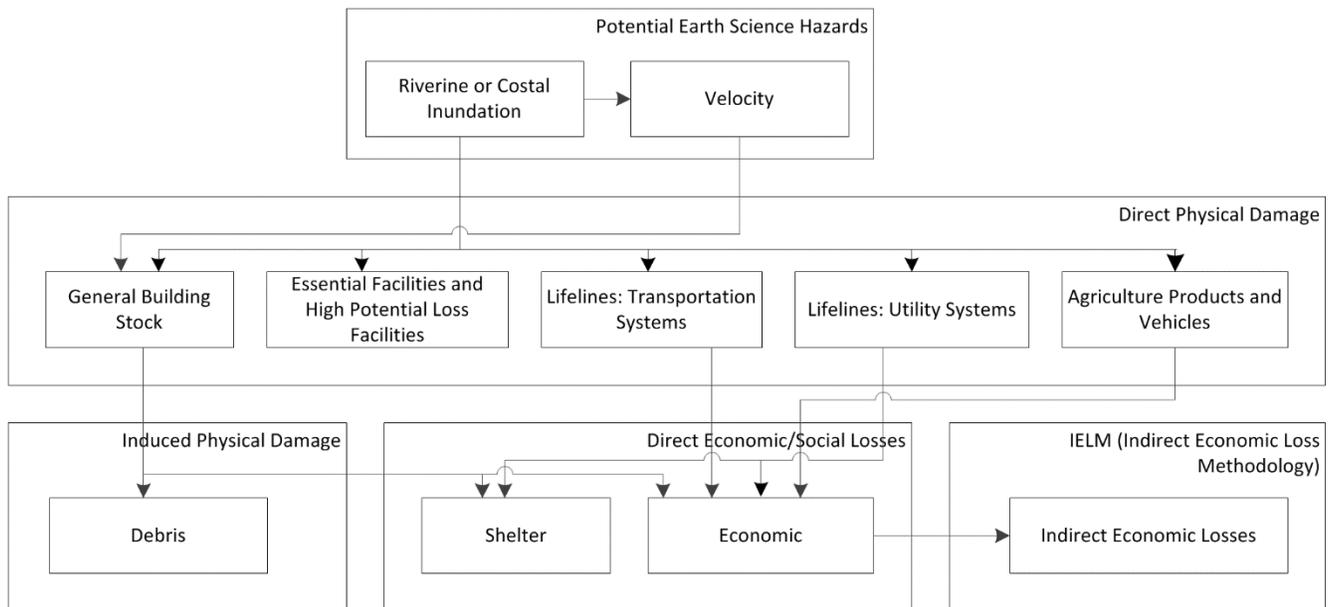


Figure 21. Hazus Flood model schematics

In short, Hazus provides an elaborated way to account for losses during flood events. However, the methodology is less concerned with the function of providing electricity to a city that experiences a flood event. At the same time, flood-relevant parameters encoded into the Hazus database can be linked to properties of the grid to account for this function. The Hazus flood-relevant parameters are outlined next.

10.2.2.2 Hazus Approach to Describe Flood-specific Characteristics of Essential Facilities and Systems

As Hazus tackles the complex task of flood disaster in a methodologically rigorous manner, the structure of the Hazus database provides a well-justified categorization of flood-related building characteristics. To highlight important flood-related characteristics, this subsection provides an overview of how Hazus considers essential facilities and systems. The structure of the Hazus database outlined in the Hazus-MH Data Dictionary [64] informs this task.

Hazus specifies a set of additional parameters to illuminate how essential facilities, transportation systems, and lifeline utility systems should be considered with respect to flood events. These parameters describe facilities by themselves. For instance, the Care Facilities Feature Class *hzCareFlty* (F.5.3.1) describes care facilities in general, while additional flood-specific characteristics are provided in the Flood Specific Care Facilities Table *flCareFlty* (the “*fl*” prefix points out that the table is relevant for flood events). A list of tables that extends descriptions of different facilities with flood-related characteristics is as follows:

From F.5 ESSENTIAL FACILITIES: EF.MDB:

- F.5.3.3 Flood Specific Care Facilities Table: *flCareFlty*;
- F.5.3.6 Flood Specific Emergency Center Facilities Table: *flEmergencyCtr*;
- F.5.3.9 Flood Specific Fire Station Facilities Table: *flFireStation*;



- F.5.3.12 Flood Specific Police Station Facilities Table: *flPoliceStation*;
- F.5.3.15 Flood Specific Schools Facilities Table: *flSchool*.

From F.6 TRANSPORTATION SYSTEMS:

- F.6.3.9 Flood Specific Highway Bridge Table: *flHighwayBridge*;
- F.6.3.16 Flood Specific Light Rail Bridge Table: *flLightRailBridge*;
- F.6.3.29 Flood Specific Railway Bridge Table: *flRailwayBridge*.

From F.7 LIFELINE UTILITY SYSTEMS: UTIL.MDB:

- F.7.3.5 Flood Specific Electric Power Facilities Table: *flElectricPowerFlty*;
- F.7.3.8 Flood Specific Natural Gas Facilities Table: *flNaturalGasFlty*;
- F.7.3.11 Flood Specific Natural Gas Pipeline Table: *flNaturalGasPl*;
- F.7.3.14 Flood Specific Oil Facilities Table: *flOilFlty*;
- F.7.3.17 Flood Specific Oil Pipeline Table: *flOilPl*;
- F.7.3.20 Flood Specific Potable Water Facilities Table: *flPotableWaterFlty*;
- F.7.3.23 Flood Specific Potable Water Pipeline Table: *flPotableWaterPl*;
- F.7.3.27 Flood Specific Waste Water Facilities Table: *flWasteWaterFlty*;
- F.7.3.30 Flood Specific Waste Water Pipeline Table: *flWasteWaterPl*.

We consider two tables — *flElectricPowerFlty* and *flCareFlty* — as particularly relevant for this document. These tables specify what properties of Electric facilities (as a component of a grid infrastructure) and Care facility (as an example of a potential critical client) are relevant to floods.

10.2.2.3 Flood Height as a Characteristic of Electricity Production and Consumption Facilities

For the case of electric facilities, the Hazus class *hzElectricPowerFlty* (see the class description in Appendix B.2) is extended with table *flElectricPowerFlty* (Table 25). This table provides Flood Model specific information of electric power facilities. It characterizes Flood Specific Electric Power Facilities and belongs to the UTIL.mdb — database that describes lifeline utility systems.

Table 25. Elements of table flElectricPowerFlty [64, pp. F-203]

Name	Description
ElectricPowerFltyId	Unique identifier for each record. It relates this flElectricPowerFlty feature class with the associated hzElectricPowerFlty in a one-to-one relationship. The standard format adopted by Hazus is SSxxxxxx, where SS is the state name abbreviation (upper case) and xxxxxx is a sequential number from 000001 to 999999.
UtilIndicator	Utility Indicator. This field is not used in the current version (MR3) of Hazus.
FoundationType	Foundation type (e.g., slab, pile)
EquipmentHt	Average height of electrical equipment (measured in feet from the floor)
FloodProtection	Flood return period (in years) for which the structure is protected
UtilDamageFnId	Originally intended to allow users to define facility specific damage curves. Utility damage functions are not used in version MR3 of Hazus.



While all these elements describe flood-related building characteristics, we are particularly interested in *FloodProtection* and *EquipmentHt* fields to link electric facilities with flood likelihoods and possible future scenarios. These fields describe how an electric facility can withstand a flood of a particular height.

The *Floodprotection* field provides a link between likelihood of flood events and specifics of a particular structure. Similarly to the above mentioned approach of associating likelihoods with event sizes, it can be described on a scale from ‘very low’ to ‘very high’. In this way, it can relate a flood’s likelihood with the facility’s ability to withstand it, in a qualitative manner. Within this document we assume that if the *Floodprotection* value of a specific facility is lower than the characteristics of specific flood, the facility will be destroyed and therefore equipment located within it will cease to function as a part of electric grid.

EquipmentHt highlights the role of positioning the equipment with respect to the flood height. Clearly, as *EquipmentHt* describes the height from the floor, additionally the height of the floor itself should be added to relate the equipment height with the flood height. Hazus Flood Model Mapping Scheme (F.12.1.2) amplifies it as follows: “First floor elevation (as determined from foundation type) is another key parameter for the estimation of flood damage. Information on foundation types for the general building stock is provided by a foundation mapping scheme consisting of a set of tables that depicts how foundation type and first floor elevations are distributed by specific occupancy.” The same logic, but in a different format, applies when Hazus accounts for the height parameters applied to Care facilities. Their first floor heights are described by a specific field (*FirstFloorHt*) and no height of electric equipment is mentioned (as can be seen from the structure of flood-related table for Care facilities included as Appendix B.3). This shift of accents in describing assets can be explained that the Hazus methodology particularly concentrates on high value assets, such as energy transformers at substations, but is less concerned with electricity communication facilities at final customers, such as hospitals.

The next sections concentrate on how flood heights can be related to specific grid components.

10.2.3 Relating water heights to grid components

Adopting a network paradigm (nodes connected with edges) can help in anticipating how a disaster event grid can cripple the grid function to provide electricity to critical customers. As mentioned, IRENE deliverable “D2.1 Threats identification and ranking” groups components of future smart grids into four categories (Table 6):

1. Energy Provider (EP): Buildings that provide energy for the grid (PP — Power Plant, PVG — Photo Voltaic Energy Generator, WF — Wind Farm);
2. Connection (CON): Elements that are in charge to carry energy, data or both from a set of components to another;
3. Building (BLD) as electricity consumers;
4. Data Center (DAC): Components that are able to process data, such as SCADA.



In this list, groups 1, 3, and 4 represent network nodes and connections (group 2) are edges between them. This document adds further details into this categorization to highlight that future grids will have more renewable generation capabilities. Therefore, we additionally differentiate energy providers into two types:

- 1a. Bulk generation;
- 1b. Distributed generation (local energy providers).

Each of the four component groups can be related to flood parameters. Specifically, functionality of grid components from category 1 (energy providers) and 3 (buildings) can be seen as buildings that possess the *FloodProtection* characteristic, where equipment height is a less relevant factor. However, because Hazus does not concentrate on the utility of providing electricity to customers from the network perspective, the relation of categories 2 (connections) and 4 (data centers such as SCADA) needs additional elaboration. This is described further below.

10.2.4 Differentiating communication lines as overhead or underground cables

A grid is unable to maintain the function of providing electricity to customers if communication lines are not functioning. This subsection illustrates how communication lines can be accounted for with respect to flood heights.

In our view, assigning a height value to each communication line wouldn't be practical for the case of a city-level analysis. Therefore, this document describes such lines as characterized by their location with respect to a ground level. As such, communication lines can be constructed using either overhead or underground cables.

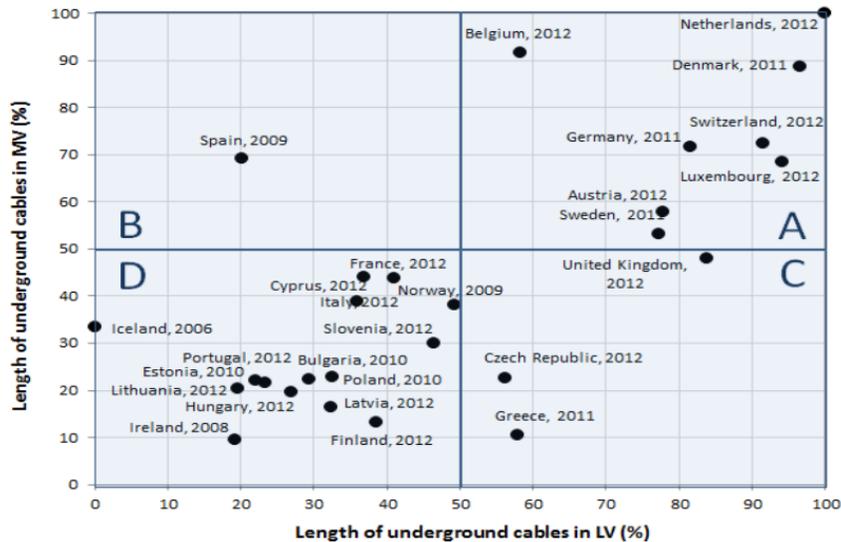


Figure 22. Clustering European countries according to technical characteristics of the network [65]

The degree to which Low voltage and Medium voltage employ underground cables varies significantly across European countries (Figure 22). For instance, Iceland operates exclusively overhead Low



Voltage lines (according to data from 2006), but such lines are completely absent in The Netherlands. Meanwhile, only about 10% of Medium Voltage cables were underground in Ireland and Finland in 2008 and 2012 correspondingly, compared to 100% in The Netherlands. In general, a mixed nature of a country-wide network (that combines above and underground lines) can be observed.

The choice of implementing electric grids using different types of cables is influenced by a number of factors. It is clear that underground lines have several advantages in addition to aesthetic considerations. Additionally, they are less vulnerable to wind and ice, as well as can be more practical to use in some areas such as in the city centers. Finally, such lines can provide increased public and personnel safety. The overall amount of outages due to underground lines is lower compared to those of overhead connections. This aspect was analyzed in the report on US outages in the period 2004 – 2011 [66]. By using several commonly used indexes (CAIDI — Customer Average Interruption Duration Index, SAIDI — System Average Interruption Duration Index, and SAIFI — System Average Interruption Frequency Index), the report demonstrated that the underground electrical system contributes a smaller percentage to the overall outage numbers experienced by customers.

At the same time, underground cabling can be costly [66]. For instance, the cost for constructing a one mile of new underground urban distribution line can be in range of 1,141,300 USD to 4,500,000 USD, while the cost of constructing an overhead line is 5 – 10 times less: from 126,900 to 1,000,000 USD. Similar financial differences in installing underground and overhead lines was also cited in other studies, e.g. [67]. Furthermore, after the installation, additional future expenses might be required to upgrade underground communications.

In addition to higher costs, underground lines come with several shortcomings that can hamper their wide adoption. These shortcomings include:

- Repairing such lines is more difficult and may take longer compared to overhead communications. For example, it can take from 8 – 48 hours or longer to find faults and repair them [67];
- Failure rates can increase at the end of their lifetime, as over time underground lines become more prone to failures;
- Storm-related flooding, particularly salt-water flooding, can cause and prolong outages in underground systems, thus shortening their life and increasing the maintenance demand. For instance, Tropical Storm Allison in 2001 and Hurricane Sandy demonstrated that underground electric facilities are very vulnerable to flooding and water damage, however undergrounding reduces the risk of grid failure due to wind damage [66]. Therefore, in the case of wind-related flooding, the picture is rather mixed.

The latter shortcoming should be considered in more detail in the light of this report. Underground connections can both fail themselves and contribute to the cascading failure of overhead lines coupled to them. For example, after Hurricane Wilma struck South Florida in 2004, the media reported that 97 or 98 percent of Florida Power & Light customers in Broward County lost power, even though 54 percent of them were served by underground lines [68]. Therefore, it is relevant to account for the



interdependency between different types of lines in the flood-related grid analysis, as overhead customers supplied by electricity from underground cables can also experience blackouts.

Underground communications are more prone to fail during flood events. Such failures can lead to blackouts for overhead consumers if their electricity delivery relies on underground connections. This document takes these two factors, i.e. failure of underground communications during flood events and their contribution to failure of overhead lines. These factors are relevant for modelling failures of edges of the electricity networks during flood events. The next section describes how electricity network node failures can be approached.

Connection Adapters and SCADA

Cables link network nodes, such as connection adapters and control centers. Given the cyber-physical nature of grid nodes, control centers should stay functional to continue delivering electricity to critical customers. Thus, their ability to function during floods should be considered.

To maintain N-1 requirement (when the grid remains operational after a single failure), several power sources should be accessible to essential nodes. For instance, SCADA center might require electricity supply to island a grid segment in case of large-scale blackouts. For this purpose, the center might be connected to batteries or diesel generators to ensure its independence from an energy supplied from comparatively less reliable renewables. The failure to provide such energy will limit islanding capabilities, as it occurred after the Tohoku Earthquake in Japan when the Sendai microgrid failed to start gas engines because the control system batteries were totally discharged [69]. Additionally, emergency supply may be required to start generating additional energy within an island. Some nodes can generate energy by themselves if they belong to group of components 1b (Distributed generation by local energy providers).

Therefore, the availability of *emergency electricity supply* (if needed) is another characteristic to consider for some components, such as Connection Adapters.

An approach to account for failed grid network components as contributors to outage scenarios

As outlined, the function of continuous supply of electricity to city-based customers during flood events depends on adequate performance of grid nodes and communication lines. While the functionality of lines is linked to flood events directly, the functionality of nodes depends whether the building that host them should withstand floods.

A building can host more than one node, for instance SCADA, Connector, and distributed generation nodes. If a building is destroyed during a flood, the hosted nodes will become dysfunctional. By following this structure, the *FloodProtection* parameter can be applied to a building, while the *EquipmentHt* parameter is to be related to individual grid components. Thus, to account for specifics of nodes we differentiate between properties of buildings and heights of electric equipment in them. Water velocity during flood events is somewhat encoded into the *FloodProtection* property as it if a building will withstand a flood event of a specific likelihood. Nodes located outdoors are subject to considering their *EquipmentHt*.

Figure 23 relates the described flood-relevant characteristics to a topology of an urban grid. In this document we consider that the *EquipmentHt* property of equipment should be considered if (1) it is located in a building that can withstand a flood of a specific likelihood or (2) the equipment is located outdoor. Figure 24 proposes an algorithm to identify what nodes and edges of the network will continue to function during a flood event with a specific likelihood and height.

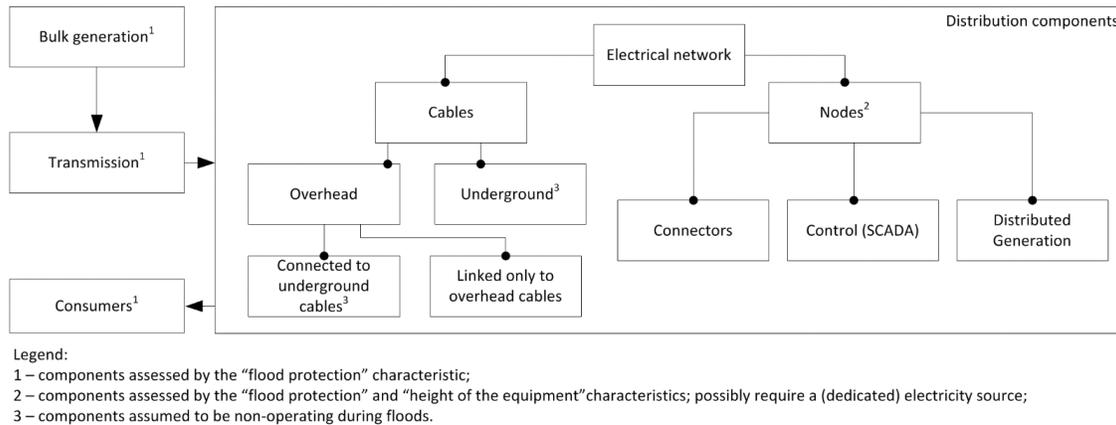


Figure 23. Grid components wrt to ‘flood protection’ and ‘height of the equipment’

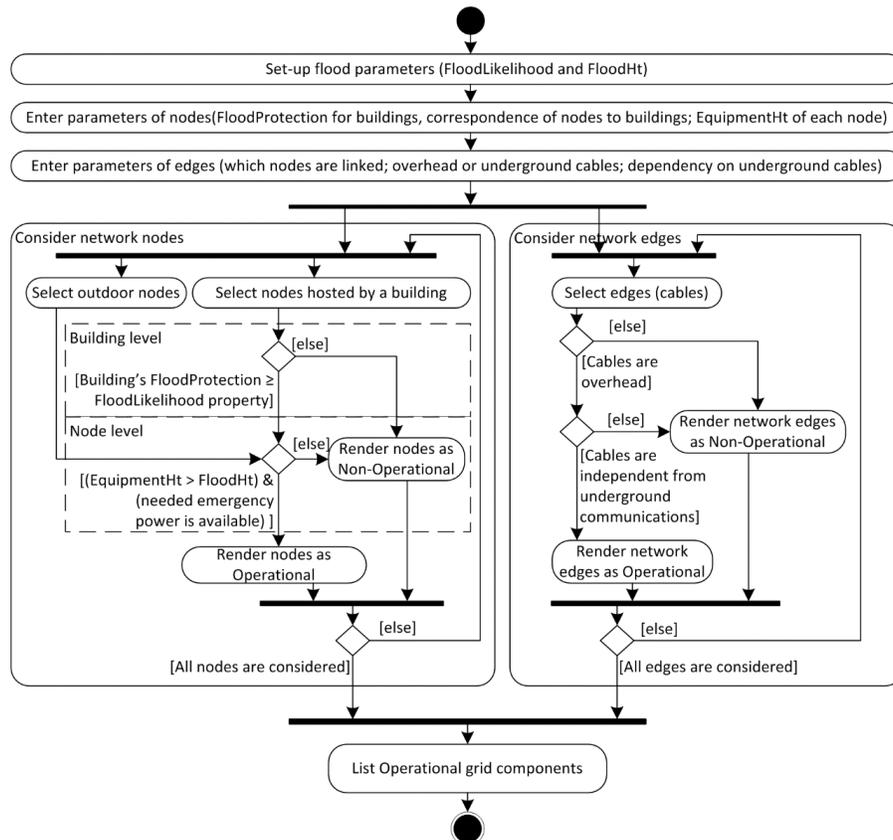


Figure 24. Activity diagram to identify components of city electricity network that stay operational during a flood



The outlined refined structure of groups of grid components and the way to apply flood parameters to these groups aim to assist in considering flood-caused blackouts. Using the approach a user can identify what grid components can fail during flood events of particular likelihood and height. By knowing which customers are not supplied with electricity, the impact to the city can be calculated. To this extend, the approach outlined provides input for flood impact assessment to critical urban infrastructures.

The next section illustrates how this approach can be applied to a city, which is located in an area with specific flood risk and that possesses a network with both overhead and underground cables.

10.2.5 Illustrative case

This subsection describes how a city component can be related to the approach described above.

According to the guidelines to account for disaster events, in the first step we need to concentrate on a particular urban grid. For this task we take a grid fragment of the grid located in named Naperville (Illinois, US), because sufficient information about it is publicly available. This distribution network fragment can be freely downloaded and visualized in ArcGIS software. The network provides sufficient illustrative power, as it utilized both overhead and underground cables. Next, we parallelize possible future states of the network with the IRENE example on grid evolution. This is adequate, as with the city that experienced rapid growth over the last few decades and was recently named ‘the wealthiest city in the Midwest. It is likely that continuously increasing population of the city and the possibility of future investments into the city’s infrastructures, that smart grid components will be adopted at an increased rate.

Within the second step, we limit our consideration to a flood disaster event, which is not linked to other disaster events, such as earthquake or tornado.

Next, we look at the likelihood of flood events and other assumptions (3rd step of the guidelines) and consider the propagation of the disaster event (4th step) as follows.

Assumptions on the grid and its context

Assumptions on the grid and likelihood of events can be derived from properties of the area where the grid is located. As Naperville is located at the elevation of 214 m, flood events are not common. A major flood event caused by the Aurora flood in 1996 [70]. At the streamflow-gaging station D48 located at Spring Brook at 87th Street near Naperville, the gage height on 18 July 96 was 10.77 ft (3.28 m). This height corresponds to the recurrence interval of >25 years [71].

Concerning other natural disaster events, Naperville is located in a relatively low risk hurricane zone. Six hurricanes have been recorded there since 1930. The largest hurricane (unnamed) took place in 1949 and the most recent hurricane (i.e. Gustav) was in 2008 [72]. The city area is also less prone to earthquakes due to its location in a non-seismic active area.

Based on the data, we assume that the area exhibits ‘very low’ exposures of the vulnerability to earthquakes, while having a ‘low’ rate for tornados and flood events. Therefore, we can classify the

likelihood of flood events as low. For the need of more detailed analysis, this assumption can be further refined based on available statistics and predictive analysis of natural disaster events.

Illustrating possible outage scenarios

A simplified view of a Naperville city grid can be applied to the provided activity diagram to identify how a flood disaster event can impact different grid consumers. This example is for illustration purposes only. A more sophisticated analysis can be conducted by building a comprehensive database of city- and district-level assets using, for instance, Hazus database. Statistical and contingency analysis can further enhance the analysis.

A fragment of Naperville's distribution grid is illustrated in Figure 25. The figure demonstrates a subset of relevant grid components from the 'ElectricDataReviewer' sample available for visualization in ArcGIS. Bold lines in the figure illustrate primary conductors.

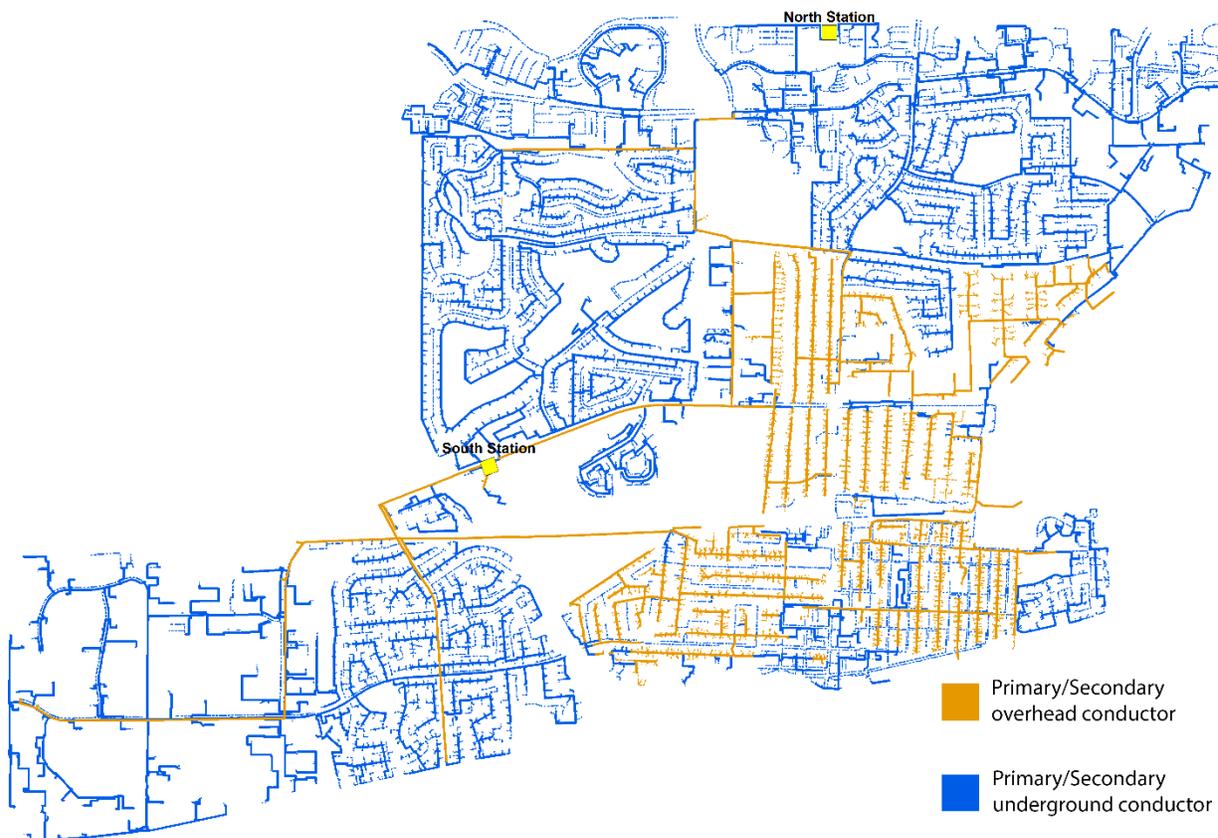


Figure 25. A fragment of the Naperville's electricity grid

The network shows that the two stations (North and South) are connected either an overhead or an underground network. The networks possess some specific advantages as outlined above. Advantages of overhead conductors (e.g. the ability to sustain a flood event) can only be obtained if the stations themselves are capable of effectively distributing the available electricity to clients. These stations host



grid nodes that might provide capabilities to re-adjust the distribution to balance the demand and available power supply (in case the grid provides no electricity due to a blackout).

As can be derived from the approach suggested above, the grid configuration should be considered in connection to several criteria to be fulfilled to ensure continuing electricity supply during floods. These criteria include:

- Power lines above the ground stay functional to supply customers;
- Buildings that host electrical equipment are sufficiently flood-protected and equipment is located at heights above the water level;
- Additional power sources for electricity supply are available;
- Control centers are functional and have emergency power supply.

By relating grid properties to these criteria, disaster scenario can be developed and projected to the IRENE grid evolution steps. The Initial grid scenario (*Case 1*) can be linked with the existing Naperville grid structure as follows. Overhead and underground cable clusters are connected to South and North Stations accordingly. These stations have the CAT (Connection Adapter with energy Transformer) functionality. The differentiation between power supply, communication lines, and substations can result in the following scenario for a flood characterized with a ‘Low’ likelihood:

- With only one power supply available, the South or North station will cease to function if *FloodProtection* property of their buildings can withstand the flood strength encoded within the ‘Low’ likelihood of the event. In this case, the outage of the lines connected to them is imminent. At the same time, even if a substation withstands the flood, the equipment can fail if it is not located at a sufficient height. In other words, if the water level rises above the height of the electrical equipment (*EquipmentHt*), the station will be non-operational;
- Because of the significant percent of underground lines, flood can cause city blackouts. It is more likely that (at least some) customers connected to overhead conductors will continue receiving electricity, contrary to the customers linked to underground conductors (i.e. provided that substations operate). Because the North Station is connected exclusively to the underground network, underground consumers will be out of service, while electricity can still be supplied through the South Station. Noticeably, either all or none of the clients of the South Station will receive electricity. While groups of houses have only electrical connections (EC), they still lack Micro Grid Connection (MG). Therefore, they cannot be dynamically de-attached from the grid to update a microgrid perimeter.

Altogether, due to the absence of emergency capacity, even if a single element of the grid is affected by flood, the supply of electrical energy is in danger. This analysis can be summarized as disaster with low likelihood as shown in Table 26.



Table 26. An exemplary disaster scenario for a simple grid in case a flood event

Scenario	Scenario description	Disaster description
	<p>1. Initial Scenario 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 lack of a controller.</p>	<p>Only one power supply is available. If a flood event impacts the PP (Power Plant), electric lines, or the connection adapter, outage is imminent.</p>

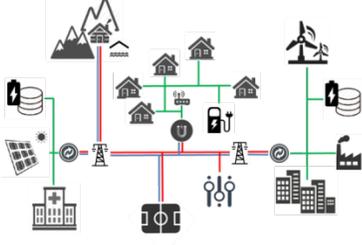
Similar analysis for *Grid evolution step 10* (Improving decarbonisation) provides a different output. In this case, a separate SCADA controller and a public charging station are located between two microgrids. Several electricity providers are distributed around the network. Large consumers (a hospital and a factory) are connected to the network.

If needed, the network can be compartmentalized into distinct parts. This process is controlled by the SCADA controller that provides the communication with the substations to monitor and control the grid. The switch to the islanding mode is performed by Connection Adapters (CA). In case of a flood event, power supply, communication lines, and substations can be affected as follows:

- For stations (LRC, CAT, and CA) the electrical equipment height and flood protection should be considered as mentioned above. At the same time, the SCADA controller implemented in the grid should be accounted for. If the controller is not adequately protected from the flood, then its ability to employ DSM for the residential area will be hampered. With SCADA dependent on reliable electric power, emergency power supply should also be included in the system. If these requirements are fulfilled, two microgrids built around the hospital and the factory will enable continuous electricity supply to these clients even if a flood damages large parts of the grid;
- Lines: Similarly to the above described outage scenario, we assume that underground lines will be employed as within the city network. The clients supplied by underground communications can experience a blackout. However, if future grid communications account for sufficient replication and redundancy in connections using overhead lines, a specific communication patten can help to avoid outages to specific clients.

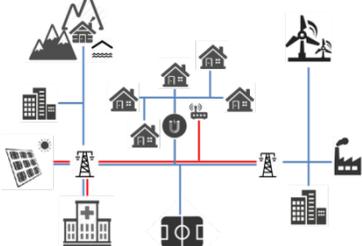
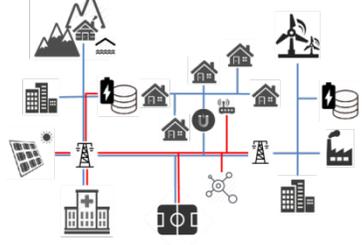
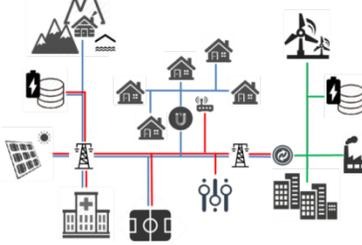
These aspects can be summarized as a low-likelihood scenario outlined in Table 27.

Table 27. An exemplary disaster scenario in case the grid is highly developed

Scenario	Scenario description	Disaster description
	<p>10. Improving decarbonisation Decarbonisation improved with encouragement to adopt EVs. A public charging point is inserted in the citizen's area.</p>	<p>Two microgrids built around the hospital and the factory can guarantee that the energy will be supplied to these clients even if a flood damages large parts of the grid. In this way, the outage impact on the city will not include elements directly related to the hospital and the factory.</p>

The grid will experience disasters differently at other steps of this evolution. The flood disaster scenarios for those evolution steps can be as described in Table 28.

Table 28. Disaster scenarios for other grid evolution steps

Scenario	Disaster description
	<p>4. Adding key buildings Because the grid has no islanding capabilities, floods can bring down the whole system. However, if only one of the available energy sources is out of order and the connections are operational, the grid can balance between the (reduced) energy supply and demands. Still, as renewable generation provides fluctuating energy supply, reaching the balance can be problematic. The absence of a data centre (BDC) can also worsen the situation.</p>
	<p>5. Inserting Storages Data and electricity storage, supported by BDC, can assist in balancing the supply and demand, if some power supplies are unavailable. Still, the centralized nature of control coupled with the lack of flexibility in grid connections render the task of ensuring continuous electricity delivery to critical clients problematic.</p>
	<p>8. Insertion of SCADA System This step is a significant improvement compared with the previous grid evolution steps. The ability of SCADA to compartmentalize the grid ensures that the factory could receive energy from the grid even if several power sources are not available. However, as the hospital is connected directly to a city grid, the control center needs to carefully balance its demand with (possible) fragmented power supply.</p>



It should be noted that these outage descriptions will not necessarily correspond to real events. With another set of assumptions, the outcome of the analysis will differ. For instance, if a grid is either located in an area prone to flood or has sophisticated capabilities to counter propagation of negative effects, the result of such analysis will differ. Additional elaboration steps might be needed to improve the suggested approach. Besides, while this document intends to provide a structured way to account for flood-caused outages based on flood characteristics, multiple improvements to it are yet possible. As an example, the assumed interrelations between flood characteristics and grid components can be further elaborated and even adjusted.

At the same time, despite the shortcomings of this document, we consider that constructing scenarios using approaches such as the one described in this section, can help better understand the needs of future smart grids. It can provide valuable input for design of future city-level solutions. Future networks enhanced with sophisticated microgrid capabilities will probably have possibilities to rearrange the grid network to localize flood impact. For this, specific improvements and clustering of functionalities of the described components can be considered. For instance, the functionality of Connection Adapter (CA) can be further enhanced with SCADA control capabilities. This can assist in ensuring that the dependency of CA from SCADA is not an obstruction in mitigating outages from disaster events. A future smart substation might need to have all these functionalities at a single place (sufficiently protected from flood events) to effectively and efficiently island a grid segment, as well as balance demand and supply within it.

11 SOCIETAL IMPACTS

With the topic of threat analysis and identifying disaster scenarios it is possible to identify grid components that will experience blackouts. This section continues the topic of blackouts by illustrating what problems essential city nodes can face as they experience blackout and how they can be related to blackout costs. Before that, we outline how what are critical infrastructures and how interrelations between them can change during prolonged outages.

11.1 CRITICAL INFRASTRUCTURES TO ANALYZE SOCIETAL IMPACT

Urban societies rely heavily on the proper functioning of critical infrastructures (CIs). These infrastructures are vital for economy, governance, and daily life. The importance of a single CI cannot be underestimated as all CIs are heavily interconnected.

The European Council Directive 2008/114/EC [73] acknowledges the significance of critical infrastructures and defines them as an asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact. The directive asks member states to identify their CIs. However, it does not give a concrete list of infrastructures to be considered.

A list of different CIs can be found in The European Commission's "Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection" [74]. The main aim of the proposal was to define a common procedure for the identification CI in the member states and to foster equal standards of CI protection in the European Union. The list of CIs below provides a comprehensive overview of CI without being complete.

Table 29. Indicative list of critical infrastructure sectors

Sector	Product or service
Energy	Oil and gas production, refining, treatment and storage, including pipelines Electricity generation Transmission of electricity, gas and oil Distribution of electricity, gas and oil
Information, Communication Technologies, ICT	Information system and network protection Instrumentation automation and control systems (SCADA etc.) Internet Provision of fixed telecommunications Provision of mobile telecommunications Radio communication and navigation Satellite communication Broadcasting

Water	Provision of drinking water Control of water quality Stemming and control of water quantity
Food	Provision of food and safeguarding food safety and security
Health	Medical and hospital care Medicines, serums, vaccines and pharmaceuticals Bio-laboratories and bio-agents
Financial	Payment services/payment structures (private) Government financial assignment
Public & Legal Order and Safety	Maintaining public & legal order, safety and security Administration of justice and detention
Civil administration	Government functions Armed forces Civil administration services Emergency services Postal and courier services
Transport	Road transport Rail transport Air traffic Inland waterways transport Ocean and short-sea shipping
Chemical and nuclear industry	Production and storage/processing of chemical and nuclear substances Pipelines of dangerous goods (chemical substances)
Space and Research	Space Research

11.2 INFRASTRUCTURE INTERDEPENDENCIES

Virtually every CI depends on the availability of electricity supply. Meanwhile, the electricity infrastructure by itself can not properly function without others. For instance, the communication infrastructure is required to provide sensor measurements to the control systems and to send control instructions to the grid components. This dependency is entangled. If power supply is missing, telecom switches cannot be operated and a backup generator, even it is available, can fail after some time (see Table on failures in Data networks later in this section). The complex dependencies between CIs were illustrated by Rinaldi et al. as shown in Figure 26 below. This illustration is incomplete, but it provides a suitable illustration of complex system of critical infrastructures.

**Table 30. Critical infrastructure dependencies for interruptions for less than two hours [76]**

Failed CI	Effect on										
	Energy	ICT	Water	Food	Health	Financial	Order and safety	Civil admin.	Transport	Chemical and nuclear	Space and research
Energy	–	0.86	1.33	2.89	1.40	2.67	1.67	0.40	2.40	4.67	1.33
ICT	2.67	–	1.00	1.67	2.20	2.33	2.67	1.40	2.40	2.67	1.00
Water	0.83	0.57	–	1.56	1.20	0.00	1.00	0.60	0.20	1.00	0.67
Food	0.00	0.14	0.00	–	0.60	0.00	0.33	0.20	0.00	0.33	0.33
Health	0.50	0.14	0.00	0.78	–	0.00	1.67	0.60	0.00	0.33	0.00
Financial	0.17	0.71	0.00	1.22	0.20	–	0.33	0.00	0.60	1.33	0.00
Order and safety	0.83	0.43	0.33	1.00	1.00	1.67	–	1.40	0.80	1.00	0.00
Civil admin.	0.33	0.86	0.00	0.38	1.00	0.33	1.00	–	0.20	1.00	0.00
Transport	1.17	1.00	0.00	1.11	1.40	1.00	2.00	0.60	–	0.00	0.00
Chemical and nuclear	1.50	0.29	0.00	0.22	0.40	0.00	2.00	1.40	0.20	–	0.00
Space and research	0.17	0.57	0.00	0.00	0.00	0.00	0.00	0.00	0.20	0.00	–

Table 31. Critical infrastructure dependencies for interruptions of more than one week [76]

Failed CI	Effect on										
	Energy	ICT	Water	Food	Health	Financial	Order and safety	Civil admin.	Transport	Chemical and nuclear	Space and research
Energy	–	4.57	4.67	5.00	5.00	4.67	5.00	4.20	4.20	5.00	4.33
ICT	4.67	–	3.67	4.89	4.00	4.67	4.33	3.40	4.60	5.00	4.00
Water	3.50	3.43	–	4.22	3.80	1.00	3.67	3.00	2.60	3.67	3.00
Food	3.17	2.57	2.00	–	4.00	0.33	4.00	3.00	0.80	1.33	3.00
Health	3.00	2.00	1.33	3.11	–	0.67	5.00	3.60	1.20	1.00	2.00
Financial	3.00	2.43	2.00	4.22	2.40	–	2.00	0.75	2.20	2.67	3.00
Order and safety	3.67	2.57	2.33	3.56	2.60	4.33	–	3.40	2.80	2.00	2.67
Civil admin.	2.50	2.57	1.33	2.50	3.20	1.67	2.00	–	2.40	2.33	3.67
Transport	3.83	3.00	3.67	4.78	3.80	3.67	4.33	3.40	–	3.67	3.67
Chemical and nuclear	3.17	2.14	3.00	2.33	2.40	0.00	3.33	1.80	1.40	–	1.00
Space and research	1.50	2.29	0.67	1.00	0.60	0.00	1.33	1.00	0.60	0.00	–

Figure 27 and Figure 28 provide a graphical presentation of the tables and help to more easily identify what infrastructures are most influential and most inter-dependent. Dependency and influence are determined by taking arithmetic mean of influence/dependency of the infrastructures. ICT and Energy supply can be identified as the most important infrastructures. The figures can be used to assess the criticality of infrastructures in the sense of interdependencies. And clearly the disaster mitigation measures should address the most influential infrastructures first. Depending on the duration of the interruption dependencies of critical infrastructures change only slightly. Food, health and public safety are to be the most depending and thus vulnerable ones.

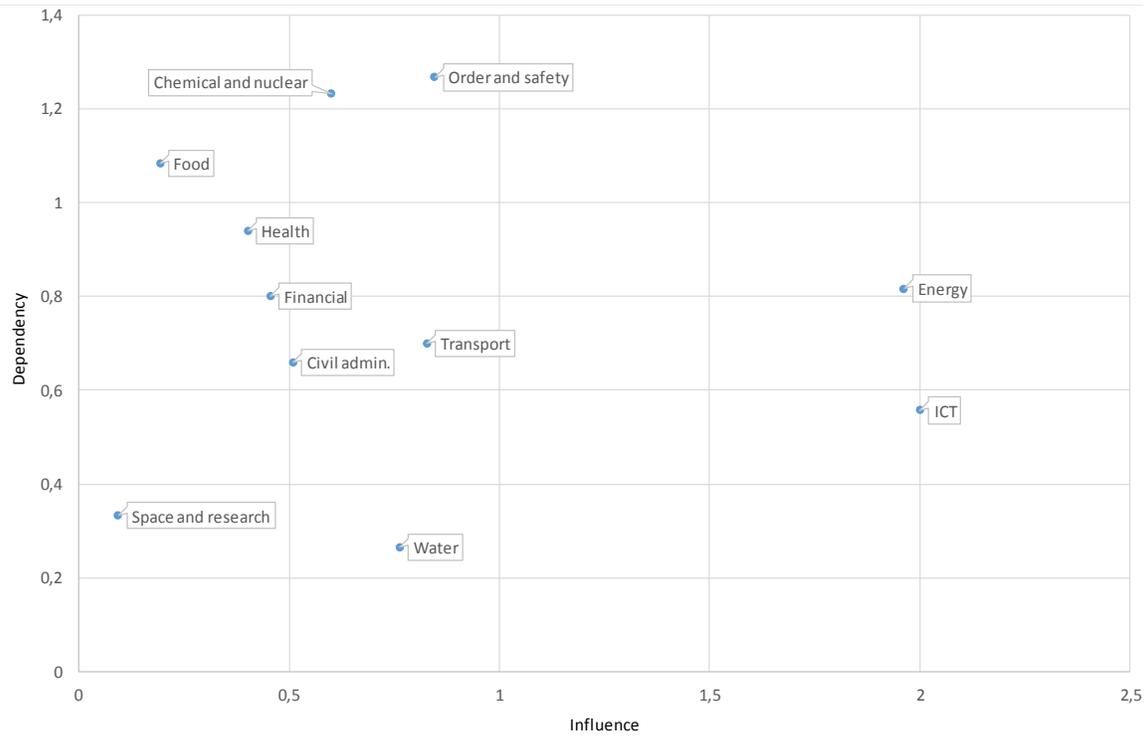


Figure 27. Dependencies and influences of interruptions lasting less than two hours [76]

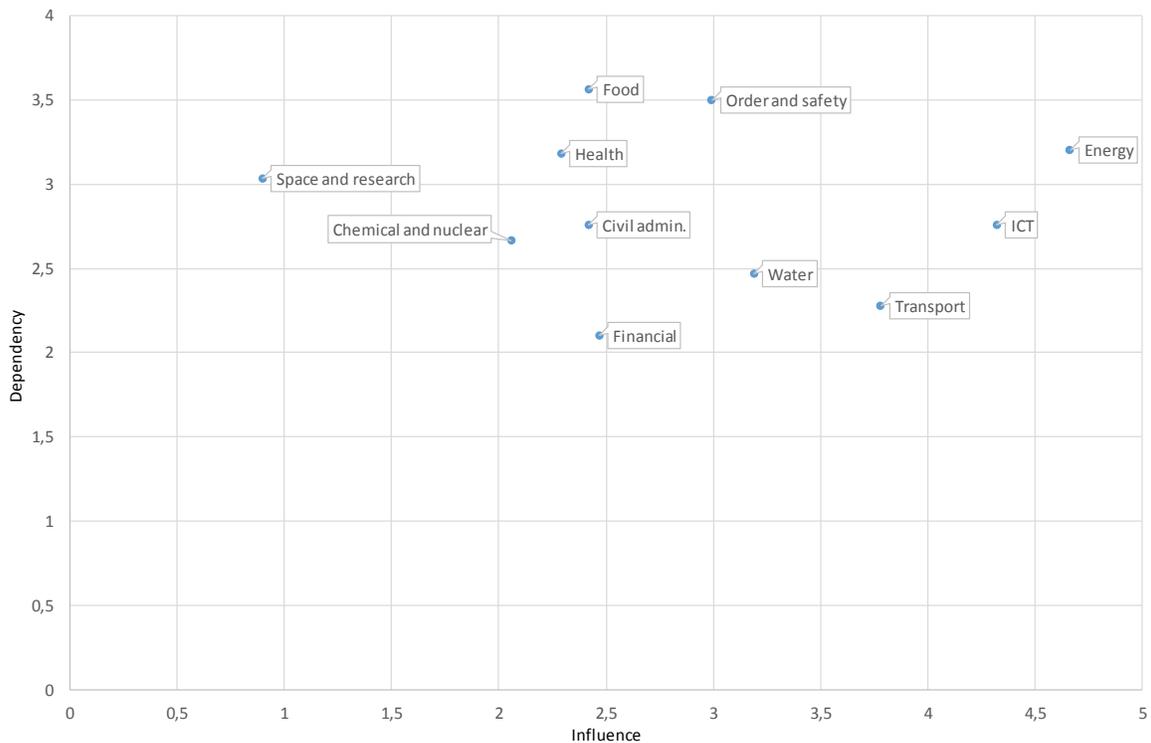


Figure 28. Dependencies and influences of interruptions lasting more than one week [76]

11.3 IMPACT OF OUTAGES TO NODES OF OTHER CIs

This subsection continues the consideration of how prolonged outages can degrade other connected CIs. It outlines the impact of large-scale power outages on nodes of other critical infrastructures with respect to three different time scales. Specifically, the results from [77] are being presented. Considering relevant threat events mapped to the timescale can help to understand how different critical infrastructures depend on the availability of electricity and how the lack of electricity threatens these infrastructures. It can ultimately help to reason about the significance of each infrastructure in the sense of a criticality rating. Listing threat events starts with ICT networks, which are probably the most closely connected to the electrical network.

Effects of power outages on information and communication technology

During blackouts communication networks in general and network nodes (e.g. switching centers, base stations, relay stations) in particular can be unavailable. Non-availability is often not the result of disruptions to the infrastructure, but of a failure of the end-user devices (telephones, Modem, PC, router). A failure of telecommunications networks can also be due to the increased communication volume.

Failure of ICT networks can severely impact crisis management of authorities and energy suppliers. Thus, they can particularly benefit from considering possible impacts of power outages on their communication systems. The relevant threat events can be as shown in tables below.

Table 32. Mobile communications

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<ul style="list-style-type: none"> - Immediate failure of unprotected base stations - Failure of protected base stations (2 h) - Failure of central link stations (Base Station Controller, BSC) (4 – 6 h) - Network overload 	<ul style="list-style-type: none"> - Loss of cell phones (depending on the charge state the battery) - Failure of emergency power-supplied base stations 	<ul style="list-style-type: none"> - Lack of fuel for emergency power supply - Loss of Mobile Switching Center (MSC) (about 4 days) - Loss of mobile phone devices (about 4 – 6 days without calls)

**Table 33. Landline**

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<ul style="list-style-type: none"> - Failure of ISDN telephones without emergency operation mode - Failure of router and back - Failure of cable modems - Short-term network interruptions - Failure of unprotected telephone exchanges 	<ul style="list-style-type: none"> - Failure of cordless telephones (depending on the charging state) - Failure of ISDN telephones with emergency operating mode - Partly failures in the network - Failure of smaller telephone exchanges 	<ul style="list-style-type: none"> - Failure of cordless telephones (depending on the charging state) - Failure of central telephone exchanges (About 3 – 4 days) - Lack of fuel for emergency power supply

Table 34. Internet

Scenario A (< 8h)	Scenario B (8 –24 h)	Scenario C (> 24 h)
<ul style="list-style-type: none"> - Failure of routers, switches, - Failure of modems - Failure of cable modems - Failure not UPS protected servers - Failure of PC and notebooks (2 – 5h) 	<ul style="list-style-type: none"> - Failure of notebooks 	<ul style="list-style-type: none"> - Lack of fuel for emergency power supply - Failure of the emergency power supply for data centers (approx. 1 week)

Table 35. Data networks

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<ul style="list-style-type: none"> - Failure of routers, switches - Failure of PCs and notebooks - Failure not UPS protected servers 		<ul style="list-style-type: none"> - Lack of fuel for emergency power supply - Failure of the emergency power supply for data centers (approx. 1 week)



Impact on water supply and de- sanitation

Water supply and sanitation is critical infrastructure to any city. This infrastructure operates under strict legal regulations and standards. These ensure the availability and quality of the drinking water, the management of crisis situations and prescribe water emergency supply regimes. Water storage capacity (in supply areas) must provide sufficient supply for the population for at least 24 hours. At the same time, in rural areas disturbances in the supply of drinking water can occur very quickly. If no emergency power is provided, boosting systems and pumping stations can fail shortly after a power interruption event.

Contrary to water supply, no regulations for sanitation facilities exist that specify prevention measures or emergency facilities (emergency generators) to handle power outages. Because of power outages, pumping stations and filters in urban drainage, sewerage system, or waste water treatment systems can stop functioning. Tables 38 and 39 illustrate some of the potential consequences.

Table 36. Water supply

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<ul style="list-style-type: none"> - Activation of emergency power supply - Breakdown of pumps without backup - Decreased water pressure - Breakdown of water supply in rural areas - Breakdown of external communication - Restricted administration 	<ul style="list-style-type: none"> - Breakdown of internal telephone system (availability ~10h) - Breakdown of battery powered monitoring systems(availability ~10h) - Breakdown of internal radio system 	<ul style="list-style-type: none"> - Reservoirs cannot be filled anymore - Fuel shortage backup supply (reserve for 5 days) - Possible problems with firefighting water



Table 37. Sanitation

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<p>Urban drainage / sewerage</p> <ul style="list-style-type: none"> - Failure of the pumps at storm-water overflow tanks - Failure of the pumps at sewer - Failure of the process control system (after about 2 – 3 h) <p>Treatment plant / sewage treatment</p> <ul style="list-style-type: none"> - Failure of mechanical cleaning stage (risk of obstruction) - Failure of compressor ventilation system - Failure of biological treatment - Failure of filtration - Failure of external communication networks - Limitation of the administrative activities 	<p>Treatment plant / sewage treatment</p> <ul style="list-style-type: none"> - Failure of monitoring - Thresholds are exceeded - Restarting of the bio-logical purification stage problematic (duration: several days) - Impairment of nitrification because temperature falls below threshold 	<p>Urban drainage / sewerage</p> <ul style="list-style-type: none"> - Flooding of low-lying roads and underpasses (for example at heavy rain) - Blockage of the sewer network - Hygiene problems (depending on weather) <p>Treatment plant / sewage treatment</p> <ul style="list-style-type: none"> - Failure of cooling water pumps - Sludge incineration - Failure sludge digestion - Shortage CO-substrate (approx. 3 – 4 days)

Effects of power outages on the fuel supply

Power outages can impact all stages of the value chain of the fuel supply chain, including

- refineries;
- tank farms;
- transport systems;
- petrol stations.

The tables below show the potential impact of a power failure on the fuel supply.



Table 38. Transportation systems

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<p>General</p> <ul style="list-style-type: none"> - Failure of communication network <p>Pipelines</p> <ul style="list-style-type: none"> - Failure of individual pumps - Activation battery operation - Switch the control, measuring and control equipment to battery power - Manual operation of valves - Extraction of crude oil with reduced throughput <p>Shipping</p> <ul style="list-style-type: none"> - Failure of pumps to debarkation of vessels (if not emergency power supplied) <p>Freight / tank cars</p> <ul style="list-style-type: none"> - Limitation of rail transport <p>Tank truck</p> <ul style="list-style-type: none"> - Failure of pumps for loading (if not emergency power supplied) - Traffic delays - Congestions in front of tank farms and refineries 	<p>Pipelines</p> <ul style="list-style-type: none"> - Operation of individual pumps with mobile power supplies 	<p>Pipelines</p> <ul style="list-style-type: none"> - Failure of monitoring, measuring and control equipment

**Table 39. Refineries**

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<p>General</p> <ul style="list-style-type: none"> – Failure of communication network <p>With island operation:</p> <ul style="list-style-type: none"> – Disconnection of the power grid and the power plants from the public electricity grid <p>Without island operation:</p> <ul style="list-style-type: none"> – Controlled shutdown of facilities – Curing of production batches in the plants – Activation of security valves for pressure relief – Increased emissions – Halt production 	<p>With island operation:</p> <ul style="list-style-type: none"> – Reduced production – Delay in transport of products – Congestions in transportation <p>Without island operation:</p> <ul style="list-style-type: none"> – Cleaning and repair works required 	<p>With island operation and failure pipelines:</p> <ul style="list-style-type: none"> – Crude oil bottleneck (After about 3 weeks)

Table 40. Petrol stations

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<ul style="list-style-type: none"> – Failure of communication network – Failure of the pumps – Loss of accounting system – Failure of monitoring systems – Additional supply from tank farms and filling of tanks possible in principle, but failure of overfill prevention 	<p>Supply of selected petrol stations with emergency power supply.</p>	

Effects on health care

As mentioned, healthcare as a critical infrastructure that is highly dependent on the electricity supply. As it is directly connected to well-being of citizens, threat events to hospitals are particularly relevant within the IRENE scope. In the health care domain power outages can lead to a disturbance of the supply processes (e.g. medical devices, food, water, and medicines), the failure of critical infrastructure and technical devices, and the organizational issues.

Table 41. Hospitals

Scenario A (< 8h)	Scenario B (8–24h)	Scenario C (> 24 h)
<p>Technology</p> <ul style="list-style-type: none"> - Activation of the emergency power supply - Failure of external communication networks - Failure of the district heating - Capacity problems of emergency power supply - Problems in the transition to emergency power supply - Compliance with standards problematic - Disturbance of security and locking systems <p>Supply</p> <ul style="list-style-type: none"> - Failure/malfunction hot water supply <p>Organization</p> <ul style="list-style-type: none"> - Increased volume of patients - Additional load of personnel - Requests from family members - Reduction of administrative activities 	<p>See scenario A, as emergency power supply needs to be available by law</p>	<p>Technology</p> <ul style="list-style-type: none"> - Failure of emergency power supply - Failure of medical equipment (diagnostics) - Failure of medical equipment (treatment) - Failure of cooling systems (drugs) - Failure of the OR-heating - Failure of the air conditioning - Failure of the general heat supply - Failure of the lift equipment - Failure of laboratories - Failure of lighting - Failure of sterilization facilities - Failure of the patient call system - Failure of toilets <p>Supply</p> <ul style="list-style-type: none"> - Failure of the kitchen (food preparation and dishes) - Failure of the water supply - Shortages of fresh laundry - Food shortages - Supply bottlenecks drugs - Lack of fuel (diesel for emergency power) <p>Organization</p> <ul style="list-style-type: none"> - Alternative compliance with hygiene standards - Failure of the electronic patient administration - Problems in the provision of personnel - Additional advent of non-sick ("lighthouse effect")

Impact of power outages on the industry

The extent of potential effects of power outages on industrial plants is significantly influenced by the dependability of production processes on power supply. It is therefore important to consider: the required amount of electricity, the type of power supply, the presence of redundant systems (such as own power- generation and electricity networks with possible isolated operation), and the availability of emergency facilities.

Business disruptions can occur due to: the direct loss of production, through supply chain interruptions, through interruptions of critical infrastructure, or through obstruction of administrative and planning processes.

Table 42. Impact of power outages on the industry

Scenario A (< 8h)	Scenario B (8 – 24 h)	Scenario C (> 24 h)
<p>General</p> <ul style="list-style-type: none"> - Loss of production <p>Facilities</p> <ul style="list-style-type: none"> - Failure of individual pumps and valves - Activation of safety valves for pressure relief - Switch of control and measurement devices to battery operation - Controlled shutdown of the plants - Reduction of production capacity - Failure of cooling systems - Release of hazardous substances <p>Supply Chain</p> <ul style="list-style-type: none"> - Failure of internal logistics systems - Failure of external logistics systems (e.g. rail) - Quality restrictions 	<p>General</p> <ul style="list-style-type: none"> - Lack of information - Send employees home - Transportation problems of employees - Lack of staff (e.g. for monitoring) <p>Facilities</p> <ul style="list-style-type: none"> - Damage to equipment, by curing and contamination - Operation of individual safety-related system components with mobile emergency power supply - Operation of facilities in safe mode <p>Critical infrastructures</p> <ul style="list-style-type: none"> - Failure of the water supply <p>Supply Chain</p> <ul style="list-style-type: none"> - Congestion on delivery and embarkation 	<p>General</p> <ul style="list-style-type: none"> - Loss of image <p>Facilities</p> <ul style="list-style-type: none"> - Failure of monitoring and , measurement devices - Cleaning and repair measures necessary - Problems with recommissioning <p>Critical infrastructures</p> <ul style="list-style-type: none"> - Failure / malfunction of the emergency power supply (due to lack of fuel) <p>Supply Chain</p> <ul style="list-style-type: none"> - Delivery bottlenecks with customers - Delivery bottlenecks with suppliers - Penalties



<p>Critical infrastructures</p> <ul style="list-style-type: none">- Failure of communication networks- Activation of the emergency power supply Switch of power supply (if possible to island operation)- Failure of heat supply- Loss of nitrogen supply (explosion protection) <p>Administration</p> <ul style="list-style-type: none">- Loss of data, lack of information		
---	--	--

The threat events described in this subsection highlights how prolonged outages can impact nodes of several critical infrastructures. The diversity of threat events, their dispersion over time, and the possibility that the nodes can have emergency power supply available make it hard to estimate how exactly a prolonged outage can impact on a society. The next section briefly illustrates several ways how it can potentially be done.

11.4 COSTS OF BLACKOUTS

On a high level, costs caused by power outages can be split into three different categories [78]:

- *Direct outage costs* result directly from the outage and can be relatively easy to estimate. They can be broken down, as pointed out in [79], into damages related to lost production, idle resources, effort for restarting production processes, spoilage of food or materials, costs associated with human health and safety, utility costs, etc. Societal costs include lack of transportation and uncomfortable building temperatures;
- *Indirect outage costs* are mainly caused by prolonged outages. Indirect costs are more difficult to quantify, as well it is harder to discriminate between societal and economic costs. Indirect costs can be linked to other infrastructures failing because of blackouts. Often this category includes costs related to social unrest. At the same time, recent studies show that crime rates can even decrease during times of outages [78]. It makes the idea of adding crime-related costs to indirect outage costs debatable;
- *Long term costs* arise mainly from measures taken to prevent or mitigate the impact of future outages. This could be a whole range of consequences from installing protective switchgear,



standby power supplies, and cogeneration up to relocation of facilities. Long term costs are most difficult to estimate as they cannot be assigned to a single event.

Numerous approaches how to calculate the costs have been proposed. Although they are barely comparable, it is possible to group them as related to three classes: analytical evaluation, case studies, and customer surveys. While one can expect case studies to be the most reliable, only few of them can be found in literature.

Analytical evaluation approaches are mainly based on macroeconomics and use existing data like tariffs, gross domestic product (GDP) or gross value added (GVA) [80] for non-domestic losses, and customer wage rates for domestic losses. The GDP and GVA (GDP without subsidies and taxes) are metrics for a country's economic production.

Value of Lost Load (VoLL, €/kWh) is the metric often used to describe blackout costs. Based on GVA the VoLL can be written as:

$$VoLL = \frac{GVA}{EC} \left[\frac{\text{€}}{\text{kWh}} \right],$$

where EC describes the annual electricity consumption. This approach assumes that there is for replacement for electricity. While this assumption holds true for most production, it does not necessarily stay applicable for the service sector. However, the service sector also relies heavily on the availability of electricity. Therefore, significant preplanning might result in additional costs [80].

The value of domestic losses is more difficult to calculate. De Nooij et al. [81] determine the value based on the costs of leisure time lost due to an outage. They assume that most activities people follow in their leisure time depend on electricity like e.g. watching TV, listening to radio, etc. Losses like the spoilage of goods in the freezer or the failing of the heating system have not been accounted in this approach. Noticeably, households account for 25% of the electricity consumption.

The results of this study [81] are given in Table 43. The costs for households are estimated as described above. Costs for other economic sectors are based on the value added calculation.

Table 43. VoLL for households, firms and government in the Netherlands (2001) [81]

	Electricity demand (GWh)	Electricity use as percentage of total electricity use	‘Value’ (million euros)	‘Value’ as percentage of total ‘value’	‘Value’ of lost load (€/kW h)
Agriculture	2889	3.3	11,26	1.5	3.90
Energy sector	72,361	–	22,91	3.0	0.32
Manufacturing	34,009	38.4	63,44	8.4	1.87
Construction	750	0.9	24,79	3.3	33.05
Transport	1577	1.8	19,59	2.6	12.42
Services	24,944	28.1	198,13	26.1	7.94
Government	2389	2.7	80,04	10.5	33.50
Firms and government	66,558	75.1	397,25	52.3	5.97
Households	22,100	24.9	362,06	47.7	16.38
Firms, government and households	88,658	100	759,30	100	8.56

According to the table, if load shedding needs to be implemented during a power outage, it would be most economically beneficial when households, construction and government users get prioritized power supply.

Another way to estimate costs of outages is by means of customer surveys. These surveys are often used to determine consumer’s the willingness-to-pay (WTP) for an interrupted supply or the willingness-to-accept (WTA) payments for interruptions [82] [83]. As these surveys ask customers how much they would be willing to accept as payment to experience an outage, to an extent they account for “Immaterial losses” to households that include stress, inconvenience, fear and anxiety. Different scenarios are presented to the survey participants and they can choose if they would prefer to pay a certain amount of money or experience the outage [82].

In [83] the authors estimated a VoLL for UK SME and domestic customers. Values for industrial and commercial customers were based on GVA. The tables below give the VoLL for a one hour electricity outage. The table shows that the VoLL for SMEs is several times higher than for residential users. An explanation could be that households have more flexibility in the way they use electricity: they can postpone tasks requiring electricity until it is available again.

**Table 44. Comparison of WTA and WTP €/kWh estimates by time of outage [83]
converted from £/MWh assuming 1 £ = 1,18 €**

		Summer				Winter			
		Off-peak		Peak		Off-peak		Peak	
		Non-work	Work day	Work day	Non-work	Non-work	Work day	Work day	Non-work
SME	VoLL WTA	44,77	43,53	39,36	40,35	52,10	46,27	41,88	47,04
	VoLL WTP	25,80	22,74	23,66	28,53	31,09	25,16	25,59	32,87
Residential	VoLL WTA	1,13	8,21	10,92	13,15	12,96	0,11	12,14	1,39
	VoLL WTP	3,26	(0,12) ⁸	(0,12)	2,13	2,64	(0,37)	(0,25)	1,95

**Table 45: Estimate of electricity UK VoLL for commercial and industrial users,
(based on 2011 data) [83] converted from £/MWh assuming 1 £ = 1,18 €**

	Total GVA €/yr. (millions)	Total Electric use (GWh)	VoLL (€/kWh)
Total	209,33	107,23	1,95
Total (manufacturing — 10 – 32)	174,67	98,25	1,78

Finally, case studies can provide insights into the impact of outages. While the causes for power outages have been extensively analyzed, studies on the impact of outages are rare. In general, there are two approaches for analyzing the impact costs. First the impact of a supply interruption is determined and then associated costs are identified. The second more reliable cost assessment is done using surveys after the incident. In their report [84] the Royal Academy of Engineering provides an overview of several outages.

⁸ Values in brackets indicate that users are not willing to pay a value statistically different from € 0.

Table 46. Outage case studies [84]

Area	Number of people affected	Duration	Cost estimates	Major impacts
Northeast US & Ontario, Canada [85]	50 million	1 to 4 days	\$4.5 to 8.2 billion	Fire caused by candles, lower crime rate, high number of emergency calls
California [86]	1,5 million	Rolling blackouts for one year	\$40 billion additional energy costs, GDP loss of 0,7 – 1,5%	Increased electricity prices, negative credit watch for California
20 countries in Western Europe and North Africa [29]	15 million	2 hours	No overall data available, \$100 million for spoiled food	People trapped in lifts
Italy, Switzerland [87]	56 million	1,5 – 9 hours	€ 1,182 million	People trapped in trains and underground
Cyprus [88]	1 million	2 – 4 hours, rolling blackouts for one month	€196 to 30,598 million	Social and political impacts were minimized through efficient communication

All in all, although numerous approaches for estimating the costs of outages have been proposed, it is difficult to get reliable information about the real costs. Most of the approaches have some shortcomings as they introduce either simplifications that make data manageable or they are based on customer surveys. In the latter case, the results indicate prices that single users or companies are willing to pay, even though it is difficult for the user to assess the real impact of an outage. Furthermore, most surveys are based on outages of one hour and do not provide an estimate for outages lasting e.g. more than 24 hours.

Another difficulty in understanding blackout costs is related to how much a city is prepared to accept prolonged blackouts and how it plans to act. If organizations or communities have emergency plans, which are well aligned and properly communicated with the public, the impact on the society might be less. Similarly, the availability of generation capabilities and emergency personnel can help to mitigate consequence and thus reduce costs of blackouts.

For the time being, more precise information is not available. Given the outlined state of the art in research and practices, it appears that the VoLL-based calculations are the most important metrics for obtaining ratings relevant to the scope and tasks of the IRENE project.



12 REFERENCES

- [1] IRENE, “D2.1 – Threats identification and ranking,” 2015. [Online]. Available: <http://ireneproject.eu/wp-content/uploads/2016/01/IRENE-D2.1.pdf>.
- [2] VIKING, “Vital Infrastructure, Networks, Information and Control Systems Management,” February 2016. [Online]. Available: <https://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/cc/proj/v/viking-1.407871>.
- [3] CRISALIS, “Securing critical infrastructures,” February 2016. [Online]. Available: <http://www.crisalis-project.eu/>.
- [4] AFTER, “A Framework for electrical power systems vulnerability identification, defense and Restoration,” February 2016. [Online]. Available: http://cordis.europa.eu/project/rcn/100196_en.html.
- [5] SESAME, “Securing the European Electricity Supply Against Malicious and accidental threats,” February 2016. [Online]. Available: <https://www.sesame-project.eu/>.
- [6] SoES, “Security of Energy Systems,” February 2016. [Online]. Available: <http://www.soes-project.eu/>.
- [7] The World Bank, “Power outages in firms in a typical month (number),” February 2016. [Online]. Available: <http://data.worldbank.org/indicator/IC.ELC.OUTG/countries/1W?display=map>.
- [8] World Bank Group, “Infrastructure dataset,” February 2016. [Online]. Available: <https://www.enterprisesurveys.org/data/exploreTopics/Infrastructure>.
- [9] J. Wirfs-brock, “Power Outages On The Rise Across The U.S.,” February 2016. [Online]. Available: <http://insideenergy.org/2014/08/18/power-outages-on-the-rise-across-the-u-s/>.
- [10] DoE, “Electric Disturbance Events (OE-417) Annual Summaries,” February 2016. [Online]. Available: https://www.oe.netl.doe.gov/OE417_annual_summary.aspx.
- [11] CPNI, “Security for Industrial Control Systems,” February 2016. [Online]. Available: <https://www.cpni.gov.uk/advice/cyber/Security-for-Industrial-Control-Systems/>.
- [12] M. Balas, “Feedback control of flexible systems,” *IEEE Transactions on Automatic Control*, vol. 23, no. 4, pp. 673-679, 1978.



- [13] G. Dondossola, J. Szanto, M. Masera and I. Nai Fovino, “Effects of intentional threats to power,” *Int. J. Critical Infrastructures*, vol. 4, pp. 129-143, 2008.
- [14] D. Kundur, X. Feng, S. Liu, T. Zourntos and K. Butler-Purpy, “Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid,” in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010.
- [15] A. Garcia Illera and J. Vazquez Vidal, “Blackhat Europe Briefings October 16 & 17,” 2014. [Online]. Available: <https://www.blackhat.com/eu-14/briefings.html>. [Accessed February 2016].
- [16] Troutman Sanders LLP, “NERC Issues AURORA Alert,” 2010. [Online]. Available: <http://www.troutmansandersenergyreport.com/2010/10/nerc-issues-aurora-alert/>.
- [17] NERC, “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,” June 2010. [Online]. Available: <http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf>.
- [18] ICS-CERT, “Alert (ICS-ALERT-14-176-02A) ICS Focused Malware (Update A),” 2014. [Online]. Available: <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A>.
- [19] ICS-CERT, “Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E),” February 2016. [Online]. Available: <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.
- [20] R. Lipovsky and A. Cherepanov, “BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry,” January 2016. [Online]. Available: <http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/>.
- [21] E-ISAC, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” 2016. [Online]. Available: <https://www.esisac.com/api/documents/4199/publicdownload>.
- [22] Dell Security, “Dell Security Annual Threat Report,” 2015. [Online]. Available: <http://www.sonicwall.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf>.
- [23] ICS-CERT, “ICS-CERT Year in Review,” 2014. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf.
- [24] ENISA, “ENISA Threat Landscape 2015,” 2016. [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/etl2015/at_download/fullReport.
- [25] Intel, “Prioritizing Information Security Risks with Threat Agent Risk Assessment,” 2009. [Online]. Available: http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_



RiskAssessment.pdf.

- [26] SESAME, “D1.1 - Report on the analysis of historic outages,” 2011. [Online]. Available: <https://www.sesame-project.eu/publications/deliverables/d1-1-report-on-the-analysis-of-historic-outages/view>.
- [27] The Open Group, “Technical Standard. Risk Taxonomy,” 2009. [Online]. Available: <http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf>.
- [28] CESG, “HMG IA Standard Numbers 1 & 2: Information Risk Management,” 2012. [Online]. Available: https://www.cesg.gov.uk/content/files/guidance_files/Information%20Risk%20Management%20%28IS1%20%26%20%29_4.0.pdf.
- [29] CRO Forum, “Power Blackout Risks. Risk Management Options. Emerging Risk Initiative - Position Paper,” 2011. [Online]. Available: https://www.allianz.com/v_1339677769000/media/responsibility/documents/position_paper_power_blackout_risks.pdf.
- [30] Canada Gov, “All Hazards Risk Assessment Methodology Guidelines 2012-2013,” 2012. [Online]. Available: <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ll-hzrds-sssmnt/ll-hzrds-sssmnt-eng.pdf>.
- [31] Commission on CI Protection, “Critical Foundations. Protecting America's infrastructures,” 1997. [Online]. Available: <https://www.fas.org/sgp/library/pccip.pdf>.
- [32] M. Rogers, “The development of a meaningful hacker taxonomy: a two dimensional approach,” 2005.
- [33] M. Rogers, “A two-dimensional circumplex approach to the development of a hacker taxonomy,” *International journal of digital forensics & incident*, vol. 3, no. 2, pp. 97-102, 2006.
- [34] A. Rege, *Cybercrimes against the Electricity Sector: Exploring Hacker and Industry Perceptions*, Newark, NJ, USA: Rutgers University, 2012.
- [35] M. Kilger, A. Ofir and J. Stutzman, “Profiling,” in *Know Your Enemy: Learning about Security Threats (2nd Edition)*, Addison-Wesley, 2004.
- [36] Octave Allegro, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” 2007. [Online]. Available: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf.
- [37] C. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley Professional, 2002.



- [38] McAfee, “McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet,” 2005. [Online]. Available: <http://www.softmart.com/mcafee/docs/McAfee%20NA%20Virtual%20Criminology%20Report.pdf>.
- [39] Intel, “Threat Agent Library Helps Identify Information Security Risks,” 2007. [Online]. Available: <https://communities.intel.com/docs/DOC-1151>.
- [40] Mandiant, “APT1: Exposing One of China's Cyber Espionage Units,” 2013. [Online]. Available: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
- [41] M. Caselli and F. Kargl, “D5.1 Security Testing Methodology,” 2012. [Online]. Available: http://www.crisalis-project.eu/sites/crisalis-project.eu/files/crisalis_deliverable-D5.1.pdf.
- [42] H. Dui, L. Zhang, S. Sun and S. Si, “The study of multi-objective decision method based on Bayesian network,” in *Industrial Engineering and Engineering Management (IE&EM), 2010 IEEE 17Th International Conference on*, 2010.
- [43] E. Vriezokolk, “RASTER: Risk Assessment by Stepwise Refinement,” 2016. [Online]. Available: <https://hmi.ewi.utwente.nl/~vriezokolke/Raster/Raster/About.html>.
- [44] B. Biringer, R. Matalucci and O. S.L., *Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures*, John Wiley & Sons, 2007.
- [45] Department of the Army, “FM 3-38 Cyber electromagnetic activities,” Headquarters, 2014. [Online]. Available: <http://fas.org/irp/doddir/army/fm3-38.pdf>.
- [46] Risidata, “Navy Radar Shuts Down SCADA Systems,” 2016. [Online]. Available: <http://www.risidata.com/Database/Detail/navy-radar-shuts-down-scada-systems>.
- [47] Y. Parfenov, L. Zdoukhov, W. Radasky and M. Ianoz, “Conducted IEMI threats for commercial buildings,” vol. 46, no. 3, 2004.
- [48] F. Sabath and H. Garbe, “Risk potential of radiated HPEM environments,” in *IEEE International Symposium on Electromagnetic Compatibility, EMC 2009*, 2009.
- [49] D. Mansson, R. Thottappillil and M. Backstrom, “Methodology for Classifying Facilities With Respect to Intentional EMI,” vol. 51, no. 1, pp. 46-52, 2009.
- [50] E. Genender, H. Garbe and F. Sabath, “Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level,” vol. 56, no. 1, pp. 200-207, 2014.
- [51] S. Bosworth, M. E. Kabay and W. E., *Computer Security Handbook, Set*, John Wiley & Sons,



2012.

- [52] R. Langner, “Cyber-Physical Attack Engineering,” 2015. [Online]. Available: <http://vimeopro.com/s42012/s4x15-week/video/121427876>.
- [53] M. Yampolskiy, P. Horvath, X. Koutsoukos, Y. Xue and J. Sztipanovits, “Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach,” in *5th International Symposium on Resilient Control Systems (ISRCs)*, 2012.
- [54] CNN, “Staged cyber attack reveals vulnerability in power grid,” 2007. [Online]. Available: <https://www.youtube.com/watch?v=fJyWngDco3g>.
- [55] M. Zeller, “Myth or reality — Does the Aurora vulnerability pose a risk to my generator?,” in *64th Annual Conference for Protective Relay Engineers*, 2011.
- [56] FLOODsite , “Deliverable D9.1 Evaluating flood damages: guidance and recommendations on principles and methods,” 2007. [Online]. Available: http://www.floodsite.net/html/partner_area/project_docs/T09_06_01_Flood_damage_guidelines_D9_1_v2_2_p44.pdf.
- [57] PPS, “Planning Policy Statement 15 (PPS15),” 2006. [Online]. Available: http://www.planningni.gov.uk/index/policy/planning_statements_and_supplementary_planning_guidance/pps15-flood-risk.pdf.
- [58] Moreton Bay Regional Council, “Flood check Fact sheet 5. Understanding the Likelihood of Floods,” 2015. [Online]. Available: <https://www.moretonbay.qld.gov.au/uploadedFiles/moretonbay/living/floodplains/likelihood-of-floods.pdf>.
- [59] H. Kreibich and B. Dimitrova, “Assessment of damages caused by different flood types,” in *Flood Recovery, Innovation and Response II, (Transactions on Ecology and the Environment; 133)*, 2010.
- [60] FEMA, “Flood Risk Assessment,” 2007. [Online]. Available: <https://training.fema.gov/hiedu/docs/fmc/chapter%204%20-%20flood%20risk%20assessment.pdf>.
- [61] C. Scawthorn, “HAZUS-MH Flood Loss Estimation Methodology. I: Overview and Flood Hazard Characterization.,” p. 60–71, 2006.
- [62] C. Scawthorn, “HAZUS-MH Flood Loss Estimation Methodology. II. Damage and Loss Assessment,” p. 72–81, 2006.
- [63] FEMA, “Department of Homeland Security, Federal Emergency Management Agency,” 2011. [Online]. Available: <http://www.fema.gov/media-library-data/20130726-1820-25045-8814/>



hzmh2_1_fl_um.pdf.

- [64] FEMA , “Hazus-MH User’s Manual, Appendix F: Hazus-MH Data Dictionary,” 2011. [Online]. Available: http://www.fema.gov/media-library-data/20130726-1800-25045-8485/hazus2_appf.pdf.
- [65] CEER, “CEER Benchmarking Report 5.1 on the Continuity of Electricity Supply Data update, Ref: C13-EQS-57-03,” 2014. [Online]. Available: http://www.ceer.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_PAPERS/Electricity/Tab3/C13-EQS-57-03_BR5.1_19-Dec-2013_updated-Feb-2014.pdf.
- [66] EEI, “Out of Sight, out of mind 2012. An updated Study on the Undergrounding of Overhead Power Lines,” 2013. [Online]. Available: <http://www.eei.org/issuesandpolicy/electricreliability/undergrounding/documents/undergroundreport.pdf>.
- [67] PubSafe, “Threats to Canada’s Critical Infrastructure,” 2003. [Online]. Available: <https://www.publicsafety.gc.ca/lbr/archives/cn000034012674-eng.pdf>.
- [68] Entergy, “Should Power Lines be Underground?,” 2008. [Online]. Available: http://www.entergy.com/2008_hurricanes/Underground-lines.pdf.
- [69] K. Hirose, J. Reilly and H. Irie, “The Sendai microgrid operational experience in the aftermath of the tohoku earthquake: a case study.,” 2013.
- [70] D. Sheehan, “Remembering the Aurora flood of 1996,” 18 July 2011. [Online]. Available: <http://www.examiner.com/article/remembering-the-aurora-flood-of-1996>.
- [71] US Geological survey, “Floods of July 18–20, 1996, in Northern Illinois,” 1997. [Online]. Available: http://il.water.usgs.gov/pubs/ofr97_425.pdf.
- [72] Homefacts, “Hurricane Information For Naperville, IL,” 2016. [Online]. Available: <http://www.homefacts.com/hurricanes/Illinois/Dupage-County/Naperville.html>.
- [73] EU Commission, *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Official Journal of the European Union, 2008.
- [74] EU Commission, *Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection COM (2006) 787 final*, 2006.
- [75] S. Rinaldi, J. Peerenboom and T. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies,” vol. 21, no. 6, pp. 11-25, 2001.



- [76] A. Laugé, J. Hernantes and J. Sarriegi, “Critical infrastructure dependencies: A holistic, dynamic and quantitative approach,” vol. 8, pp. 16-23, 2015.
- [77] M. Hiete, *Krisenhandbuch Stromausfall Baden-Württemberg*, Stuttgart, Bonn : Innenministerium Baden-Württemberg, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), 2010.
- [78] G. Wacker and R. Billinton, “Customer cost of electric service interruptions,” in *Proceedings of the IEEE* 77.6, 1989.
- [79] D. Lorenz, *Kritische Infrastrukturen aus Sicht der Bevölkerung*, 2010.
- [80] S. Piaszeck, L. Wenzel and A. Wolf, *Regional Diversity in the Costs of Electricity Outages – Results for German Counties*, 2013.
- [81] M. De Nooij, C. Koopmans and C. Bijvoet, “The value of supply security: The costs of power interruptions: Economic input for damage reduction and investment in networks,” vol. 29, no. 2, pp. 277-295, 2007.
- [82] J. Reichl, M. Schmidthaler and F. Schneider, “The value of supply security: The costs of power outages to Austrian households, firms and the public sector,” vol. 36, pp. 256-261, 2013.
- [83] London Economics, “The Value of Lost Load (VoLL) for Electricity in Great Britain,” 2013. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/224028/value_lost_load_electricity_gb.pdf.
- [84] Royal Academy of Engineering, “Counting the cost: the economic and social costs of electricity shortfalls in the UK,” November 2014. [Online]. Available: <http://www.raeng.org.uk/publications/reports/counting-the-cost>.
- [85] ELCON, “The economic impacts of the August 2003 blackout,” Washington DC, 2004.
- [86] R. Farmer, D. Zimmerman and C. G., “Causes and lessons of the California electricity crisis,” US Congressional Budget Office, 2001.
- [87] M. Schmidthaler, J. Reichl and J. Cohen, “Assessing the socio-economic effects of power outages in the European Union ad hoc using www.blackoutsimulator.com,” in *CIREN Workshop*, Rome, 2014.
- [88] T. Zachariadis and A. Poullikkas, “The costs of power outages: A case study from Cyprus,” vol. 51, pp. 630-641, 2012.



13 ABBREVIATIONS

CI	Critical Infrastructure
EMP	ElectroMagnetic pulse
FAIR	Factor Analysis of Information Risk
GDP	Gross Domestic Product
GVA	Gross Value Added
HEMP	High-altitude EMP
HILF	High-Impact, Low-Frequency
HVAC	Heating, Ventilation, and Air Conditioning
IEMI	Intentional ElectroMagnetic Interference
LEF	Loss Event Frequency
SCADA	Supervisory Control And Data Acquisition
Tcap	Threat capability
TEF	Threat Event Frequency
VoLL	Value of Lost Load
WBG	World Bank Group



A FIRST APPENDIX. IRENE THREAT ANALYSIS

A.1 IRENE GRID COMPONENTS (LIST FROM IRENE D2.1)

Image	Name	Code	Description
<i>Connections</i>			
	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.
	Connection Adapter with Energy Transformer	CAT	Adapter that has also the ability to transform the energy and make it usable from element that needs lower voltages.
	Long-Range Connector	LRC	Component that indicates connections between far elements at the edges of the connections.
<i>Energy Provider</i>			
	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.
<i>Building</i>			
	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 ...
<i>Data Center</i>			
	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 system provides the basic functionality for implementing EMS or DMS, especially provides the communication with the substations to monitor and control the grid
<i>Others</i>			
	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.



A.2 IRENE THREAT EVENTS LIST ATTRIBUTED TO THREAT ACTORS

IRENE Index	IRENE Event	NIST/IRENE categories ⁹	Relations and dependencies ¹⁰		
			C1: Commodity threats (not targeted)	C2: Hactivism (targeted and persistent)	C3: APT (advanced)
1	Perform perimeter network reconnaissance/scanning	PRGI		X	X
2	Gather information using open source discovery of organizational information	PRGI	X	X	X
3	Perform reconnaissance and surveillance of targeted organizations	PRGI		X	X
4	Craft phishing attacks ¹¹	CCAT	X	X	X
5	Create and operate false front organizations to inject malicious components into the supply chain or deliver known/modified malware to internal organizational information systems	DIIMC			X

⁹ List of adversarial (ADV) categories: PRGI — Perform reconnaissance and gather information; CCAT — Craft or create attack tools; DIIMC — Deliver/insert/install malicious capabilities; EC — Exploit and compromise; CA — Conduct an attack (i.e., direct/coordinate attack tools or activities); AR — Achieve results (i.e., cause adverse impacts, obtain information); CC — Coordinate a campaign.

List of non-adversarial (NA) categories: ACC — Accidental; ENV — Environmental; HI — Hardware and Implementation.

¹⁰ We outline three classes of malicious external threat sources as follows:

- C1: Commodity (or opportunistic) threat source. This class is characterized by relatively low *Focus (Targeting + Intent)* and *Capabilities* characteristics;
- C2: Targeted threat source. This class extends the threats posed by the commodity class and possesses higher *Focus* characteristic.
- C3: Advanced Persistent Threat class. This class extends the threats posed by C2 and possesses advanced *Capabilities*. There are possibilities that C3 sources collude with insiders.

¹¹ This deliverable highlights that threat 4 as representative of the CCAT category can be differentiated into: 4a. Preparing cyber-attack (including phishing); 4b. Preparing physical attacks; and 4c. Preparing cyber-physical attacks with IEMI devices.



6	Install sniffers or scanning devices on organizational information systems and networks	DIIMC		X	X
7	Insert subverted individuals into organizations	DIIMC			X
8	Exploit physical access of authorized staff to gain access to organizational facilities	EC		X	X
9	Exploit poorly configured or unauthorized information systems exposed to the Internet	EC	X	X	X
10	Exploit split tunneling	EC		X	X
11	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones)	EC	X	X	X
12	Exploit recently discovered vulnerabilities	EC	X	X	X
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	EC			X
14	Compromise software of organizational critical information systems	EC		X	X
15	Conduct communications interception attacks	CA		X	X
16	Conduct wireless jamming attacks	CA		X	X
17	Conduct attacks using unauthorized ports, protocols and services	CA	X	X	X
18	Conduct Denial of Service (DoS) attack	CA	X	X	X
19	Conduct physical attacks on organizational facilities	CA			X
20	Conduct cyber-physical attacks on organizational facilities	CA		X	X

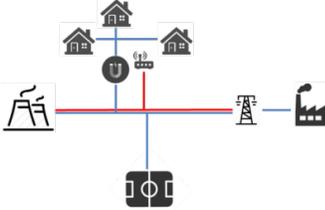
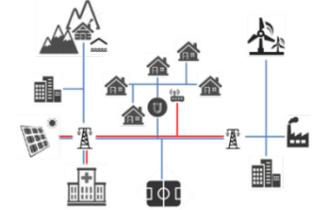
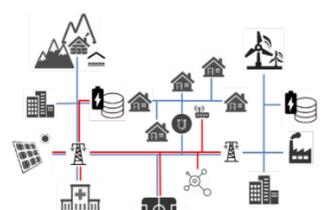
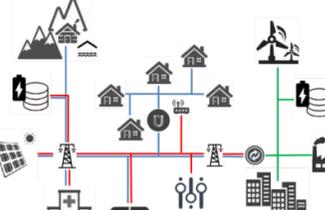
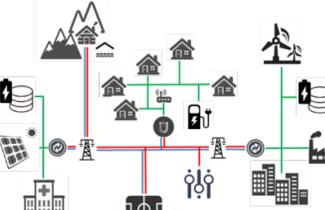


D2.2 — Societal impact of attacks and attack motivations

21	Conduct Man In the Middle attacks	CA		X	X
22	Conduct social engineering attacks targeting and compromising personal devices of critical employees	CA		X	X
23	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement)	AR	X	X	X
24	Obtain unauthorized access.	AR	X	X	X
25	Obtain information by opportunistically stealing or scavenging information systems/components	AR	X	X	X
26	Coordinate a campaign of multi-staged (e.g., hopping) or multi-typed (e.g outsider, insider, supplier) attacks	CC		X	X
27	Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome	CC			X
28	Coordinate a campaign that spreads attacks across organizational systems from existing presence	CC			X
29	Spill sensitive information	ACC	Can be precursor to threat events 1 – 3		
30	Mishandling of critical and/or sensitive information by authorized users	ACC	Similarly to threat event 29, it can lead to threat events 1 – 3		
31	Incorrect privilege settings	ACC	Incorrect privilege settings can directly lead to multiple other threat events, including events 23 – 25		
32	Earthquake at primary facility	ENV	Can lead to threat event 33		
33	Fire at primary/backup facility	ENV	-		
34	Flood at primary/backup facility	ENV	-		
35	Hurricane at primary/backup facility	ENV	Can lead to threat events 33 and 34		
36	Resource depletion	HI	-		
37	Introduction of vulnerabilities into software products	HI	Can lead to threat event 36		
38	Disk error	HI	Can lead to threat event 36		

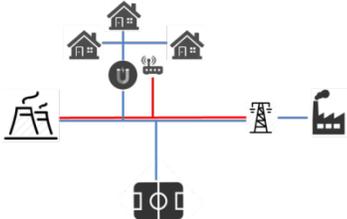
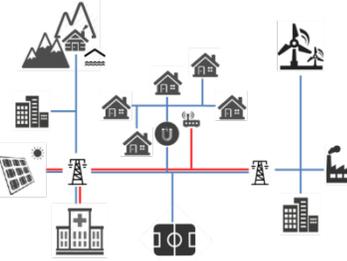
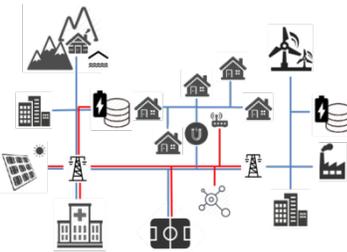
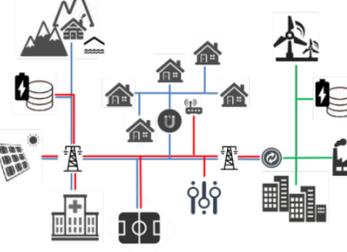
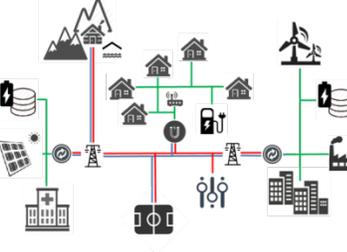
B SECOND APPENDIX. IRENE DISASTER SCENARIOS

B.1 DISASTER SCENARIOS BASED ON SOME PRE-SELECTED DISASTER EVENTS

Grid configuration	Disaster description	Likelihood
Disaster event 1: Bomb attack on key connection		
	<p style="text-align: center;">1. Initial Scenario</p> <p>The bombing hits the connection between PP and S during a sport event. This leaves the stadium without energy, leading to a disaster event due to the high concentration of people during sport events.</p>	Moderate
	<p style="text-align: center;">4. Adding key buildings</p> <p>Lot of critical buildings can be found here. The bombing hits the connections near the hospital, that needs continuous providing of energy</p>	High
	<p style="text-align: center;">5. Inserting Storages</p> <p>The data center introduces advanced balancing and energy providing techniques, that could fail when a DC near the block (e.g., the one that leads to F, O, DES, WF) is damaged. This is damaged by the bombing. The outcome is a strategy that is not able to provide the right energy to the right buildings due to missing data coming from other components.</p>	High
	<p style="text-align: center;">8. Insertion of SCADA System</p> <p>The BDC is replaced by a full SCADA system, which improves all the already implemented advanced techniques. The bombing damages the DC, this is still a problem that is not resolved by the adoption of SCADA instead of a rougher BDC.</p>	Very High
	<p style="text-align: center;">10. Improving decarbonisation</p> <p>In the final scenario we have lots of critical buildings that needs of continuous providing of energy. The bombing hits the ECs that conduct electricity. This results in leaving the building without energy with different huge consequences.</p>	Very High

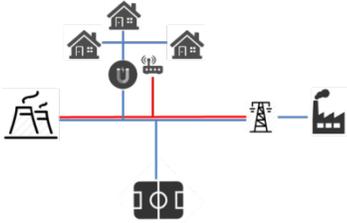
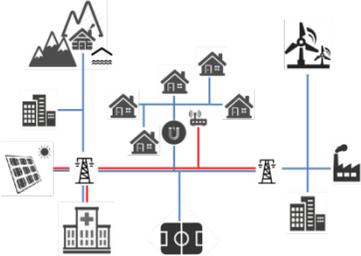
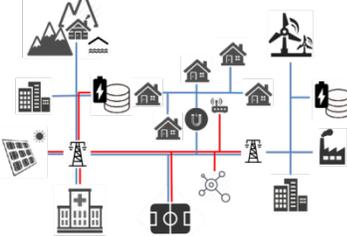
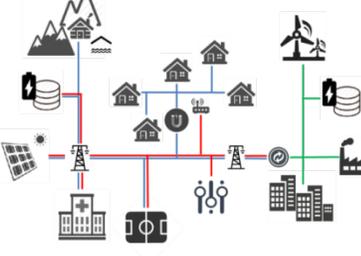
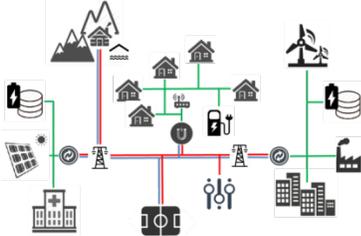


Disaster event 2: Compromisation of critical functionalities		
	<p>1. Initial Scenario</p> <p>Inserting subverted individuals into organizations leads to consequences that are directly linked to the relevance and the criticality of behaviours owned by the company. Here a subverted individual exploits the permissions and his role into the PP organization to trick the production of energy, leaving the city building without enough power.</p>	<p>Low</p>
	<p>4. Adding key buildings</p> <p>New buildings are added, so the subverted individual exploits his role to damage H functionalities (e.g., damaging the spare generator if any, or some internal data exchanges) or others (S, O ...).</p>	<p>Moderate</p>
	<p>5. Inserting Storages</p> <p>A subverted individual that works on the algorithm of BDC causes a disaster event that can target islanding, load balancing or DSR techniques implemented and provided by this component. Since the city uses lots of these techniques, compromising one of these software (e.g., slow down or inserting bugs) result in a wide variety of negative consequences.</p>	<p>Moderate</p>
	<p>8. Insertion of SCADA System</p> <p>SCADA have more techniques and mechanisms to optimize the city resilience and disaster response. Its manumission is very dangerous for the health of the grid and, consequently, of the citizens. The subverted individuals use some of the techniques listed for the BDC to compromise the behaviour of the controller.</p>	<p>High</p>
	<p>10. Improving decarbonisation</p> <p>Scenario's changes do not affect the disaster description.</p>	<p>High</p>

Disaster event 3: Compromisation of data		
	<p style="text-align: center;">1. Initial Scenario</p> <p>Data centres / SCADA systems are not present in this scenario</p>	-
	<p style="text-align: center;">4. Adding key buildings</p> <p>Data centres / SCADA systems are not present in this scenario</p>	-
	<p style="text-align: center;">5. Inserting Storages</p> <p>Data are compromised by a MiM attack, resulting in corrupted or missing packets, or in the replication of some chosen ones. When polluted data reach the BDC to be analysed and to contribute to the tuning of city resilience mechanisms, wrong information leads to crisis due to the wrong behaviour of DSR or load balancing techniques.</p>	High
	<p style="text-align: center;">8. Insertion of SCADA System</p> <p>The BDC is replaced with the SCADA, which has more power and more responsibilities. Given the same MIM attack, the result is that wrong decisions lead to more serious consequences compared to the ones described for the previous scenario.</p>	High
	<p style="text-align: center;">10. Improving decarbonisation</p> <p>Scenario's changes do not affect the disaster description.</p>	High



Disaster event 4: Earthquake on key building		
	<p>1. Initial Scenario</p> <p>When an earthquake heavily damages a key component of the grid, the consequences will last for a long time after the disaster. In this scenario, damaging the PP leaves the city without energy provider.</p>	<p>Very Low</p>
	<p>4. Adding key buildings</p> <p>Here the PP is substituted by a PV central and supported by a WF in the generation of energy for the city. An earthquake damaging this component softly impacts grid strategies. We have to consider that since no DESs are available, the WF might not be able to support all the city components when the PV is not working due to the earthquake.</p>	<p>Very Low</p>
	<p>5. Inserting Storages</p> <p>A DES support is inserted in the grid, resulting in a more resilient city context. The WF and the PV are damaged by the earthquake, and the DES compensates the absence of an energy provider using its power reserves (if the connections are still working).</p>	<p>Very Low</p>
	<p>8. Insertion of SCADA System</p> <p>Scenario's changes do not affect the disaster description.</p>	<p>Very Low</p>
	<p>10. Improving decarbonisation</p> <p>Scenario's changes do not affect the disaster description.</p>	<p>Very Low</p>

Disaster event 5: Theft of energy between components		
	<p>1. Initial Scenario CP and MG are not present in this scenario.</p>	-
	<p>4. Adding key buildings CP and MG are not present in this scenario.</p>	-
	<p>5. Inserting Storages CP and MG are not present in this scenario.</p>	-
	<p>8. Insertion of SCADA System CP is not present in this scenario.</p>	-
	<p>10. Improving decarbonisation Using a CP in which the privileges are not set correctly, the citizens ask for energy to charge their cars, stealing it from the near components (in the neighbourhood, most of them are SH). Concurrently, an adversary exploits this vulnerability to maliciously steal energy from the grid, leading to blackouts in the targeted grid parts.</p>	Low



Disaster event 6: Substation fire		
	<p>1. Initial Scenario The substation is a key component of the grid and needs to be replaced. If no alternative lines can be established to supply the area it is without electricity for several days.</p>	<p>Low</p>
	<p>4. Adding key buildings Few residential buildings can be supplied by the PV but as there is no redundant control equipment this is only possible for the buildings directly connected to the PV.</p>	<p>Low</p>
	<p>5. Inserting Storages Few residential buildings can be supplied by the PV and the storage backup. The decentralized control of PV and storage allows supplying several building including the hospital.</p>	<p>Low</p>
	<p>8. Insertion of SCADA System The SCADA system enables for advanced control of demand and supply. As control mechanisms are aware of the criticality of loads supply of most critical services can be assured.</p>	<p>Low</p>
	<p>10. Improving decarbonisation Charged EV batteries can be used as an additional power source in order to supply critical services.</p>	<p>Low</p>



B.2 DISASTER-RELEVANT CHARACTERISTICS OF POWER FACILITIES

Class Electric Power Facilities Feature Class: hzElectricPowerFlty¹² (belongs to UTIL.mdb). Provides the geometry of electric power facilities. During the creation of a study region, for all hazards, geometries are transferred to a geodatabase named UTIL.mdb in the Region folder. Field information is transferred to a table with the same name (hzElectricPowerFlty) in the SQL Server database in the Region folder. Data are subsequently used for Hazus-MH estimation of hazards, damages, and loss of functionality, as well as mapping.

Name	Description
ElectricPowerFltyId	Unique identifier for each record. It relates this hzElectricPowerFlty feature class with the associated eqElectricPowerFlty and flElectricPowerFlty tables. The standard format adopted by Hazus is SSxxxxxx, where SS is the state name abbreviation (upper case) and xxxxxx is a sequential number from 000001 to 999999.
UtilFcltyClass	Indicates the facility classification. It is used by Hazus-MH to identify the appropriate damage curve to assess loss estimations produced by the EQ Model.
Tract	2000 US Census tract number
Name	Facility name
Address	Physical address
City	City
Statea	USPS state abbreviation
Zipcode	Zip code; for instance, 30067 or 30067 – 2564 or 300672564
Owner	Facility owner name
Contact	Facility contact person
PhoneNumber	Facility contact phone number
Use	Use
YearBuilt	Year structure was built
NumStories	Number of stories
Capacity	Volts/Watts
Cost	Replacement cost (in thousands)
Latitude	Latitude
Longitude	Longitude
Comment	Comments

¹² (F.7.3.3) [64, pp. F-198]



B.3 DISASTER-RELEVANT CHARACTERISTICS OF CARE FACILITIES

F.5.3.3 Flood Specific Care Facilities Table: flCareFlty (belongs to EF.mdb). The table provides Flood Model specific information of hospitals and medical clinics. During the creation of a study region, the table content is transferred to another table with the same name (flCareFlty) in the SQL Server database in the Region folder. Data are subsequently used for Hazus-MH Flood Model estimation of hazards, damages, and loss of functionality. There must be one record in flCareFlty for each record in hzCareFlty with same CareFltyId unique identifier.

Name	Description
CareFltyId	Unique identifier for each record. It relates this flCareFlty feature class with the associated hzCareFlty in a one-to-one relationship. The standard format adopted by Hazus is SSxxxxxxx, where SS is the State name abbreviation (upper case) and xxxxxx is a sequential number from 000001 to 999999.
BldgType	General building type: Null, Masonry, Concrete, Wood, Steel, ManufHousing
DesignLevel	Design level (Pre/Post FIRM): Null, 0 = Pre-FIRM, 1 = Post-FIRM
FoundationType	Foundation type (e.g., slab, pile): Null, 1 = Basement, 2 = Crawl, 3 = Fill, 4 = Pier, 5 = Pile, 6 = Slab, 7 = SolidWall
FirstFloorHt	First floor height
BldgDamageFnId	Default building damage function id
ContDamageFnId	Default content damage function id
FloodProtectIon	Flood protection return period