Towards a Collaborative Framework to Improve Urban Grid Resilience

Oliver Jung
Sandford Bessler
AIT Austrian Institute of Technology

Alexandr Vasenev
Lorena Montoya
University of Twente

Andrea Ceccarelli
Tommaso Zoppi
University of Firenze

Tony Clarke
Keith Chappell
Ethos VO

***Abstract*— Two trends will help to ensure resilient electricity supply in Smart Cities: a) the ongoing deployment of Smart Grid technology and b) the adoption of distributed energy resources. Unfortunately, the increased reliance on ICT in the Smart Grid will expose new threats that could result in incidents that might affect urban electricity distribution networks by causing power outages. Diverse specialists will need to cooperate to address these threats. This position paper outlines a methodology for establishing a collaborative framework that supports the definition of response strategies to threats. We consider the ongoing evolution of the electricity grids and the threats emerging while the grid evolves. After outlining possible scenarios of urban grid development, we highlight several threats and the strategies of attackers. Finally, we introduce a framework that aims to foster the collaboration of stakeholders involved in city resilience planning taking into account grid vulnerability and criticality from a city's perspective.**

I. INTRODUCTION

Urban Smart Grids offer the possibility to improve grid resilience through the ability to integrate Distributed Energy Resources (DER) like photovoltaic generation (PV) or Combined Heat and Power (CHP) plants [1]. The introduction of demand response approaches and Distribution Automation, provide a wide set of options to Distribution Network Operators (DNO) to reconfigure the grid in case of faults. These benefits come with the price of introduction of IT solutions, which might lead to grid reliability degradation. Resilience is the ability of a system to mitigate and rapidly recover from a disruptive event [1]. However, in this paper we are focusing the degraded state of the grid considering grid islands as a measure for mitigating outage impacts and improving resilience.

In order to improve the resilience of cities against grid malfunctioning, all stakeholders such as city planners, DNOs, and critical infrastructure operators have to cooperate in a meaningful way. DNOs alone can hardly perform this task as additional investments into the infrastructure will not necessarily result in generating revenues. Therefore, DNOs can only together with other stakeholders leverage Smart Grid technology to set up specific grid islands or microgrids to power city elements, even though power from the central utility is no longer available.

Because it is not possible to set up islanding everywhere in the grid due to the lack of money, city stakeholders have to face several challenges on the way to improve city resilience: the stakeholders need to decide which parts of the grid are a) most vulnerable to attacks and b) most critical from a societal, economical, or functional point of view.

A possible way adopted in this paper, is to consider an asset/impact-oriented approach to account what threats can degrade city infrastructures. Looking at a threat landscape in connection to a grid topology and applying risk assessment lenses appears to be a natural choice in this case.

The Collaborative Framework aims to provide the stakeholders with the means to establish the roles, governance mechanisms (decision-making) and policies needed for an effective resilience planning capability. The framework can assist in identifying relevant stakeholder groups, threat and attacker data, vulnerability assessments and analysis methods. Consequently, the structure of roles for prevention and reduction for specific urban grid disaster scenarios can be assigned, guidelines and policies can be outlined and the requirements of a tool for facilitating this process can be drawn.

This paper outlines a structured approach for establishing a collaborative framework that can support the development and deployment of responses to both the physical and cyber-threats an electricity grid will be exposed to as it evolves. It illuminates required components by providing illustrations how to interrelate a grid topology and threats and how to conduct threat analysis. Both add to the framework and help to identify the stakeholders that have to contribute to a coordinated response. The main contributions are the approach for identifying relevant stakeholders based on the considered threats and the decision support for identifying the parts of the grid where islanding should be deployed.

This work was partially supported by the JPI Urban Europe initiative through the IRENE project.

978-1-4673-8463-6/16/$31.00 ©2016 IEEE

The rest of the paper is organized as follows: section III illustrates how threats "Compromise Critical Functionality" and "Substation Fire" can cripple the city. Section IV further elaborates on threat analysis. It demonstrates how cyberattacks as a specific threat can be broken down into consequent threats. Section V introduces the collaborative framework before Section VI finally summarizes and concludes the paper.

II. RELATED WORK

A. Risk Assessment

Although Smart Grids are still rarely deployed, there is a growing awareness of the security threats and risks that arise with their advent. In order to tackle these risks, cities and their stakeholders do not only have to take appropriate actions to protect their infrastructure but also have to make the infrastructure more resilient by preparing attack and disaster response strategies [1].

Several approaches for threat assessment of Smart Grid can be found in the literature. For example, in [5], [7], and [8] a risk assessment process is applied to investigate the analysis of security threats to the Smart Grid, smart meters or power grids.

Standards for risk assessment exist for generic domains e.g., NIST 800-30 [6]. However currently no standard methodologies for conducting cyber risk assessment of Smart Grids or energy control systems are available, despite the fact that IEC and NIST recently published a Roadmap [3], respectively a Guideline document [4].

B. Collaborative Frameworks

When improving city resilience, the collaboration of stakeholders is vital. Their involvement is needed in order to get a good understanding of the infrastructure, its vulnerability and the interdependencies between infrastructures. It is without doubt that the electricity grid is the most important one. Guidelines for the collaboration between stakeholders in crises have been developed by several organizations.

The Federal Emergency Management Agency (FEMA) [10] proposes the so called whole community approach for enhancing the resilience and security for communities in the United States. The main aim of this concept is to bring together people that need to be involved in emergency planning. However, it also helps evaluate their needs, find the stakeholders, get them engaged and raise awareness.

The German Federal Office of Civil Protection and Disaster Assistance analyzed the impacts of power outages, lasting for more than 24 hours. The guideline describes for different critical infrastructures the timeline of parts failing. It gives a list of stakeholders and emphasizes the importance of public private partnerships (PPP) in disaster response [11], which requires the involvement of infrastructure operators, civil protection authorities, and media.

To our knowledge there is no collaboration approach that brings together the threat identification and risk assessment with the collaboration of stakeholder. This paper defines the process from the identification of Smart Gird disaster scenarios over the risk assessment to the collaboration of relevant stakeholders.

III. DISASTER EVENTS AND RELATED USE CASES

We identify use cases that describe two energy-related disaster event-types that could occur in Smart Cities. The definition of three exemplary use cases constitutes the first step of our approach to set up a collaborative framework. In this section, we present i) the Smart City scenarios, ii) two selected disaster event-types occurring in the Smart City scenarios and the threats causing such disaster events, and iii) the exploitation and effect of such threats for each selected scenario.

Three Smart City scenarios were identified with the aim to represent the possible evolution of a city, starting from the low-smart setting towards the high-smart setting. The three scenarios are shown in the first two columns of Table I, where they are described both graphically and textually. Starting from a Smart City with a limited number of smart features, new features are added in the successive two scenarios.

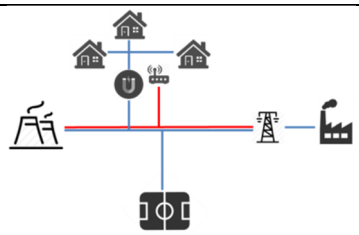
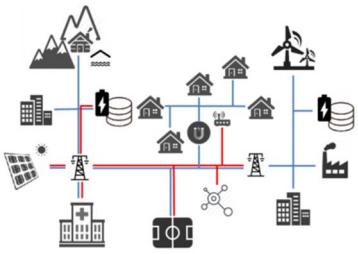
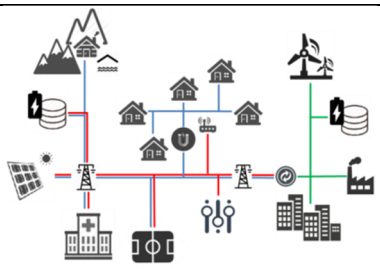
A disaster event is the multiple, severe or catastrophic effect of a threat on organizational operations, assets, individuals, other organizations, or on the Nation [14]. We identify two disaster events: i) compromise critical functionalities of the Smart Grid, and ii) a fire accident in a substation. As reported in Table I the first disaster event is due to an adversarial threat (ADV), while the second is due to a non-adversarial threat (NA). Different components of the Smart Grid are involved, and the potential chain of events in case of cascading effects is described.

It should be underlined that we based the identification of such disaster events on the results of a threat analysis that was carried out on the identified scenarios. The whole analysis is reported in [13]. In the analysis we applied 102 threat events from the NIST standard [6] to the various components and connections of several city scenarios, amongst which we selected the three reported here. Amongst all the resulting disaster events that were identified, we selected two in Table I.

The two threats reported in Table I are next discussed in light of the three different scenarios. In fact, such threats may lead to different effects and may have a different likelihood depending on the scenario considered.

For example, a city ranked as *high smart* may suffer significantly from subverted individuals that change configurations; instead, these configurations may not even exist in a city ranked *low smart*.

TABLE I. GRID SCENARIOS

Scenario Representation	Scenario description	Disaster event: Compromise Critical Functionality	Disaster event: Substation Fire
	Initial "low-smart" scenario: Setting: a power plant, a factory, a simple residential complex and a stadium. The data connection exists between several buildings but it is not relevant due to the absence of a controller.	Inserting subverted individuals into building's organization leads to consequences that are directly linked to the relevance and the criticality of building. A subverted individual in a power plant exploits his access privileges and his role to reduce the production of energy. Thus, the city will have less energy at disposal. *Likelihood: low*	The substation is a key component of the grid and in case of fire it needs to be replaced. If no alternative lines can be established to supply the area, it will cause a blackout for several days. *Likelihood: low*
	The city administration follows the social needs as for example the requirement of complete de-carboni-sation or that of building a new hospital .Two **data and energy storages** are introduced to start exploiting smart functionalities. A data control center is installed to provide simple Demand-Side Response (DSR) and load balancing strategies.	A subverted individual (insider attacker) which has the privileges to operate the algorithms of data control center compromises islanding, load balancing or DSR techniques. Since the energy network relies on such techniques, compromising one of them (e.g., slowing down or inserting bugs in the software) exposes the grid to potential failures. *Likelihood: moderate*	Few residential buildings can be supplied by the photo voltaic (PV) and the storage backup. The decentralized control of PV and storage allows supplying several building including the hospital. *Likelihood: low*
	"High-smart" scenario: The Data Control Center is replaced with a 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.	SCADA systems have additional techniques and mechanisms to optimize the city resilience and disaster response. Its manumission is can alter the status of the grid and, consequently, it is dangerous for the city. The subverted individuals may alter the algorithms mentioned above to compromise the behavior of the controller. *Likelihood: high*	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. *Likelihood: low*

electricity connection: ——— data connection: ——— micro-grid connection: ———

We proceed as follows. First, we identify assumptions that describe the grid and its context. The key assumptions for the three scenarios are:

- We make an assumption on the political and geographical location of the city: *the city has an important strategic relevance and is consequently exposed to terrorism*.
- We introduce an assumption on the exposure of the grid, ease of exploitation, relevant security control, severity of impacts and compensating controls in place: *due to the terrorism risk, the permissions and the policies for the utilization of resources are strict, in order to mitigate possible malicious actions*.

These assumptions allow us to decide on the occurrence likelihood of the disaster events under investigation. Correspondingly, the likelihood of compromise critical functionalities is rated low in the first scenario, moderate in the second and high in the third, as the number of exposed components increases. For the substation fire, the likelihood is always set to low in the three scenarios.

This likelihood ranking comes from the NIST structure [14] for the factors related to vulnerability severities. We acknowledge the inherent complexity of the risk assessment task, especially evident if future grid solutions should be considered. At the same time we aim to provide guidelines that can help to mitigate or plan disaster events particularly related to Smart Grids. It should be noted that within the factors derived from NIST, the scope of this paper is focused mostly on likelihood. We leave aside the factors related to the ease of the vulnerability exploitation, and security controls, whose characteristics are included in the list of assumptions reported above. Severity of impact is dealt with in the criticality assessment (Section IV).

IV. EXPERTISE TO UNDERSTAND CYBER-THREATS

A better understanding of how future cyber-threats can manifest is essential to anticipate potential risks for Smart Cities. The high amount of future threats requires a method for identifying specific threats. Such a process would answer the following questions: (1) what expertise is required (i.e., which experts

should be involved in the threat analysis), and (2) how the relevant experts can analyze and prioritize threats in a repeatable and sound manner.

This subsection outlines which experts are needed to assess threats relevant for particular grid components. We illustrate how a threat list for city grids, derived from 102 NIST threats, can guide considerations regarding threats relevant to specific city components. The city distribution infrastructure layout allows to further concentrate on specific grid assets.

A. Search for expertise required for threat analysis

Concentrating on specific threats requires involving specialists that can adequately assess threats relevant to the city under consideration. As the city might possess location-specific characteristics (e.g. a dam is nearby) or other properties (e.g. advanced production facilities are situated within the city), outlining an initial list of threats is useful.

A threat taxonomy (see e.g. Figure 1) constructed for a city-specific case can aid the process of producing such list of threats. The taxonomy might embody two components. First, it can take a structure of general threats. Second, it populates the generalized categories with examples of threat events. Figure 1 illustrates this by merging a top-level NIST taxonomy populated with exemplary threats, shown in italic.

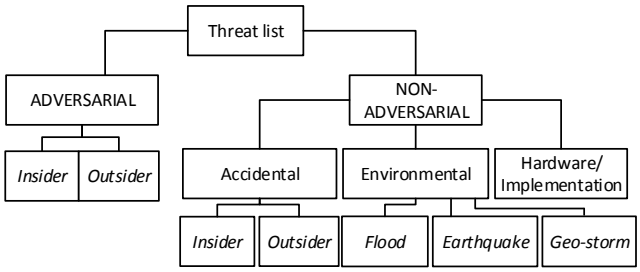


Figure 1. An illustrative threat taxonomy

By populating the overall taxonomy with threat events (given the city assumptions described in the previous section), it is possible to identify which expertise would be required for future threat analysis.

Once the needed expertise and domain experts are identified, the process by which experts prioritize threats within their taxonomy element has to be developed. The next section illustrates how experts can follow an "Adversarial-Outsider" threat category from the taxonomy.

B. An approach to analyse cyber threats using kill chains

We concentrate on external malicious threats to complement the examples from Section II with a cyber-attack scenario. We adopt suggestions proposed for Smart Grids in "Best practices in identifying threats" [15]. Specifically, we take into account different classes of attackers (BP-RA6) and relate each class to possible targets (BP-RA7). By demonstrating how threats can be analyzed, we illustrate the expertise requirements of the framework.

Kill chains are commonly used to describe the diversity of cyber threats that are part of the threat landscape. It is widely acknowledged that they can help to structurally describe attack steps and identify countermeasures. Several kill chains are described in the literature:

- Lockheed Martin Intrusion Kill Chain [16] differentiates between the following attack steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C2, Actions;
- Mandiant's attack lifecycle [17] considers Initial Recon, Initial Compromise, Establish Foothold, followed by a loop of four steps (Escalate Privileges, Internal Recon, Move Laterally, and Maintain Presence), and Complete mission;
- NIST SP 800-115's [18] attack example consists of Discovery phase (supported by information from System Browsing within the Attack Phase) and the Attack Phase. The latter constitutes four steps (Gaining Access, Escalating Privileges, System Browsing, and Install Additional Tools). The last step of the Attack Phase also fuels the first one (Gaining Access);

Dell Secureworks [18] inter-relates three threat sources (Commodity Threats, Advanced Persistent Threat, and Hacktivism) and twelve attack steps. The attack steps are: Define Target, Find and organize accomplices, Build or acquire tools, Research target infrastructure/employees, Test for detection, Deployment, Initial intrusion, Outbound connection initiated, Expand access and obtain credentials, Strengthen foothold, Exfiltrate data, and Cover tracks and remain undetected.

Designated experts can choose from such kill chains to prioritize the cyber threats under consideration. Clearly, adopting or re-defining a specific kill chain as a guiding principle for structuring cyber-threats can be also a context-specific task. In the rest of the section we illustrate how kill chains can assist experts to approach cyber threats in a structured manner. Noticeably, this description does not impose this structure as a requirement for the framework, but merely provides a suggestion on how experts can guide their analysis process.

Due to our intention to build the threat analysis on the basis of NIST 800-30, we derived several adversarial threat categories from this document. These categories include:

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

Arranged as consequent steps, where each one is related to 'Coordinate a campaign' category, this kill chain can be graphically represented as shown in Figure 2. This kill chain is relevant for each city component and thus provides a first step in relating cyber threats to grid components. Elaborating this generic kill chains would be the second step in this task.

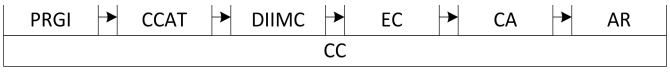


Figure 2. Structured cyberthreats

The experts can adopt the BP-RA6 recommendation mentioned earlier for performing further analysis. For instance, for group attackers into three classes, such as: commodity threats (class C1), targeted threats (C2), and Advanced Persistent Threat (APT, C3). The classes can be characterized based on their focus (i.e. their targeting and intent") and capabilities. The concepts of "Targeting", "Intent", and "Capabilities" outline characteristics described in NIST 800-30 and are well aligned with the FAIR taxonomy's concept of threat event frequencies [20]. These attacker behavior characteristics have also been identified as important by rational choice argumentation approaches. The characteristics are therefore readily extendable into dimensions of comprehensive risk analysis and account for attacker motivation.

The characteristics of the three classes of malicious external threat sources can be therefore described as follows:

C1 class: Commodity class corresponds to opportunistic sources. This class can be described as having low focus (targeting and intent) and capabilities;

C2 class: targeted threats that possess additional focus as a threat source characteristic;

C3 class: APT class that in addition to targeting and intent possess advanced capabilities.

Since attackers have different capabilities, they can have class-specific kill chains. The capabilities of threat sources therefore describe threat sequences relevant to these sources.

Besides differences in their kill chains, threat sources can also have different foci. In their analysis, the experts can relate this characteristic to specific city grid components. For instance, the attractiveness or value of an asset for an attacker within a specific class can be considered. This consideration may additionally account for a plausible attacker's motivation. Noticeably, these tasks, as well other steps of threat analysis may require involving additional experts in the analysis process. The outcome of this analysis is a list of threats to be considered during the subsequent risk analysis.

Clearly, the way in which the experts can construct and manage a list of threats, as well as the later use of this list, can be facilitated by a specialized decision-support tool. The same tool could model how this threat, can impact the city.

To summarize, this section first outlined how to establish which expertise is relevant for considering threats for a specific grid. As the diversity of the taxonomy element shows, threat analysis of the city Smart Grid might require input from different expert domains. Once the scope of analysis is identified, the experts might need to concentrate on a repeatable and sound methodology to assess threats. For illustrative purposes, we showed how experts can analyze external malicious threat events.

V. COLLABORATIVE FRAMEWORK

The previous sections explored the themes and approaches for understanding the future grid and the emerging threats. To make effective use of these insights, in a real urban setting, we propose a "collaborative framework" that will facilitate city planners engage relevant stakeholders in the decision making processes that will aim to enhance grid resilience. Moreover, the framework provides means to understand the need of how electricity contributes to city-critical societal functions.

An effective framework will need several key components: (1) a decision support tool to understand current resilience and the impact of possible changes, (2) guidelines on "Planning Group(s)" i.e. those planning organizations that will be used to bring together key stakeholders to carry out and coordinate the city's resilience planning activities, (3) the policies that will guide the Planning Groups(s) in their decision making, clarifying the scope of their authority and responsibilities, and (4) risk assessment to be able to prioritise areas where mitigation measures should be deployed.

The later takes into account the vulnerability of a specific part of the grid depending on deployed technology, degree of exposure to threats and the level of criticality of connected infrastructure. A simple rating of vulnerability, threat likelihood and criticality as high, moderate, low, and summing them up provides a metric for assessing the risk. Naturally, resilience or response mechanisms need to be deployed first in areas with a high vulnerability, high threat likelihood and high criticality, which can be assessed by rating the dependency and influence of infrastructures [21].

The Resilience Evaluation tool will form the core of the Collaborative Framework and will provide the means to model the current grid resilience in such a way that the impact of possible changes can be understood. This will allow planners to gather inputs in a consistent manner from selected grid elements that relate to a demand, a source or both (including storage). These elements will be associated with individual nodes and interconnections between nodes (typically cables). The tool will then aggregate inputs with specific nodal constraints to allow nodal and internal processing by the tool.

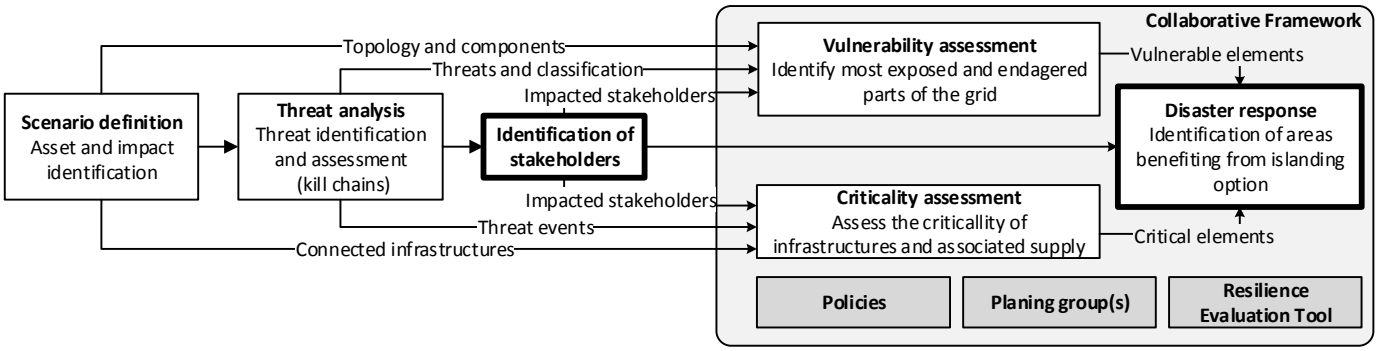


Figure 3: Collaboration Framework

The results will be presented on a per node basis, depending on a number of engineering and human factors. These factors include, but are to limited to, demand, supply, criticality, load profile (summer and winter), availability (Mean Time Between Failure), reliability, maintainability, maintenance history, spares/skills availability (Mean Time To Repair), specific local vulnerabilities (flood, blast, EMC) and specific local mitigation measures (elevation, fencing, etc). This would allow infrastructure planners to safely explore different network configurations in order to optimise resilience.

VI. Summary and Outlook

This paper outlined a methodology for establishing a collaborative framework that can support the definition of responses to both physical and cyber-threats to urban electricity grids. This methodology will also enable stakeholders to apply a threat analysis, while providing opportunities to connect threat analysis to other fields, such as the criticality analysis and the vulnerability analysis.

Defined grid scenarios and derived threat events help to constitute Planning Groups and identify needed participants (e.g. city planners, DNOs, key infrastructure owners, critical service delivery organisations, etc.) and provide the basis for their engagement (captured as policy). With a resilience evaluation tool in place we will be in a position to evaluate the effectiveness of responses, e.g. grid islanding.

Key aspects for selecting areas to be equipped with grid islanding solutions are the criticality and the vulnerability of an area. With acquiring a more detailed information about the electricity grid and connected infrastructures in future a quantitative analysis would provide a more solid evidence for taking this decisions.

References

[1] M. Panteli and P. Mancarella, "The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience," in IEEE Power and Energy Magazine, vol. 13, no. 3, pp. 58-66, May-June 2015.

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

[3] SMB Smart Grid Strategic Group SG3, "IEC Smart Grid Standardization RoadMap", Ed 1.0, June 2010

[4] NIST, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," Sep 2010.

[5] Farzan, Farnaz, et al., "Cyber-related risk assessment and critical asset identification in power grids," Innovative Smart Grid Technologies Conference (ISGT), 2014 IEEE PES. IEEE, 2014.

[6] NIST 800-30 risk management guide for information technology systems, 2002.

[7] Kharchenko, Vyacheslav, Eugene Brezhnev, and Artem Boyarchuk, "The smart grid's safety: Dynamical hierarchical criticality matrices-based analysis," Innovative Smart Grid Technologies (ISGT Europe), 2nd IEEE PES International Conference and Exhibition on. IEEE, 2011.

[8] Habash, Riadh WY, et al., "A risk assessment framework for the smart grid."Electrical Power & Energy Conference (EPEC), 2013 IEEE.

[9] Bouchon, Sara, and Carmelo Di Mauro, "Resilience? Insights into the role of Critical Infrastructures Disaster Mitigation Strategies." TeMA Journal of Land Use, Mobility and Environment 5.3 (2012): 103-117.

[10] Federal Emergency Management Agency, "A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action," 2011.

[11] Hiete, M., et al. "Krisenmanagement Stromausfall. Krisenmanagement bei einer großflächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg." 2010.

[12] Institute for Public Policy Research,"A New Approach To Electricity Markets, How New, Disruptive Technologies Change Everything," 2014

[13] IRENE project, "IRENE D2.1: Threats identification and ranking," 2015. [Online]. Available: http://www.ireneproject.eu

[14] CEN/CENELEC/ETSI Smart Grid Coordination Group, "Smart Grid Reference Architecture," 2012

[15] Soes, "Deliverable 4. ICT Security in Energy Smart Grids Best Practices," 2014.

[16] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences, 2011, pp. 113–125.

[17] Mandiant, "APT1Exposing One of China's Cyber Espionage Units." [Online]. Available: http://intelreport.mandiant.com/

[18] Stouffer, Keith, Joe Falco, and Karen Scarfone. "NIST SP 800-115: Technical Guide to Information Security Testing and Assessment." National Institute of Standards and Technology (2008).

[19] Dell secureWorks, "Advanced Persistent Threats Analysis." [Online]. Available: http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threat/understand-the-threat/t

[20] The Open Group, "Risk Taxonomy, Technical Standard." [Online]. Available: http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf

[21] Laugé, Ana, Josune Hernantes, and Jose M. Sarriegi. "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach." International Journal of Critical Infrastructure Protection 8 (2015): 16-23.