Analysing Non-Malicious Threats to Urban Smart Grids by Interrelating Threats and Threat Taxonomies

Alexandr Vasenev, Lorena Montoya
Services, Cybersecurity and Safety research group,
Faculty of EEMCS, University of Twente
Enschede, The Netherlands
{a.vasenev; a.l.montoya}@utwente.nl

A comprehensive study of the smart grid threat landscape is important for designing resilient urban grids of the future. To this end, an analysis could first cross reference threat categorizations and interrelate treat events on the basis of threat lists that complement each other. This paper show how to cross-relate threat taxonomies and analyze relations between threats and system components to reasonably link diverse threats to a smart grid. We illustrate how one can look beyond a specific threat by (1) relating threat sources from one taxonomy to threat lists from other taxonomies; (2) analyzing how threats can be cross-related to identify possible scenarios of undesirable events; and (3) assigning threat categories to system components. These steps in sequence or individually aim to provide input to threat identification and (thus) risk assessment tasks. This paper focusses on threats listed in the IRENE research project and relates them to threat taxonomies used in the AFTER and SESAME projects which focused on smart grids as well.

Smart grid; electricity; critical infrastructure; threat; taxonomy

I. INTRODUCTION

Complex systems, such as urban grids, are exposed to numerous threats that can interrupt service delivery to customers. In electrical systems, it relates to power outages.

Power outages (blackouts) are experienced everywhere in the world. An OECD (Organization for Economic Co-operation and Development) country, for instance, experiences on average 4 outages during a ten month period. Each blackout lasts about 2.9 hours [1]. Outside the OECD outages occur more often and last longer. For example, a country from East Asia & Pacific experiences about 4.4 outages per month (average duration of 6.4 hours). A Middle East & North Africa country – 17.6 (9.7 hours), while a South Asian country about 25.4 (5.3 hours). Given that in the US the five-year annual average of outages doubled every five years between 2000 and 2013 [2], one can expect that the amount of outages around the world might further increase.

To ensure continuity of electricity supply – often critical to business operations and services –threats to current and future grids should be considered carefully. However, while the increasing use of information technologies can improve grid resiliency, it also increases the grid exposure to new threats. An accident in a smart grid IT layer can 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" [3]. Thus, considering grid threats holistically is an important task and it might be a part of a collaborative effort to ensure improved resilience of urban electric grids [4].

An analyst constructing a list of grid-related threats for future risk assessment faces a daunting task. Its complexity is due to the interlinked nature of electrical and IT networks, diversity of contexts in which the grid operates, the role of timely control, maintenance, and many other factors.

One way to account for diverse threats could involve employing well-developed constructs from the field of dependability and secure computing (e.g. [10]) For instance, work on threat taxonomy extension (originally focusing on computer systems) to outline challenges in networking systems is described in [11]. Another approach would involve interrelating and analyzing threats listed in taxonomies which specifically focus on electricity grids. This paper provides an initial vision for moving forward using the second type of approach. We link taxonomies and explore a threat landscape of a complex system, i.e., a smart grid. We don't aim to neither complete nor exhaustively cover all possible relations between threats to smart grids. Also, we don't elaborate on the strength of such connections. Instead, we provide a scheme to: relate threats by considering threat sources of different threat taxonomies, analyze threat to threat links within a single taxonomy, and associate threat categories to groups of system components. Instantiations of the scheme for a specific system should be made by specialists familiar with system specifics.

This paper illustrates how lists of different non-malicious threats to the grid can be cross-related. The next section describes threats taxonomies employed within three research projects. We then analyze how the taxonomies can be cross-related. Next, we illustrate how non-malicious threats can be cross-related and linked to system components, describe root cause analysis of threats, and discuss the conducted analysis.

II. BACKGROUND: EXISTING TAXONOMIES

This section outlines electric grid threat taxonomies from the AFTER, SESAME, and IRENE research projects. While the AFTER taxonomy (http://www.after-project.eu/) explicitly

This work was partially supported by the Joint Program Initiative (JPI) Urban Europe via the IRENE project.

978-1-5090-1846-8/16/$31.00 ©2016 IEEE

differentiates between physical and cyber-threats to the grid, SESAME [5] elaborated threats relevant to natural disasters. IRENE [6], as it stems from an information security standard (NIST 800-300), concentrates on cyber-threats and differentiates between adversarial and non-adversarial threats.

A. AFTER Taxonomy

EU FP7 project "A framework for electrical power systems vulnerability identification, defense and restoration" (AFTER) categorized threats by differentiating between cyber- and physical- grid layers. Stemming from the partitioning between adversarial and non-adversarial threats, AFTER looks at external or internal threats as follows (below threat groups are encoded using bold font):

- **Phys**ical:
  - **Nat**ural: **Ext**ernal (Lightings, fires, ice/snow storm, solar storms); **Int**ernal (Component faults, strained operating conditions);
  - **Man** related: External (Unintentional damage by operating a crane, sabotage, terrorism, outsider errors); **Int**ernal (Employee errors, malicious actions by unfaithful employees);
- **ICT** threats:
  - **Nat**ural: **Ext**ernal (Ice and snow, heavy flood, fire and high temperature, geomagnetic storm); **Int**ernal (Out of range, internal faults, ageing);
  - **Man** related: **Ext**ernal (Hacker, sabotage, malicious outsider); **Int**ernal (Employee errors, malicious actions by employees, software bugs).

While AFTER separates physical and IT threats, it is rather broad and has little consideration for their specifics, hence further structuring of threats for smart grids can be beneficial.

B. SESAME Taxonomy

EU FP7 SESAME project ("Securing the European Electricity Supply Against Malicious and Accidental Threats") provided a more extensive taxonomy of threats:

- **Nat**ural disasters:
  - Geological disasters (avalanches, earth-quakes, volcanic eruptions, landslides);
  - Hydrological disasters (floods, limnic eruptions, tsunamis);
  - Meteorological disasters (blizzards, cyclonic storms, droughts, hailstorms, heat waves, tornadoes, lighting, thunder, rainstorm);
  - Fires (wild fires);
  - Health disasters (epidemics, famines);
  - Space disasters (impact vents, solar flares, gamma ray burst);
  - Contamination.
- **Acc**idental threats:
  - Operational faults (design error, wrong decision, maintenance accident);
  - Equipment failures (technical failure, human and animal interference).
- **Mal**icious threats:
  - Physical threats (terrorists, war, sabotage);
  - Human threats (insider threats);
  - Cyber-threats (malware, terrorist hacking).

In addition to the taxonomy, SESAME [5] accounts for sequences of threats and distinguishes between 4 outage stages: pre-condition, origin, chain of events and end. It outlines different aspects of threats, events, effect, and phenomena developed. A chain of events, encoded using abbreviations of threats, can be used to describe grid failures.

In SESAME threats can also be related to grid parts, e.g.:

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

SESAME's classification therefore covers a threat landscape in great detail. However, although it can clearly help to structurally approach threat analysis, the accent of malicious threats to the IT level of the grid is less considered. Potentially, IT threats can be additionally considered by cross-relating them and linking such threats to grid components.

C. IRENE Taxonony

IRENE threat categorization is based on NIST 800-30 and inherits its taxonomy. The following is the structure of threat sources:

- **Adv**ersarial, such as an individual, outsider, insider, trusted insider, privileged insider, competitor, supplier, partner, customer, nation state;
- Non-Adversarial:
  - Accidental (**ACC**), e.g., mistakes made by a user or privileged user/administrator.
  - Environmental (**ENV**), including natural or man-made disaster e.g., sunspots, flood, earthquake, bombing, overrun, telecommunications infra-structure failure/outage.
  - Hardware or Implementation (**HI**) - failures of equipment (including IT, storage, processing, communications, display, sensor, controller, environmental & temperature/humidity controls, power supply), environmental controls, or software (operating system, networking, general- and mission-specific applications) due to aging, resource depletion, etc.

IRENE has its accent on IT security. Thus, relating threat sources from one taxonomy to threats from another one can provide more complete threat landscape.

III. Analysing Threats

A. Interrelating Taxonomies

Relating taxonomies can help an analyst to make lists of threats to smart grids that adequately cover the threat landscape. A possible mapping between these taxonomies is shown in Fig. 1. Interrelations of taxonomies highlight their differences and opportunities for adjustments. Sesame.ACC threats can be linked to different IRENE threat sources (Accidental and Hardware and Implementation). The same

applies to After.ICT.Man.Int threats. After.Phys threats can be seen as a subgroup of After.ICT threats if viewed in relation to the IRENE taxonomy. This points out that the IRENE grouping logic differs from that of SESAME or AFTER.

A threat assessment expert can choose whether to group several threats. For instance, she can consider jointly IRENE environmental threat events and the SESAME's detailed natural disaster list. Similarly, as the IRENE list could account for different threat origins to a smart grid as a cyber-physical system, it can be useful to think about its relation to the AFTER categorization. This can be useful if threats to the IT infrastructure, electrical network, or the control system of the grid are within the focus of attention.

B. Interrelating Threats

Cross-relating threats can be useful for considering threats in connection to a specific threat source in a structured manner. It can help analyze disaster events in hindsight by constructing chains of threats and describing precursors to an outage, as in SESAME. It can also help anticipate plausible disaster scenarios and controls needed for individual threats or threat groups. Structures such as attack trees in terms of AND-gates (see [7] for a short introduction) can support such analyses.

Non-malicious threats and their relations can be analyzed based on the IRENE threat list as shown in Table 1. The analysis of malicious threats differs from that of non-malicious ones due to the adaptive and intelligent nature of adversaries. This subsection analyzed IRENE non-malicious threats, complementing the analysis of malicious threats (e.g., IRENE.ADV threats 1–28, SESAME.MAL, and After.ICT.Man.Ext) described in [8].

IRENE ACC threats 29 – 31 are accidental and thus have no precursors, involve handling information by authorized users, and are not the result of malicious actions. However, these threats can lead to undesirable complex contingencies. Spill of sensitive information (threat 29) about grid configuration, as well as impacts of threat 30 can assist reconnaissance (e.g., open source intelligence) of malicious actors. Incorrect privilege settings (31) can allow malicious actors to achieve their objectives (e.g., cause adverse impacts, steal data) significantly easier.

Environmental threats 32 – 35 are divided into two groups to account for resilience: external threats (threats 32, 34, and 35) and threats both internal and external (33). External threat events can be interlinked and can cause internal threats, while the opposite is hardly possible. Earthquakes and hurricanes are independent external individual events. Flood at a primary or backup facility can be caused by a hurricane, but can also be an individual threat event. Hardware and implementation (HI) threat 37 (Introduction of vulnerabilities into software) or 38 (Disk error) can lead to 36 (Resource depletion).

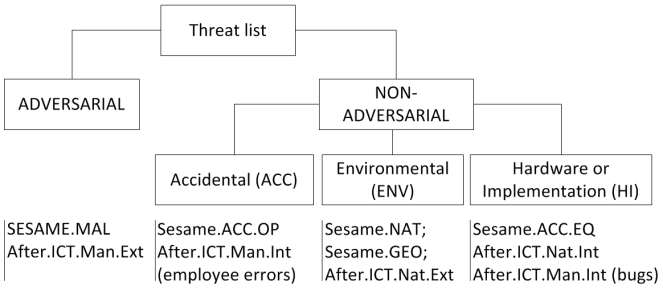

Fig. 1. Relating IRENE threat sources to threat lists from SESAME and AFTER projects.

TABLE I. IRENE THREATS AND THEIR DEPENDENCIES

Threat index	Threat event	IRENE[a] Category	Dependency
29	Spill sensitive information	ACC	Can be precursor to reconnaissance-related threats
30	Mishandling of critical and/or sensitive information by authorized users	ACC	Similarly to 29, it can lead to recon-related
31	Incorrect privilege settings	ACC	Incorrect privilege settings can directly lead to multiple other threat events, including 23 – 25
32	Earthquake at primary facility	ENV	Can lead to 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 33 and 34
36	Resource depletion	HI	-
37	Introduction of vulnerabilities into software products	HI	Can lead to 36
38	Disk error	HI	Can lead to 36

[a.] In relation to AFTER and SESAME: threats 29 – 31 are internal human-related threats; 33 and 36 – 38 – internal with no human involved; 32 – 35 – external natural threats.

Fire (threat 33) can be an internal or external threat – individual or caused by, e.g., an earthquake. Although fire could also be triggered by a flood (due to short circuits), this can be less elaborated, as well as connection between fire and resource depletion (due to increase of the temperature).

Noticeably, links between threats differ in terms of their strength. Understanding the context and system properties of the grid is needed to assess the corresponding degrees of strength. This can be done by experts who would assign specific correlation coefficients, expected values, and other properties of the system operating in context.

C. Relating threat categories to buildings

Cross-relating threat categories to groups of grid components allows to reduce the number of threats to be considered for the system as a whole. As the grid normally balances the electricity production and demand in real time, relating threats to this function of the grid is useful. With malicious threat events to buildings described [8] in Fig. 2, we provide mapping of IRENE non-malicious threat categories to groups of grid components. Similarly to [9], we specifically

build on the logic of relating blackout causes to increased demand, failure of transmission and failure of production.

Among threat categories, environmental (weather-related) ENV threats can impact all classes of grid components. In unfavorable weather conditions the flexibility of the grid (e.g., spared amount of generated reserves) is reduced. Weather can push the grid out of the generating and consumption balance, degrade functionality of components, and result in the direct destruction of components. For example, weather can increase energy demand due to heat waves or cold weather, such as during an ice storm in the winter of 1998 in Montreal. In another example, weather can hamper the electricity production. Specifically, during droughts the lack of water available to cool down energy production stations 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.

ACC and HI threats are to be considered differently from ENV threats. HI events are random and therefore can threats production and transmission grid components. Still, ACC and HI do not commonly pose threats to multiple grid components at once. Thus, as a failure of one consumer will not necessarily leads to a blackout, such threats can be less considered in connection to consumers if the grid stability is a major concern.

IV. Conclusions and Discussions

The contribution of this paper relates to outlining a variety of ways for constructing a threat landscape for future risk assessments using threat taxonomies. It describes analysis of (1) relations between threat taxonomies relevant to smart grids, (2) links between non-malicious threats, and (3) relations of threat categories to grid components. By delineating ways to look beyond a particular list of threats, it helps to study the grid threat landscape in more detail. It can also support envisioning of possible scenarios of undesirable events. The illustrations provided in this paper are based on the IRENE threat list. This threat list stems from information security risk assessment recommendations of NIST 800-30. Thus, the conducted analysis can be integrated into frameworks of risk assessment of an information system, business process, or organization.

As this paper aims at outlining a vision, we acknowledge that the relations between the three taxonomies are not fully worked out and hence constitute future research. Also, as the paper is high level in nature, further analysis of links within event chains is needed. For threat-to-threat dependencies experts are needed to examine such relations. Experts can consider the strength of the outlined relations, e.g., by fault-error-failure-fault error propagation chain [10] and other approaches from the dependability domain. The same applies to correlating threats in different taxonomies, including deriving qualified dependencies between threats stochastically.

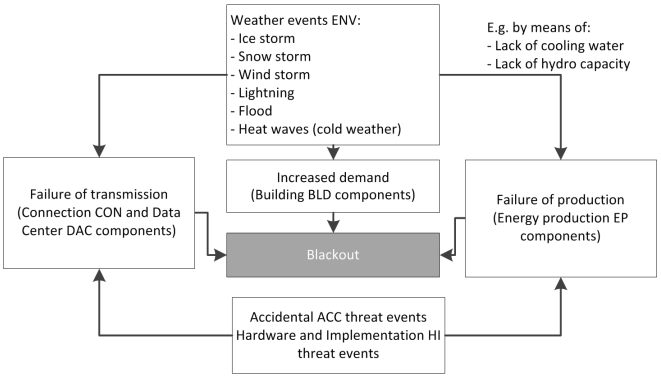

Fig. 2. IRENE threat categories related to grid components.

Aspects related to the impact of interruptions caused by different threats are outside the scope of this article. Risk assessment methodologies accounting for both the impact and probability of a particular threat can be used once relevant threats are identified. These methodologies are construct and investigate chains of events, e.g., with the help of Bayesian solutions. One example of such a model is a way to combine Bayesian networks and the FAIR taxonomy [12].

Another future research direction concerns spatio-temporal data management systems capable to cope with intricate threat mapping in space and time dimensions.

References

[1] World Bank Group, “Infrastructure dataset,” June 2016. [Online]. Available: www.enterprisesurveys.org/data/exploreTopics/Infrastructure.

[2] J. Wirfs-brock, “Power Outages On The Rise Across The U.S,” June 2016. [Online]. Available: http://insideenergy.org/2014/08/18/power-outages-on-the-rise-across-the-u-s/.

[3] CPNI “Security for Industrial Control Systems,” June 2016. [Online]. Av.: www.cpni.gov.uk/advice/cyber/Security-for-Industrial-Control-Systems/.

[4] O. Jung, S. Besser, A. Ceccarelli, T. Zoppi, A. Vasenev, L. Montoya, T. Clarke, and K. Chappell, “Towards a Collaborative Framework to Improve Urban Grid Resilience.” In: IEEE International Energy Conference, Energycon 2016, 4-8 Apr 2016, Leuven, Belgium. pp. 1-6. IEEE.

[5] SESAME, “D1.1 - Report on the analysis of historic outages,” 2011. [Online]. Av.: https://www.sesame-project.eu/publications/deliverables/d1-1-report-on-the-analysis-of-historic-outages/view.

[6] IRENE, "D2.1 – Threats identification and ranking," 2015. [Online] Av.: http://ireneproject.eu/wp-content/uploads/2016/01/IRENE-D2.1.pdf.

[7] W. Pieters, C. W. Probst, Z. Lubszo, and L. Montoya, "Cost-Effectiveness of Security Measures: A Model-Based Framework.," In Approaches and Processes for Managing the Economics of Information Systems, T. Tsiakis, T. Kargidis, and P. Katsaros, Eds., ed Hershey, PA USA: IGI Global, 2014, pp. 139-156.

[8] A. Vasenev, L. Montoya, A. Ceccarelli, A. Le, and D. Ionita, D., “Threat navigator: grouping and ranking malicious external threats to current and future urban smart grids.” In: 1st EAI International Conference on Smart Grid Inspired Future, 19-20 May 2016, Liverpool, United Kingdom. pp. 1-8.

[9] 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.

[10] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, C., “Basic Concepts and Taxonomy of Dependable and Secure Computing.” IEEE Trans. Dependable Secur. Comput., 1(1), pp. 11-33.

[11] E. Çetinkaya and J. Sterbenz, "A taxonomy of network challenges," Design of Reliable Communication Networks (DRCN), 2013 9th International Conference on the, Budapest, 2013, pp. 322-330.

[12] A. Le, Y. Chen, M. Chai, A. Vasenev, and L. Montoya, “Assessing loss event frequencies of smart grid cyber threats: Encoding flexibility into FAIR using Bayesian network approach”. In: 1st EAI International Conference on Smart Grid Inspired Future, May 2016, Liverpool, United Kingdom. pp. 1-8.