Threat navigator: grouping and ranking malicious external threats to current and future urban smart grids

Alexandr Vasenev[1], Lorena Montoya[1], Andrea Ceccarelli[2], Anhtuan Le[3], and Dan Ionita[1]

1-University of Twente, 7522 NB Enschede, The Netherlands
{a.vasenev,a.l.montoya,d.ionita}@utwente.nl
2-University of Florence, Viale Morgagni 65, Firenze, Italy
andrea.ceccarelli@unifi.it
3-Queen Mary University of London, E1 4NS, London, United Kingdom
a.le@qmul.ac.uk

Abstract. Deriving value judgements about threat rankings for large and entangled systems, such as those of urban smart grids, is a challenging task. Suitable approaches should account for multiple threat events posed by different classes of attackers who target system components. Given the complexity of the task, a suitable level of guidance for ranking more relevant and filtering out the less relevant threats is desirable. This requires a method able to distil the list of all possible threat events in a traceable and repeatable manner, given a set of assumptions about the attackers. The *Threat Navigator* proposed in this paper tackles this issue. Attacker profiles are described in terms of *Focus* (linked to *Actor-to-Asset* relations) and *Capabilities* (*Threat-to-Threat* dependencies). The method is demonstrated on a sample urban Smart Grid. The ranked list of threat events obtained is useful for a risk analysis that ultimately aims at finding cost-effective mitigation strategies.

Keywords: Smart Grid; Threat Assessment; FAIR; NIST; Risk Analysis

1 Introduction

Since smart grids are common targets of cyber-attacks [1], there is a clear need to inform smart grid stakeholders about relevant security threats. Moreover, it is of great benefit if a structured ranking of threats is provided.

However, ranking threats for a specific system poses several challenges: i) first, it is complicated or time-consuming to explore each individual threat in detail in relation to complex smart grids; ii) second, there is a severe lack of suitable and widely-accepted methods. In particular, although *qualitative* approaches (e.g., built on the NIST 800-30, NISTIR 4628, or NIST 800-53) benefit from advanced categorizations of threats, they comprise only high-level descriptions that do not specify how to achieve the threat ranking goal. A *quantitative* analysis based on the FAIR [2] taxonomy, has the potential to address the challenge, but using it alone may hamper reusing the threat categorization previously mentioned. Therefore, a method for coherently ranking threats for smart grids using a fusion of these two approaches,

e.g., when threats are identified using NIST and ranked using FAIR, would constitute a significant research contribution to smart grids threat assessments. To achieve such an objective, this paper proposes the *Threat Navigator*, which involves a method to filter out less relevant threats, and rank threat events in a rigorous yet flexible manner.

The *Threat Navigator* aims to help stakeholders concentrate on threats with high Loss Event Frequency (*LEF*) in a traceable and repeatable way, thus reducing the number of threat events that need to be further analysed. Input data for the *Threat Navigator* can be extracted from NIST standards with different levels of granularity.

The practical relevance of the *Threat Navigator* relates to that of Intel's TARA methodology [3], specifically, because efficiency and efficacy of cyber-physical risk assessments can be increased if a suitable level of guidance is adopted to distil large amounts of possible attacks into a digest of the most relevant [3].

The method advances the state of the art with regards to other publications in the domain, e.g., [4], [5], [6], as it offers the possibility to relate system threats to system assumptions. This allows the rapid investigation of system design alternatives or identification of the most feared attackers (malicious actors) and threats, even when assumptions on attackers or threats change.

In the next sections we outline the adopted threat taxonomy, present the *Threat Navigator* method, and show how it can be applied to urban smart grids.

2 Threat taxonomy

This section describes the adopted relevant threat factors derived from the mentioned methodologies. These factors are later applied to threat grouping and ranking. We build on the FAIR taxonomy, where *Risk* (the probable frequency and probable magnitude of future loss) is calculated using *Loss Event Frequency* (*LEF*, the frequency, within a given timeframe, that loss is expected to occur) and *Probable Loss Magnitude*. *LEF* is further subdivided into *Threat Event Frequency* and *Vulnerability*. Vulnerability deals with *Control Strength* and *Threat Capability*.

The adopted taxonomy bridges constructs from FAIR and NIST (Fig. 1). We consider NIST's *Targeting* concept to correspond to FAIR's *Contact* concept, while *Intent* corresponds to malicious *Actions*. It enables the use of the standards in a complementary manner, thus benefiting from both of them. This includes the possibility to calculate LEF for a threats' list that stems from the application of NIST 800-30.

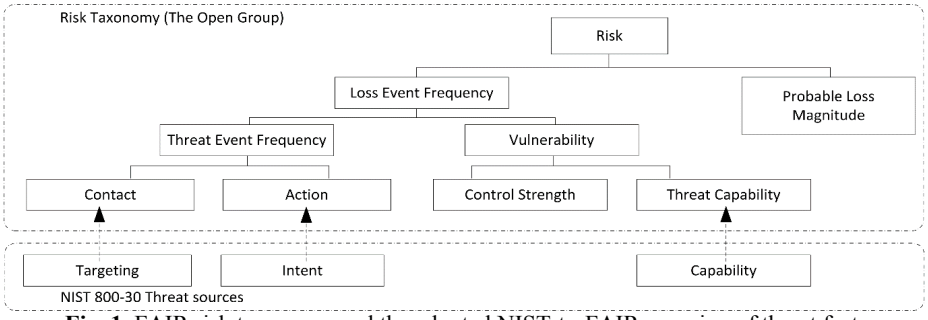

Fig. 1. FAIR risk taxonomy and the adopted NIST-to-FAIR mapping of threat factors.

In our methodology, we group *Contact* and *Action* (i.e. *Targeting* and *Intent*) into the *Focus* construct. This grouping is reasonable as *Targeting* can be linked to (e.g., reinforced by) *Intent* and both factors are asset-specific. *Focus* depicts how a malicious actor(s) aims at a specific asset (e.g., a type of electric grid element) and indicates the degree of probable physical and cyber contacts of the attacker with the grid assets, together with the attacker intention to launch attacks. *Control Strength* indicates the strength of a counter-measure to limit the success of the attacker.

The adopted threat taxonomy for the needs of this research is therefore composed of *Focus* and *Vulnerability*. The latter includes *Control Strength* as a system characteristic and *Threat Capability* as an attacker characteristic. Together, *Focus* and *Threat Capability* are two threat factors that depict attacker profiles and constitute a structure to differentiate specific classes of threat actors. These factors are used within the *Threat Navigator* to find and rank relevant threats.

3 *Threat Navigator* as a method to rank *LEF* of threats

The proposed *Threat Navigator* method (Fig. 2) takes pre-processed input data and outputs the *LEF*s of relevant threats.

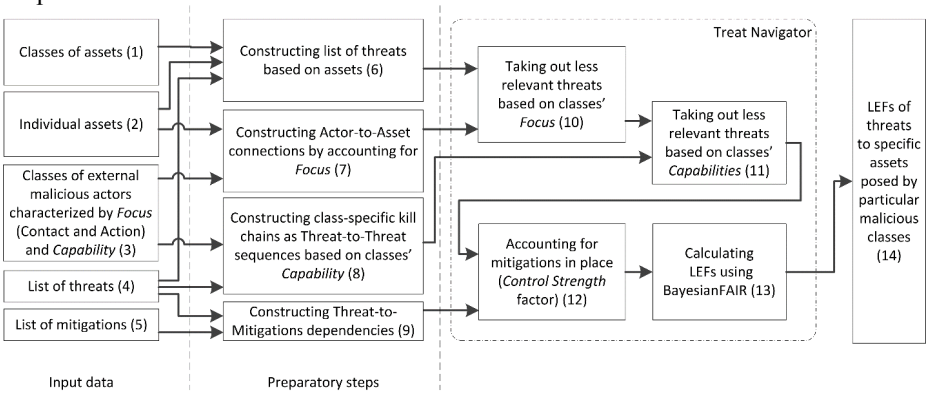

Fig. 2. Proposed *Threat Navigator* method.

The input data are the following: 1) "Classes of assets" are grid assets, 2) individual grid components reflect the categories and individual assets, 3) "Classes of external malicious actors" define which actors apply to individual threats, 4) "List of threats" represents the generic list of threats to be considered; it is later used to identify all threats for the given assets, 5) "List of mitigations" includes controls that can be implemented against the threats listed in [4]. These data are pre-processed to construct 6) a list of threats to be refined, 7) *Actor-to-Asset* and 8) *Threat-to-Threat* connections, and 9) *Threats*-to-*Mitigations* links.

Subsequently, the *Threat Navigator* uses the constructed relations to remove threats less relevant to specific classes of attackers based on their *Focuses* (10) and *Capabilities* (11). Next, the method accounts for implemented mitigations (12) and finally calculates *LEF* for threats (13).

4 An example of input data and pre-processing blocks

Input data (1)-(5) and pre-processing (7)-(9) blocks are generic and remain relevant for every grid configuration, while (6) is linked to a particular grid configuration.

(1) Relevant classes of components include Connections, Energy Provider, Building, Data Centre, and Others.

(2) The list of grid components includes: 1. Electricity Connection, 2. Data Connection, 3. Micro Grid Connection, 4. Connection Adapter, 5. Connection Adapter with Energy Transformer, 6. Long-Range Connector, 7. Power Plant 8. Photo Voltaic Energy Generator, 9. Wind Farm, 10. Factory, 11. Stadium, 12. Hospital, 13. Offices, 14. Offices District, 15. Smart Home, 16. Generic Special Building, 17. Basic Data Centre, 18. SCADA, 19. Data and Electricity Storage, 20.EV Charging Point, 21.Access Point.

(3) We consider three basic classes of malicious actors. *Commodity actors* (C1) are opportunistic; most often they do not have organizational support, e.g., recreational hackers, vandals, and sensationalists. *Targeted actors* (C2), e.g. virus writers, crackers, can have some organizational support. *Actors posing advanced persistent threats* (C3) are highly motivated and may include terrorists and actors of nation-states, organized crime, or corporate espionage.

(4) and **(5).** The list of all of 28 adversarial threats and 13 mitigations identified using NIST references can be found in [7] together with the selection reasoning.

(6) Contrary to other input data and pre-processing elements, this block is specific to a grid configuration. Using a system of systems approach, it constructs lists of threats for grid features (one or more grid components) under consideration. This includes threats relevant to i) individual components, ii) classes of components, and iii) groups of components. The specifics of this process are described in [8].

(7) *Actor-to-Asset* connections depict how the classes of attackers are linked to the list of assets (blocks 1 and 2) for the C1-3 threats classes (block 3) based on their *Focus* characteristic. Three sets of such mappings are constructed [8]: a) C1_set {1, 2, 11-16, 20, 21}, b) C2_set {1-6, 8-17, 19-21} and C3_set {1-21}. Only Power Plant and SCADA components are linked exclusively to class C3. This is because these assets remain significantly less available to insufficiently organized actors.

(8) *Threat-to-Threat* sequences are patterns of attacks i.e., kill chains [9], which vary across different actors. NIST-based threats can be constructed as a kill chain based on threat categories [8] e.g., 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 (CA, i.e. direct/coordinate attack tools or activities), Achieve Results (AR, i.e., cause adverse impacts, obtain information), and Coordinate a Campaign (CC). This generic kill chain structure can be populated for classes C1-C3 as follows (number in parenthesis indicate the threat number):

C1: PRGI (2)-CCAT(4)-EC(9,11,12)-CA(17,18)-AR(23-25)

C2: PRGI(1-3)-CCAT(4)-DIIMC(6)-EC(8-12,14)-CA(15-18,20-22)-AR(23-25)+CC (26)

C3: PRGI(1-3)-CCAT(4)-DIIMC(5-7)-EC(8-14)-CA(15-22)-AR(23-25) +CC (26-28)

These sequences represent *Threat-to-Threat* connections. They include interrelations between i) individual threats, ii) individual threats and threat categories, and iii) categories of threats.

(9) *Threat-to-Mitigation* links are described in [7]. Essentially, these are many-to-many relations, where every mitigation is linked to several threats.

5 An example of applying the Threat Navigator

In this section the calculation of the *LEF*s of threats relevant to a Factory feature (Factory and Long-Range connector components) within an urban smart grid is illustrated. We assume that the threats (posed by all attackers) identified in block 6 are {5, 13, 22, 23, 30, 36, 37, 2, 3, 7, 8, 12, 14, 19, 26, 28, 32, 33, 34, 35, 1, 6, 15}.

(10) According to the *Focus* property, one can identify that both Factory and the Long-Range connector are linked to attacker classes C2 and C3, hence the sets of threats C2_set and C3_set are the ones to be considered.

(11) Filtering based on the Capability of threat actors is performed, thus filtering FFactory threats with respect to attacker classes C2, and C3. Table 1 illustrates threats: (1) Related to a particular attacker class (denoted as "X" in the following table); (2) Not attributed to a specific class (marked as "|"); and (3) Absent in the list of threats of this feature ("-"), although it should be considered in principle, given the Capability of threat actors.

Table 1. Threats relevant to the factory feature.

Steps of kill chain	Considered threats	Relevance to Class C1	Relevance to Class C2	Relevance to Class C3
PRGI	1/2/3	|	X	X
CCAT	4	-	-	-
DIIMC	5/7	|	|	X
	6	|	X	X
EC	8	|	X	X
	9/10/11	-	-	-
	12	X	X	X
	13	|	|	X
	14	|	X	X
CA	15/16/22	|	X	X
	17/18	-	-	-
	19	|	|	X
	20/21	|	-	-
AR	23	X	X	X
	24/25	-	-	-
CC	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+ ΔC2-C3, where ΔC2-C3 corresponds to threats related to C3 but less to C2. The Factory feature list includes threats {5, 7, 13, 19, 28}.

(12) Mitigations for each threat taken from (9) can be grouped according to C2 or C3, as shown in the first two columns of Table 2. The result of analysing which actors can pose threats to specific grid features provides: (1) A list of threats relevant to C2 actors for the grid feature, including threats that apply if a more advanced class should be taken into account; (2) A list of mitigations relevant to these lists of threats. This provides a checklist of mitigations that can be implemented to make the feature more robust to attacks related to a specific class.

In this example it is assumed that mitigation number 4 (Security Assessment and Authorization) was implemented for the list of identified threats of the Factory feature. Essentially, as interrelations between the threats and mitigations are intricate, implementing an individual mitigation may give rise to input vector changes for several threats. The update concerns controls to threats {3, 6, 8, 14, 26} for class C2 (table below). Similarly, we can find the change in controls for threat {7, 19, 28} relevant to the transition from C2 to C3.

Table 2. Identifying the degree of implemented controls as a FAIR construct for C2 threats.

Threat number	Relevant mitigations	% of mitigations implemented	Qualitative characterization of controls
1	11, 12, 18	0%	Very Low
2	11	0%	Very Low
3	4, 12, 16, 19	25%	Low
6	4, 17, 19	33%	Medium
8	1, 4, 12, 15	25%	Low
12	8, 10, 13, 16	0%	Very Low
14	4, 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	4, 9, 10, 12	25%	Low

Thus, controls for several threats {3, 8, 26, 7, 19, 28} are improved from 0 to 25%, while for threats {6, 14} the control increased to 33%. Because of these changes, the *LEF* of each threat changes.

(13) BayesianFAIR [10] is then used to calculate *LEF* of [*Contact, Action, Threat Capability, Control Strength]* of an individual threat. The vector elements are within the range of qualitative values from 'Very Low' to 'Very High'. This approach is described in [8]. The first three elements of the vector are known from attacker profiles and the last one is derived based on the mitigations implemented. For example, without mitigations, the input vector for C2 threats {1, 2, 3, 6, 8, 12, 14, 15, 22, 23, 26} is [Medium, Medium, Medium, Very Low]. The logic of forming the input vectors for calculating *LEF*s is shown in Table 3.

Table 3. 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	

(14) *LEF*s of threats relevant to class C2 calculated using BayesianFAIR are:

1. For threats without mitigations {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] is [0.013; 0.045; 0.503; 0.265; 0.174]. The value of *LEF* is 701.9.
2. For threats with 25% increase in mitigations {3, 6, 8, 14, 26}, the 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
3. For threats with 33% increase in mitigations {6, 14}, the input 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 (e.g., the decrease in *LEF* for threats with only one mitigation implemented is found to be 17). Two mitigations lower a *LEF* by 50. Fig. 3 shows *LEF* values of C2- and C3-relevant threat events calculated in the same manner. Potentially, some absolute or relative *LEF* values can be targets for stakeholders who seek to introduce balanced and sufficient mitigations with respect to the threat landscape.

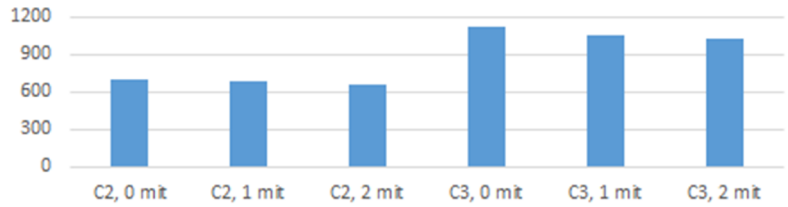

Fig. 3. Ranking groups of threat events.

6 Conclusions

This paper proposes the *Threat Navigator* which provides a method for a) filtering out less relevant threats for a complex system and b) ranking the rest of the threats. The threat taxonomy adopted within the method bridges the NIST and FAIR methodologies, thus benefiting from both of them, including the calculation of *LEF* for NIST-specified threats using the FAIR taxonomy.

The presented approach is structured but is also highly adjustable, as changes in input data update the consequent filtering and ranking steps in a traceable manner.

Unfortunately, due to the page limit this article cannot fully illustrate the degree of the flexibility embedded into the method, such as: (1) the possibility to account for more attacker classes by applying the briefly outlined profiling approach and (2) specifying the *Control Strength* value increase as a non-linear function of implemented Mitigations. Similarly, other topics were not described in the paper e.g., positioning of the method within the wider assessment process, some specifics of attackers for urban smart grids, and illustrations on how the method can be applied to more sophisticated examples. Further research includes evaluating the extent to which it increases efficiency of cyber-physical risk assessments in comparison to e.g., Intel's TARA. Nevertheless, the *Threat Navigator*'s modular structure suggests that the mentioned modifications and the integration of the method into a risk assessment is plausible.

Ultimately, the aim of this asset-based approach is to focus the risk assessment on what is most relevant. From the point of view of data processing, it avoids the need to manually update vast amounts of data. Thus, smart grid stakeholders can rapidly consider relevant threats and related countermeasures for multiple threats simultaneously. Together with impact analysis, it can therefore help to determine the most cost-efficient mitigation strategies to be implemented.

Acknowledgments. This work has been partially supported by the Joint Program Initiative (JPI) Urban Europe via the IRENE project. We would like to thank Prof. Roel Wieringa for his valuable contribution.

References

1. CS-CERT: ICS-CERT Year in Review, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/ Year_in_Review_FY2014_Final.pdf.
2. The Open Group: Technical Standard. Risk Taxonomy, http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf.
3. Intel IT: Prioritizing Information Security Risks with Threat Agent Risk Assessment, http://www.intel.com/Assets/en_US/PDF/whitepaper/ wp_IT_Security_RiskAssessment.pdf
4. Najgebauer, A., Antkiewicz, R., Chmielewski, M., Kasprzyk, R.: The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution. Journal of Telecommunications and Information Technology (2008): 14-20.
5. Lund, M.S., Solhaug, B., Stølen, K.: Risk analysis of changing and evolving systems using CORAS. In: Foundations of security analysis and design, Heidelberg, 2011: 231-274.
6. Morison, K., Wang, L., Kundur, P: Power system security assessment. Power and Energy Magazine, IEEE 2.5 2004: 30-39.
7. IRENE: D2.1 Threats identification and ranking, http://www.ireneproject.eu.
8. IRENE: D2.2 Societal impact of attacks and attack motivations, http://www.ireneproject.eu
9. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Bethesda, MD: Lockheed Martin Corporation, 2010, 3.
10. 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.