8

STECA – Security Threats, Effects and Criticality Analysis: Definition and Application to Smart Grids

Mario Rui Baptista[1], Nuno Silva[1], Nicola Nostro[2], Tommaso Zoppi[3,4] and Andrea Ceccarelli[3,4]

[1]CRITICAL Software S.A., Coimbra, Portugal
[2]Resiltech s.r.l., Pontedera (PI), Italy
[3]Department of Mathematics and Informatics, University of Florence, Florence, Italy
[4]CINI-Consorzio Interuniversitario Nazionale per l'Informatica-University of Florence, Florence, Italy

8.1 Introduction

The reliability of electrical power systems, since their first use, has been addressed focusing on ensuring the continuous power supply and on the management of critical situations in order to avoid electrical disruption due to potential failures. In the last decade, we are witnessing the increasing development of Smart Grids, with €3.15 billion investment in Smart Grids projects amongst the EU-28 Member States only in the period 2002–2014 [1]. Smart Grids enhance the classical electrical systems by introducing optimization of grid management, both from transmission and quick reaction to power disruption through real-time and automated technologies; deploying and integrating of large-scale renewable energy systems; reducing management and power costs, for final users; and introducing and integrating of smart appliances and consumer devices. While these new aspects make the electrical systems effective, they become more and more interconnected thus making them vulnerable to cyber and physical attacks [2–4]. Indeed, it is possible to remotely perform changes (e.g., to instructions, commands and configurations), disabling actions, shut down or in general interfere with the

proper functioning of the system, thus causing in the worst case significant damages and safety issues [3, 5].

In the Smart Grid domain, security threats can be originated by several agents: consumers, insiders, and terrorists [3]. Customers could be interested in falsifying smart meters data in order to steal electrical power. Similarly to attacks performed to broadband modems, customers may try to attempts attacks to smart meters aiming at modifying the firmware controlling the reporting operation, thus decreasing the usage of electricity [3]. Terrorist attacks to smart grids may lead to unprecedented black-outs, from the point of view of spatial and time extension [4]. This calls for a fundamental attention to the identification and management of potential security threats.

This chapter proposes the STECA (STECA – Security Threats, Effects and Criticality Analysis) approach to perform security assessment of Smart Grids. The hereby proposed process describes a way in which to identify vulnerabilities, their related threats, and proposes a risk assessment approach and a path to identify appropriate countermeasures. This process is based on the same principles used for the Failure Mode and Effect Analysis (FMEA)/FMECA process, which is a technique widely used for safety critical analysis and is highly regarded by the majority of international standards [6]. STECA starts from a vulnerability point of view and moves on towards threat analysis and criticality assessment. Following the guidelines defined in [7], the approach is instantiated on a Smart Grid use case, resulting in a set of precise guidelines and a systematic way to perform security assessment including vulnerability evaluation and attack impact analysis.

8.2 Motivation

8.2.1 Motivating Concerns in Industry

A fundamental aspect that has to be considered in the implementation of Smart Grids and that is currently under the stakeholders' spotlight is related to the security issues yet to unveil in the overall Smart Grid or at the connected devices [3, 8], and the consequent impact on safety. Among the impact situations of a service disruption due to a cyber or physical attack, *property/financial damage* and *human life hazard* should be kept in closer consideration, as the time for recovering is currently unpredictable.

Previous works on Smart Meters qualification revealed potential security weakness and exposed some of the equipment vulnerabilities [3]. This can present a great risk for the future implementation of Smart Grids. It is also true that, due to the ground-breaking character of this technology and the

quantity of interfaces that are made available, the *security requirements of the components that will operate in the grid and the grid system itself are not yet sufficiently accurate* (either they are not studied or implemented/tested, not analysed or imposed yet at a larger scale). This is also strengthened if we consider these systems general exposure in terms of pervasive interfaces.

In fact, in an informal *industrial security assessment of Smart Grid* components, the company CRITICAL Software identified security problems that are usually disregarded by traditional assessment approaches if performed without a proper process or tools. Examples of these problems included: (i) denial of service possibility, (ii) proscribed access to equipment; (iii) physical security deficiencies; (iv) unintended access to systems parameters that should be read-only; and (v) communication protocol implementation and specification weakness. The experience of CRITICAL Software's industrial assessment projects ended up providing most of the incentive for the development of the STECA process due to the gaps found. First, CRITICAL Software was providing a security assessment to substantiate a test framework being developed at the time. Security issues were observed in the assessed Smart Grid components, both on requirement analysis and actual component functional tests, despite the work was focused only on a limited part of the target Smart Grid equipment. In yet another case only the communications protocols were under test on a preliminary stage. For instance, it was identified that it is possible without much trouble to generate conditions that force the interruption of energy supply to a user on the grid. Either by simulating excessive energy demand or by tampering with billing contract parameters, it is also possible to provoke a Denial of Service. This form of service disruption by hacking the metering equipment is a commonly acknowledged threat, but the impact is largely underestimated. Several other ways of generating conditions that will switch off the Load Control Switch can also be identified. It was also clear from the functional testing that the meter's communication ports could easily be disabled by setting its timeout parameter to zero, rendering the equipment incommunicable and thus impossible to be reconfigured remotely.

Though this experience identified serious security impact scenarios that justified the need of security assessment, the support available today to security assessment is limited. There is no history on the components usage and thus no clear way to understand the attack trends or attacker profiles, the attacker objectives and the effects of the attacks. It is extremely difficult to rate the likelihood of a threat, on which to perform a risk or hazard assessment. Summarizing, there are no real data to work on, which obstacles the possibility to create a solid base to build a security assessment upon. Also,

as there is no relevant history of these analyses, it is impossible to even start by using previous knowledge, checklists, pre-defined lists, etc.

One should also consider the constant struggle that resides in identifying the vulnerabilities and security threats. On a system of this sort the number and diversity of security threats could be huge. An undertaking of this magnitude should inevitably find trouble when aiming to achieve completeness: to claim that all vulnerabilities have been identified and all security threats analysed will prove to be a nearly impossible task. Even an expert experience based approach to identify a procedure to tackle this problem is not a straightforward exercise.

8.2.2 State of the Art and Background

Standards such as [9–11] propose general, high level methodologies to guide the security assessment of systems. However, standards typically present the main steps but they do not describe the techniques that can be exploited to realize these steps. This calls for solutions that, still maintaining compatibility with the standards, are able to provide an adequate support to the security engineers. Additionally, several challenges are still open, such as verifying the completeness of an analysis or compute likelihood and impact of a given threat.

Several works target techniques for security assessment, also considering interdependencies between security and safety. The work presented in [12] proposes an extension of the FMEA safety analysis technique, aiming to analyse likelihood and impact of cyber-attacks to embedded multicore systems in the automotive industry. Another contribution, still related to the automotive domain [13] aims at proposing a novel approach to deal with both safety hazard and security threat analysis combining the Hazard Analysis and Risk Assessment with the security STRIDE approach for the automotive battery management [14] proposes a framework for quantitative security analysis used to identify potential attack points and paths, thus to recognize those that are feasible from the perspective of an attacker and finally proposing meaningful countermeasures to the system. In [7] the authors propose a general methodology to understand issues' criticality and the difficulties in finding a proper solution able to deal with interdependencies between safety and security. To this purpose, in their work a general security threats library has been developed, which can be updated over the time and has been mapped to the NIST security controls [8]. Other contributions evaluating the effects of security breaches exploits exist as the work in [15], which states a

comprehensive and practical framework for electric smart grid cyber-attack impact analysis using graph-theoretic dynamical systems paradigm.

The STECA process presented in this chapter is specifically focused on Smart Grids. It naturally includes the objective of detecting potential security threats and providing efficient mitigations, and it translates the concept of FMEA to a *vulnerability-oriented* security assessment where reference categories are extracted from supporting *threat libraries*. Additionally, it guarantees compatibility with main standards [9–11]: in fact, the reference data to build the threat libraries are extracted from the standard [10], and it is easy to define a correspondence between the main steps of the STECA process and the steps of methodologies in [9, 11].

8.3 STECA Process Description

This section presents a detailed description of the STECA process, along with a running example to illustrate the application of the process to an actual industry problem related to the main theme of this publication.

8.3.1 The High Level STECA

The hereby proposed process (Figure 8.1) describes a way to identify vulnerabilities, their related threats, proposing both a risk assessment approach

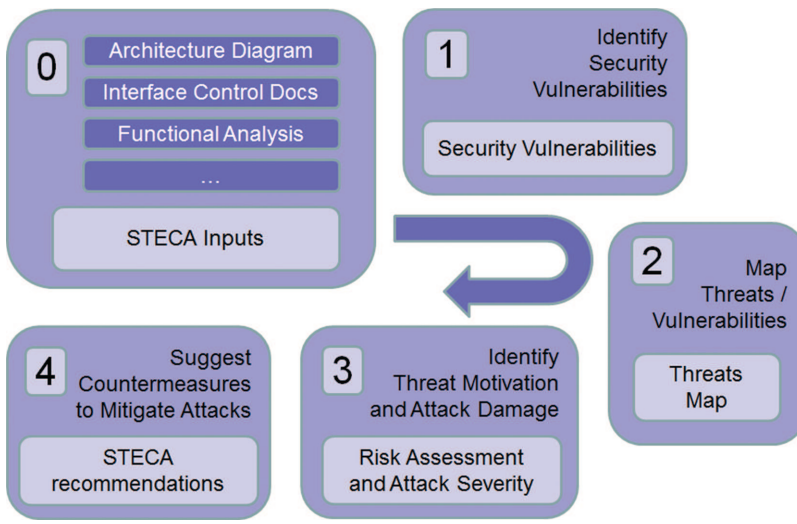

Figure 8.1 High level view of the STEC process.

and a path to identify appropriate countermeasures. Four high-level steps are identified.

This process is based on the same principles used for the *FMEA/FMECA* process [12] which is widely used for safety critical analysis, and is highly regarded by the majority of international standards. Subsequently, the high level steps depicted in Figure 8.1 will be described in closer detail.

8.3.2 STECA Inputs

In order to efficiently apply the process several inputs are required and need to be collected. The input set includes, but is not limited to:

1. *The Architecture Diagrams*. These, along with the Functional Analysis, will be used to identify the system's vulnerabilities.
2. *The Interface Control Documents*. These will allow a better threat identification while analysing vulnerabilities.
3. *A Functional Analysis.* This, along with the Architecture Diagrams, will be used to identify the system's vulnerabilities.
4. *Other useful input information*. Typical security attacks, history data, system requirements, environment conditions, requirements, etc.

For the running example we're using the diagram in Figure 8.2 – an energy industry Smart Grid, focusing on the Smart Meter Home Area Network (HAN) – the most widespread case of user connected to the Smart Grid, also a high vulnerability spot as it exposes the metering devices to the internet through the Consumer HAN.

8.3.3 Security Vulnerabilities

With the STECA inputs we can identify possible intrusion and attack locations considering the system weak spots listed in Table 8.1. For each of them, we reported an extended description and the links to the consolidated ISO/IEC 27005 [6] vulnerability classification which lists the hardware, network and software vulnerability categories. Additional vulnerability classifications are the Microsoft Security envelopment Lifecycle (SDL) [16] and the CWE3 (Common Weakness Enumeration [17]), which is a detailed and community-developed list of common software weaknesses.

Traditionally, the vulnerability assessment [2, 11] of architectures such as the one in Figure 8.2 are performed by (i) cataloguing assets and capabilities (resources) in a system, (ii) assigning quantifiable value (or at least rank order) and importance to those resources, (iii) identifying the vulnerabilities

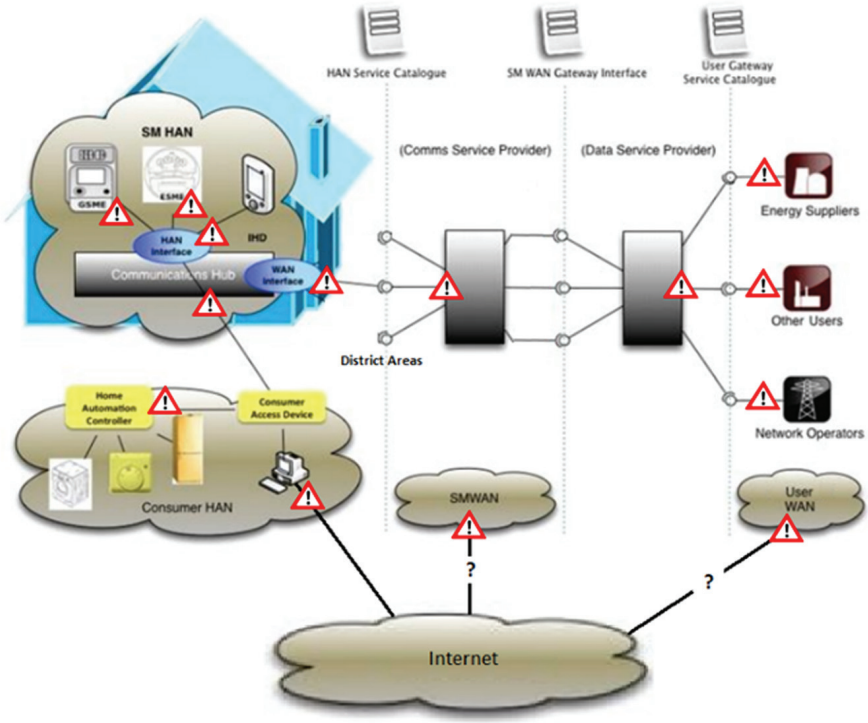

Figure 8.2 Example from the Energy industry showing the architecture of a Smart Grid.

or potential threats to each resource and, (iv) mitigating or eliminating the most dangerous vulnerabilities for the most valuable resources.

The first three steps are required to be performed in order to obtain a vulnerability list. Also, by assigning an order (value) to the resource (vulnerability) we are simplifying the threat severity definition described in Section 8.3.5.

Each component (system resource) should be classified with a value (as of an asset) which could simply be a traditional High, Medium or Low grade according to the associated monetary replacement cost – to be defined by the system/subsystem owner; and a severity grade based on the impact that its failure would inflict on the system. To do this, the catalogue depicted later in Section 8.3.5 is proposed to be used.

Continuing the running example, and focusing on the Communications Hub (in the Smart Meter HAN) as it is a gateway to the metering devices, and

Table 8.1 Vulnerabilities, weak spots, and security threats

Vulnerabilities	Weak Spots	Weak Spots	Security Threats
Network	CH communications protocol Smart Meter access control	CH communications protocol	Message Modification Man in the middle Footprinting
Software	CH communications protocol Smart Meter access control Smart Meter functions	Smart Meter access control	Unauthorized access Password cracking Disclosure of confidential data
Hardware	Smart Meter functions	Smart Meter functions	Conduct cyber-physical attacks on organizational facilities Arbitrary code execution

the electricity Smart Meter itself, as it is a big concern in the motivation, we obtain the following:

- **Communication Hub**: *Value*: Low; *Severity:* Minor;
- **Electricity Smart Meter**: *Value* Low; *Severity:* Critical/Catastrophic.

8.3.4 Threats Map

In this step of the process the security threats shall be identified and catalogued by performing the following sub-steps:

- *Identify the threats for each vulnerability*. Following the list produced in the previous step, we list the threats that may exploit each vulnerability. This operation will produce a list of threats per vulnerability.
- *Catalogue Threats (NIST classes)*. Identified threats will most likely be found in the known threats list, thus having associated countermeasures. Most possibly, the gathered threats have already been identified in different contexts and catalogued in a generic fashion in existing documents, thus a set of countermeasures and preventive actions might already be available. For this purpose, already existing classification taxonomy may be used. For this process we're using the threat library already created in [7], which will help to catalogue the threats to the NIST classes and the suggested countermeasures.

- *Threat Classification Completeness Check*. If unlisted threats arise, countermeasures should be suggested to mitigate them and the threat library should be complemented by adding this new information to the respective taxonomy class.

Next in the running example, the weak spots are identified and respective Vulnerability categories. Some examples are reported in Table 8.2.

Following through with the running example and mapping these threats to the Threat Library it is possible to catalogue almost all of them to the NIST classes and gather the respective countermeasures to mitigate them. The NIST 7628 [9] states, in more than one occasion, that its focus is cyber-security and therefore "The requirements related to emergency lighting, fire protection, temperature and humidity controls, water damage, power equipment and power cabling, and lockout/tag-out are important requirements for safety. These are outside the scope of cyber security and are not included in this report. However, these requirements must be addressed by each organization

Table 8.2 Linking weak spots and ISO/IEC 27005 vulnerability categories

Weak Spots	Description	ISO/IEC 27005 [6] Categories	Threat Example
Component interfaces, communications ports/ protocols	These are usually the targets to corrupt communications either to attain disruption or impersonating another party.	Network	Man in the middle packet sniffing conducted between the smart meter and the Energy Management Gateway
		Software	Inject malicious code into the USB device controller (*BadUSB*, [18])
Memory and Storage Units	These may be used to store malicious code for later execution or even altered firmware when system reconfiguration is required.	Software	Installation of a malware which damages user data or key memory areas
		Hardware	Damaging the Hard Drives (i.e., putting a magnetic source near the storage rack servers)
Processing Units	These, of course, may be used to execute the malicious code.	Software	Inserting malicious code that calls for ALU operations slow downing the whole execution
		Hardware	Malicious hardware module targeting the performance of the cache accesses or generating power faults

in accordance with local, state, federal, and organizational regulations, policies, and procedures." In this example, the "Conduct cyber-physical attacks on organizational facilities" threat could be the example stated in the motivation section where an Electricity Smart Meter is rendered inoperative and incommunicable, inducing a denial of service occurrence with potentially catastrophic impact, and will be the focus of the running example in the following sections.

8.3.5 Risk Assessment and Attack Severity

For this step, similar to the *Cause and Effects analysis*, there are two things that need to be accounted for when considering each threat event: *probability* and *impact*.

Probability: (Attack Profit – Motivation). In several contexts the parameters used to calculate the probability of an attack are based on a likelihood extracted from existing data. In general, there are no "reasonable" approaches to compute the likelihood of an attack, apart using past history, meaning that this specific approach is applicable only for few systems. As in this case there is no such data, we propose to use the estimated benefit that the attacker may obtain due to a successful attack. This can be seen as a combination of (i) *Cost:* availability of resources to perform the attack (time, money, state of the art hardware), (ii) *Risk of detection* (to what extent can the attacker hide his actions and how much does he care about being detected) and (iii) *Payoff* (the benefit that an attacker expects from exploiting a vulnerability). These three components can be considered separately or grouped together to build a unique likelihood score that can be obtained depending on the specific needs. One possible likelihood example could be an index that represents the cost/benefit trade-off, calculated as the fraction of *Payoff* over *Cost* but, for this purpose, we propose a form of calculation using the three variables as shown in Figure 8.3.

Having the lowest values on the origin (0,0,0) and increasing each variable in each of the respective axis. Colour code (green, yellow and red) represents the likelihood of an attack as depicted (unlikely, moderate and likely, respectively).

The Attack Probability assigned values are just an example and, when applied, should be adapted to the respective domain requirements. If it is considered that a system exposure to attack is less dependent on payoff than the other variables, more red and yellow dots should be reflected on the graph.

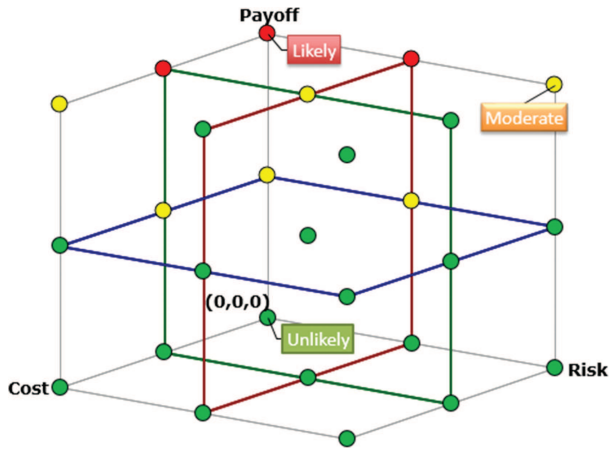

Figure 8.3 Attack probability graph.

Impact: (Attack Damage). The extent to which an attack may cause damage. This should include all harmful consequences. It may be calculated based on the individual resources involved (associated value and severity), the effects produced by a general failure of the resources involved and the derivate pernicious effects from the aftermath. The worst case scenario should be considered for the Impact calculation.

The Risk of a given Threat Event used in this case is based on a traditional Criticality approach. The values used in this example have a higher weight on the Impact rather than the Probability.

The values in Figure 8.4 were calculated by multiplying the grades assigned to the respective probability and impact ranks. A green code was assigned to values lesser than or equal to 3, yellow to values between 4 and 9 inclusive and red to values greater than or equal to 10. Again, this is an illustrative example and the colour code should be adapted to the

Threat Event Risk		Attack Probability		
		Likely (3)	Moderate (2)	Unlikely (1)
Impact Severity	Catastrophic (5)	15	10	5
	Critical (4)	12	8	4
	Major (3)	9	6	3
	Minor (2)	6	4	2
	Negligible (1)	3	2	1

Figure 8.4 Threat Event Risk Matrix.

Category	Severity	Description of Consequences
	Catastrophic	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
	Critical	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
	Major	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
	Minor	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
	Negligible	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Figure 8.5 Description of impact categories.

domain requirements. Higher a criticality is inherent the intervals should slide accordingly.

As for the Severity categories, the consequences were gathered from the NIST Threat Events Impact Assessment Scale but, once again, they should be dependent on the domain requirements. Discrimination goes as in Figure 8.5.

Picking up the running example, to assess a likelihood value for the "Conduct cyber-physical attacks …" threat by using the suggested process, we would come out with the following result: *Cost: low, Risk: Medium, Payoff: Medium/High*.

In the case of the Payoff the assigned grade may depend on the objective of attacker. If the objective is the actual denial of service, the Payoff could be considered High – the worst case scenario. This would produce a Probability result of Moderate to Likely (2 or 3 in Figure 8.5). Moving to the Threat Event Risk calculation, and considering the Smart Meter asset severity grade of Critical/Catastrophic (4 or 5 in Figure 8.5), the result would come out in the range of 8 to 15 (mostly Red).

8.3.6 STECA Recommendations

After all vulnerabilities and respective threats are considered and analysed, countermeasures and preventive actions should be suggested for each of them.

Either from the existing documentation and standards and the educated analysis performed where the vulnerabilities are yet to be acknowledged. Countermeasures should be suggested according to their respective mitigation type, as in:

- *Vulnerability*: the optimal option if possible. If a vulnerability may be avoided all the associated threats will be cleared.
- *Threat Event*: if a treat event may be prevented, the associated security threat will be cleared.
- *Threat probability/impact*: If it is impossible to avoid a threat, consideration should be given to reducing its impact. By downsizing the probability and/or the impact its risk will be downgraded making the system a bit safer. The priority will be set according to the domain and/or system requirements.

The countermeasures are not mutually exclusive and more than one might be applied for each threat. There are, of course, a number of considerations while selecting from the available options, most typically the trade-off between the countermeasure implementation costs vs. its effective security improvement. For a better evaluation in this regard, further iterations of the process including the countermeasures implementations should be performed.

To aid and formalize the process of the security threats analysis, a STECA report depicted in Figure 8.6 should be produced based on the proposed template. For each security threat one of these entries should be included (the fields should be self-explanatory once one is acquainted with the process):

1: STECA ID	4: Weak Spot (Vulnerability)	5: Vulnerability (ISO/IEC 27005 connected categories)	6: Security Threats	7: Threat Library Mapping	8: NIST Proposed Countermeasures	12: Treat Event Risk	13: Alternative Countermeasures	14: Recommendations
STECA-001-01	Smart Meter functions	- Software - Hardware	Execute or generate conditions that lead to the execution of unscheduled functions	Arbitrary code execution	Stay current with patches and updates to ensure that newly discovered buffer overflows are speedily patched.	6		
STECA-001-02	Smart Meter functions	- Software - Hardware	Induce a power cut and reconfigure the communications port to render the meter inoperative and incommunicado	Conduct cyber-physical attacks on organizational facilities	None	10	Use a Smart Meter with redundant metering equipment activated through manual bypass	Should be mandatory for households having infants, seniors or patients on life support systems

Figure 8.6 STECA report example.

1: STECA ID – Unique identifier of a security threat;
2: Architecture Diagram/Model – Relevant Model and/or Diagram files for the process;
3: Domain – Domain to which the process will adapt (Space, Automotive, Railway, Energy...);
4: Weak Spot (Vulnerability) – A mark on the Diagram/Model to signal a weak spot on a component (as in Table 8.1);
5: Vulnerability (ISO/IEC 27005 connected categories);
6: Security Threats – Threat on a vulnerable component (weak spot);
7: Threat Library Mapping – Respective threat in the Threat Library;
8: NIST Proposed Countermeasures – Countermeasure info from the Threat Library;
9: Countermeasure Effectiveness – Applicability of the Threat Library proposed countermeasure to this specific security threat;
10: Attack probability – Calculated as described in Section 8.3.5;
11: Impact Severity – Calculated as described in Section 8.3.5;
12: Treat Event Risk – Calculated as described in Section 8.3.5;
13: Alternative Countermeasures – Countermeasure suggestion if none are available or are considered ineffective;
14: Recommendations – Further considerations to be kept in mind;
15: Assumptions – Assumptions to security threat or regarding information if any;

Notes: Any additional information that might be relevant and does not fit any of the previous.

Note that some of the columns in Figure 8.6 are hidden considering only the most relevant ones for the example. After the report is concluded, meaning all the threats in all the weak spots are analysed and addressed, the STECA process iteration is finished.

To conclude the running example, and as far as countermeasures are concerned (apart from the ones suggested by the Threat Library as shown in Figure 8.6), the suggestions could be something along the lines of the physical countermeasures referred in Section 8.2, filling in the gap in the Threat Library:

- Dumb Meter Bypass
- Smart Meter Black Box

Even if cyber security issues are addressed by threat and risk assessment processes, the STECA can help to identify unaddressed high impact security issues, and support a security/safety report to deliver to the proper authorities.

Based on the STECA results new security requirements may be derived or the existing ones may be improved; those new/updated requirements will lead to improvements in the system safety architecture and design.

8.4 Conclusion

In this chapter, we presented the STECA (Security Threats Effects and Criticality Analysis) process to help formalizing the security analysis of complex systems such as Smart Grids. The necessity of devising STECA stems from the direct experience of engineers working in the security assessment of the Smart Grid domain. The proposed process is established on a similar mature technique used for safety critical systems for decades (FMEA/FMECA) and maps to the well-known NIST taxonomy for the security vulnerabilities and threats analysis. We demonstrated that STECA application is straightforward and useful for security assessment.

References

[1] European Commission. (2014). *JRC Science and Policy Reports, Smart Grids projects outlook*.

[2] European Union Agency for Network and Information Security (ENISA). (2013). Smart Grid Threat Landscape and Good Practice Guide.

[3] Parks, R.C. (2007). *Advanced Metering Infrastructure Security Considerations*. Sandia Report SAND2007-7327.

[4] National Research Council. (2012). *Terrorism and the Electric Power Delivery System.* Washington, DC: The National Academies Press.

[5] NIST. (2011). *NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security*.

[6] International Organization for Standardization (ISO). (2008). *ISO/IEC 27005, Information technology – Security techniques – Information security risk management*.

[7] Nostro, N., Bondavalli, A., and Silva, N. (2014). Adding Security Concerns to Safety Critical Certification," in *Software Reliability Engineering Workshops (ISSREW)* (New York, NY: IEEE), 521–526.

[8] NIST. (2013). *Joint Task Force Transformation Initiative, Security and privacy controls for federal information systems and organizations NIST SP 800-53r4*.

[9] NISTIR. (2014). *NISTIR 7628*: *Guidelines for smart grid cyber security strategy and requirements*.

[10] NIST. (2013). *NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*.

[11] NIST. (2012). *Special Publication 800-30 Revision 1*: *Guide for Conducting Risk Assessment*.

[12] Schmittner, C., Gruber, T., Puschner, P., Schoitsch, E. (2014) "Security Application of Failure Mode and Effect Analysis (FMEA)," in *Computer Safety, Reliability, and Security*, eds A. Bondavalli, F. Di Giandomenico. SAFECOMP 2014. Lecture Notes in Computer Science, Vol. 8666. Springer, Cham.

[13] Macher, G., Höller, A., Sporer, H., Armengaud E., and Kreiner C. (2015) A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems, in *Computer Safety, Reliability, and Security*, eds Koornneef, F. and van Gulijk, C. Lecture Notes in Computer Science, Vol. 9338. Springer, Cham.

[14] Nostro, N., Matteucci, I., Ceccarelli, A., Di Giandomenico, F., Martinelli, F., and Bondavalli, A. (2014) On Security Countermeasures Ranking through Threat Analysis," in Computer Safety, Reliability, and Security, eds A. Bondavalli, A. Ceccarelli, F. Ortmeier. SAFECOMP 2014. Lecture Notes in Computer Science, Vol. 8696. Springer, Cham.

[15] Kundur, D., et al. (2010). "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Smart Grid Communications (SmartGridComm)* (New York, NY: IEEE).

[16] Microsoft. (2010). *Security Development Lifecycle*.

[17] Common Weakness Enumeration. (2017) *A Community-Developed Dictionary of Software Weakness Types*. Available at: https://cwe.mitre.org/index.html

[18] Kaspersky Lab. (2014). *Release of Attack Code Raises Stakes for USB Security*. Available at: https://threatpost.com/badusb-attack-code-publicly-disclosed/108663/ (accessed on 2 October 2014).