ASSESSMENT OF CYBER SECURITY REQUIREMENTS FOR THE FUTURE DIGITAL POWER SYSTEM

Roberta TERRUGGIA
RSE - Italy
roberta.terruggia@rse-web.it

Giovanna DONDOSSOLA
RSE - Italy
giovanna.dondossola@rse-web.it

Mauro Giuseppe TODESCHINI
RSE - Italy
maurogiuseppe.todeschini@rse-web.it

ABSTRACT

This paper addresses the assessment of the cyber security requirements in terms of standards and architectural solutions needed by the evolution of the digitalized power infrastructure.
A use case related to the requirement analysis for the implementation of a congestion management function is addressed by the study to explain the methodology and to propose some results. These types of results represent a valid support to the following security by design implementation of the extended smart grid operation infrastructure by the utility.

INTRODUCTION

The current power system operation is facing the integration of new distributed and intermittent energy resources: this new landscape requires to rethink the operation strategies considering the benefit offered by the flexibility that the generation and load resources can provide. This allows to obtain not only the stability of the grid, but also some ancillary services and a more efficient grid operation. To achieve these objectives the ICT (Information and Communications Technology) architecture needs to be enhanced including new components and extending the communication infrastructures in many cases with heterogeneous technologies and commercial services.
The digitalization of the power grid required by the new control strategies leads to the necessity to address the cyber security aspects. The inclusion of flexible resources implicates some adaptations of the ICT architecture and the enhancement of the cyber security solutions implemented into the infrastructure.
A key aspect for the definition of new applications and for the extension of an operational environment is the assessment of the system in terms of the cyber security requirements and implemented infrastructure solutions. It becomes of paramount importance to evaluate and compare the security posture of the solutions under analysis to address the more appropriate setup.
The assessment methodology proposed in this paper allows to establish the cyber security posture of the system under analysis in terms of security requirements identifying the vulnerabilities and highlighting the main improvements required to maintain a suitable level of security. To this purpose the analysis deploys a tool able to evaluate the compliance to a set of cyber security guidelines and standards of the system under study. Moreover, it allows the detection of the main vulnerabilities and weaknesses of the ICT architecture comprising the key information, communication and operational components.
The paper presents an analysis method based on the Cyber Security Evaluation Tool (CSET®) [1] developed by the Department of Homeland Security to study the more important set of requirements identified by the security standards and architectural solutions.
The paper is structured as following: first the assessment methodology is presented, then a use case related to the inclusion of a congestion management function in the infrastructure is described. This will be used as guide for the analysis. The standard and architectural assessment is then explained and some analysis results presented. Then the conclusions are provided.

METHODOLOGY

The methodology is applied to the evaluation of the cyber security posture of a smart grid monitoring and control infrastructure extended with a new congestion management functionality currently under specification in the OSMOSE European project [2].

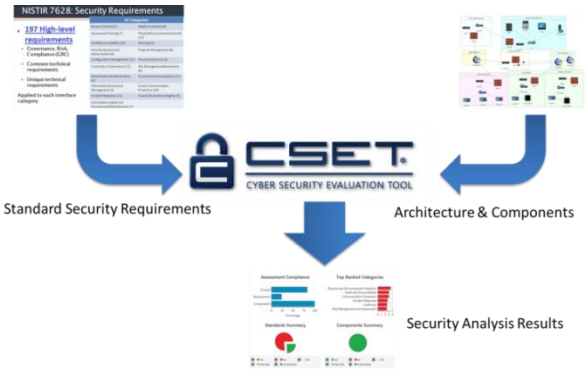

Figure 1 General analysis approach for the cyber security requirement selection

The focus of the analysis is on the NISTIR 7628 guidelines [3] for smart grid cybersecurity and on the architecture comprising the main information, communication and operational components required to perform the congestion management functionality.
The CSET tool allows to perform a standard and guideline analysis, an architectural analysis and to combine both to obtain an overall analysis. In this study

the approach depicted in Figure 1 is addressed, where the standard and architectural analyzes are combined.
The tool allows to assess the importance of each requirement extracted from the guidelines and supports in the selection of the more noteworthy ones considering the required system security level. Moreover, the main information, communication and operational assets are identified and the architecture evaluated in terms of vulnerabilities in network and security components. A sensitivity analysis is performed to compare different security setup. This approach allows to evaluate various solutions changing the analysis parameters to estimate the more appropriate configuration and set of requirements to address.

Figure 2 Security assessment outcomes

Examples of possible results that can be obtained from the security assessment of the smart grid monitoring and control infrastructure, augmented with the new congestion management functionality, are presented in graphics and ranking tables of the type depicted in Figure 2. These are in terms of requirement analysis and component analysis where both the standard and architectural requirement compliance and the infrastructure weaknesses are highlighted.

USE CASE

The use case addressed by the study is related to the requirement analysis for the implementation of a congestion management function.
The congestion management is performed by an enhanced Energy Management System (EMS) able to achieve a reliable, economic and secure grid operation with periodic updates of the dispatching plans involving flexible loads, power flow control devices and renewable generators.
This function operates within a Zonal Energy Management System (ZEMS) that optimizes the use of energy resources connected in a defined geographical zone.

It receives information about the state of the national transmission network, consisting of the electrical network measurements, the status of the switches and the actual scheduled power flow at the boundaries of the controlled Zonal network.

It also receives information from the sub-transmission network in which it operates, consisting of the requirements for the loads, the generation of DERs (Distributed Energy Resources) and the availability of Zonal interruptible/flexible loads.

ZEMS processes this information periodically and sends the output data relating to control action to resolve or mitigate the congestion to a Regional Control Center. The operator will use the information to dispatch the zonal network optimally and safely.

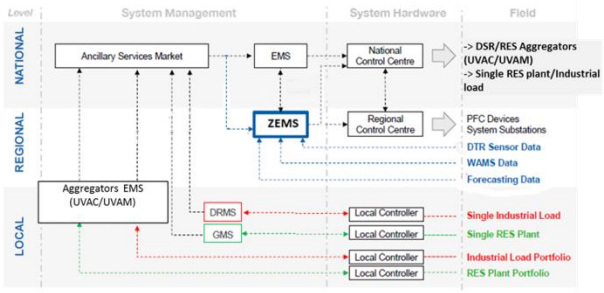

Figure 3 Component interaction for congestion management function [2]

Figure 3 presents an overview of the main components and their interactions for the execution of the congestion management function.

STANDARD SECURITY REQUIREMENTS

The CSET tool allows to perform the assessment selecting different standards and guidelines. Some of them are related to general requirement of cyber security in IT context, others are more specific. Considering the power and Smart Grid domain, in this analysis the NISTIR 7628 has been selected in order to evaluate the main cyber security requirements considering the use case.
NISTIR 7628 is a document that presents an analytical framework useful for organizations to develop effective cybersecurity strategies addressing the combination of specific structural aspects, risks, and vulnerabilities. The methods and the supporting information presented in the document can be used as guidance for assessing risk and identifying and applying appropriate security requirements.
The standard security requirement assessment can be performed following the exact text formulation of the standard or by means of more customer oriented questions.
Indeed, the assessment based on the specified standard (or different standards in case of more complex analysis) can be completed following a Question-based approach where simple questions are answered or using a Requirements-based approach, where the exacting wording of the standard is applied. In the following analysis the second one option has been chosen.

ARCHITECTURE & COMPONENT REQUIREMENTS

In order to perform a more complete analysis of the security requirements of a specific infrastructure is useful to consider the architectural aspects and the involved components. The CSET tool provides a network diagram editor that allows to draw the ICT architecture including the main nodes, networks and security solutions.
These components represent the basis for the assessment phase, indeed the general system cyber security posture depends on the single solutions implemented in the infrastructure. The different assets are grouped in categories, the questions used for the analysis refer the asset categories, but the answers can be specialized for each single component.

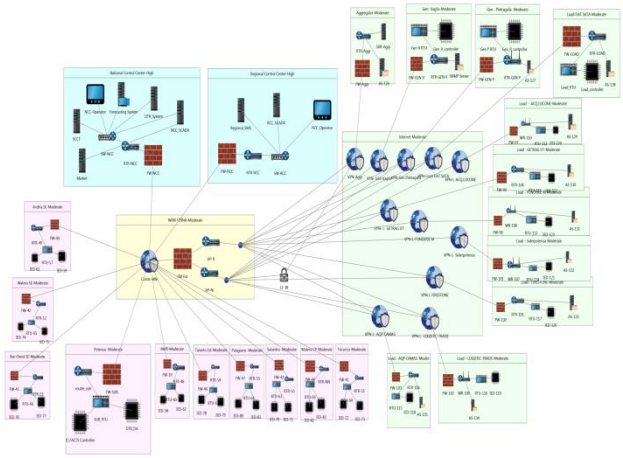

Figure 4 ICT Architecture

Moreover, the analysis allows to identify the weaknesses of the architecture and proposes some mitigation solutions.
The isolation of the critical assets allows to highlight where to concentrate the action in order to make the whole system more secure.
Figure 4 presents the architecture derived from the use case and used for the analysis presented in this paper.
It comprises several areas: the National and the Regional Control Centers are depicted in blue. These contain the service servers and the main nodes for the monitoring and the control of the power system. Specifically the congestion management functionality is performed by the ZEMS placed at the Regional Control Center site.
The control centers communicate by means of a Wide Area Network (WAN) with the peripheral site (pink in the picture) where the control and measurement components are placed.
The architecture involves also external areas representing the renewable flexible loads and generation plants (green in Figure 4). The communications with them are performed through VPNs (Virtual Private Networks) connecting specific access points. In order to assure the availability of the connection, each external site is able to communicate both via wired as well as wireless channels in redundant way.

ANALYSIS

In this section some results coming from the analysis are presented. Both the standard and architectural requirements have been evaluated in order to identify the more important ones to be implemented considering the use case under study.
Moreover, the system is examined as a whole performing an overall analysis addressing together the two different aspects considered in the previous studies.

Standard assessment

The NISTIR 7628 guideline identifies seven domains relevant for the smart grids and each of them contains specific actors. A logical reference model specifies for each actor the main logical interfaces used for the connection.
Each logical interface in the logical reference model is assigned to a logical interface category. The logical interfaces are grouped in categories in order to simplify the identification of appropriate standard security requirements. Indeed many of the individual logical interfaces are similar considering the security characteristics.
Moreover, the NISTIR 7628 guideline identifies about 200 high level security requirements grouped in 19 families and addressing governance and technical scope.
The guideline selects for each logical interface category a set of high level security requirements taking into account the main peculiarity in terms of risk components.
This set of requirements need to be refined considering the specific context and environment of the system under analysis.
In particular taken into account the congestion management use case, after the identification of the main actors and the association of the logical interfaces of interest, it is possible to obtain a set of high level requirements. This set will be enhanced using the CSET tool.
CSET evaluates the compliance to the standard, in this case the NISTIR 7628 guideline, considering the questions with positive answer. In the analysis the requirements from the guideline application, considering the specific actors and interfaces, are set as satisfied in the assessment phase. This is the basis that will be improved taking into account the results of the analysis.
In order to estimate the compliance of the set of requirements considered as input, it is necessary to identify the level of Security Assurance Level (SAL) in terms of Confidentiality (C), Integrity (I) and Availability (A) required by the system.
The three C-I-A security objectives are defined as:

- **Confidentiality** - A loss of confidentiality is the unauthorized disclosure of information.

- **Integrity** - A loss of integrity is the unauthorized modification or destruction of information.
- **Availability** - A loss of availability is the disruption of access to or use of information or an information system.

Each objective can assume a qualitative value between "Low", "Medium", "High" and "Very High".
The selection of the levels impacts the number of requirements that need to be satisfies.
The Federal Information Processing Standards (FIPS) Publication 199 [4] and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 [5] identify for several sectors the related security objective levels. Considering the Energy sector the suggested levels are: "Low" for Confidentiality, "Medium" for Availability and Integrity.

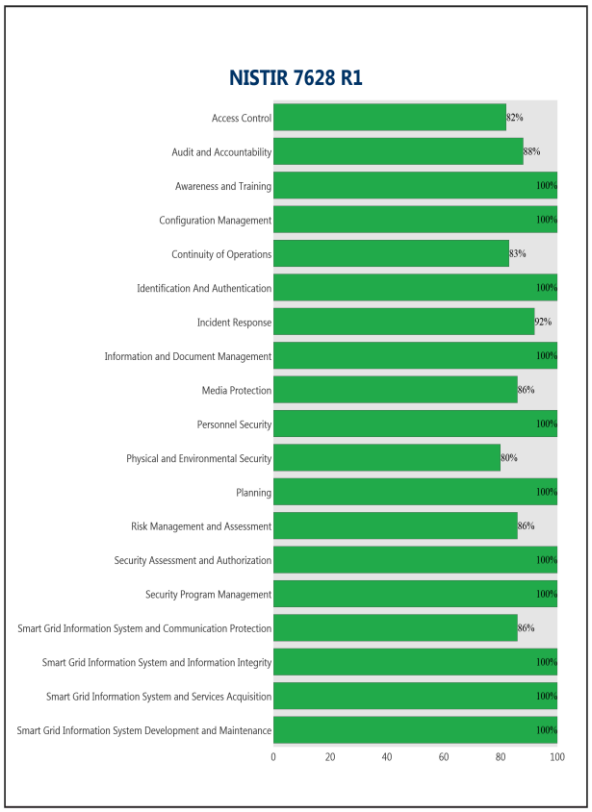

Figure 5 Compliance analysis with C=L, I=M and A=M

Following the above directions, in Figure 5 are shown the results coming from the assessment where the Confidentiality component is set to "Low" and the Integrity and Availability objectives are "Medium". The NISTIR logical interface selection provides a set of about 190 requirements, 20 of them are not considered very important by the CSET analysis. Moreover, from the assessment analysis emerges that there are 5 requirements not included in the NISTIR 7628 set that are considered important (with an high rank) by CSET. These are related to "Access Control" and "Smart Grid Information System and Communication Protection" families.

Architecture – Components assessment

In order to obtain a complete assessment of the security requirements needed to be implemented in the system, the components and architectural aspects need to be addressed. With reference to the congestion management use case and considering the architecture presented in the previous section, an analysis of the more significant security requirements at component level is presented.
The architectural components are partitioned in main categories. These are used to group questions related to similar security aspects.
Figure 6 shows the number of requirements for the different categories, according to the importance of the comprised requirements.
Here a baseline security is considered, only the default security component configurations are considered, all the requirements proposed by the assessment questions are discharged in order to understand which of them have to be implemented following their ranking.

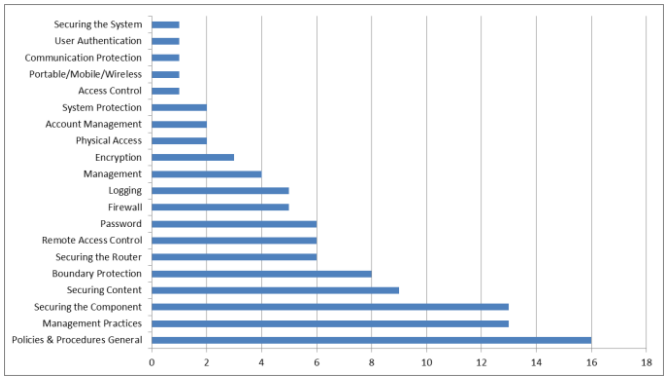

Figure 6 Number of requirements for each category

Figure 7 presents the table with the rank values for each category.

	Rank	Failed	Total
Policies & Procedures General	13.88	16	16
Management Practices	13.11	13	13
Securing the Component	12.43	13	13
Securing Content	8.29	9	9
Boundary Protection	8.29	8	8
Securing the Router	6.64	6	6
Remote Access Control	5.84	6	6
Password	5.8	6	6
Firewall	5.03	5	5
Logging	4.19	5	5
Management	3.24	4	4
Encryption	2.46	3	3
Physical Access	2.13	2	2
Account Management	1.97	2	2
System Protection	1.91	2	2
Access Control	1.11	1	1
Portable/Mobile/Wireless	1.06	1	1
Communication Protection	0.94	1	1
User Authentication	0.87	1	1
Securing the System	0.81	1	1

Figure 7 Category Ranking

The architectural and component assessment allows to identify the weaknesses of the infrastructure under

analysis.
Considering the components and the communications included in the diagram, the analysis highlight where there could be security failings that need attention in the design. Moreover the tool provides some suggestions about how to mitigate the weaknesses.
In Figure 8 the infrastructure diagram of the use case under analysis is depicted. It is similar to Figure 4, but highlights with some red circles: the point of the infrastructure that need attention. Each circle has a number that denotes a reference in the report of the analysis provided by the tool. The numbered references provide specific suggestions on how to improve the architecture.

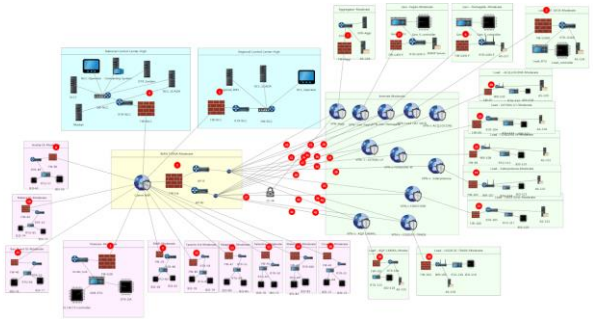

Figure 8 ICT Architecture with identified weaknesses

Moreover each circle is an active link that can be opened in order to explore the specific suggestion. An example is reported in Figure 9.

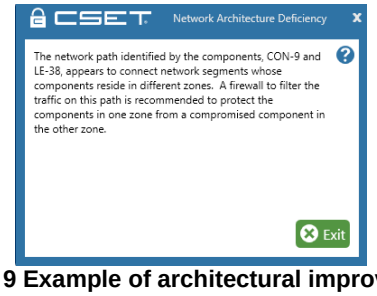

Figure 9 Example of architectural improvement suggestion

Overall assessment

CSET provides an overall analysis where both standard and architectural requirements are considered.
All the questions are ranked and classified in a unique set of categories. This allows to obtain a global view of the security posture of the system and highlight the point of weakness that need to be improved in terms of security requirements.
Figure 10 presents the results achieved by the overall analysis considering the combination of standard and architectural analyzes.

Figure 10 Overall analysis

CONCLUSION

This paper presents a methodology for the assessment of the cyber security posture in terms of standard and architecture requirements. The selected use case addresses the infrastructure extensions needed for the inclusion of new functionalities, in this case the congestion management function. Some examples of analysis are presented. The results depend on the architecture under study, but this methodology is applicable to different scenarios. The results represent a valid support to the following security by design implementation of the extended smart grid operation infrastructure by the utility.

Acknowledgments

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°773406 for the OSMOSE project [2] and by the Research Fund for the Italian Electrical System in compliance with the Decree of Minister of Economic Development April 16, 2018.

REFERENCES

[1] CSET tool - *Department of Homeland Security. ICS-CERT* https://ics-cert.us-cert.gov/Assessments
[2] OSMOSE – European project https://www.osmose-h2020.eu/
[3] NISTIR 7628 rev 1 - Guidelines for Smart Grid Cybersecurity – NIST
[4] FIPS 199 – Federal Information Processing Standards (FIPS) Publication 199 United States Federal Government
[5] NIST 800-60 - Guide for Mapping Types of Information and Information Systems to Security Categories - NIST