21, rue d'Artois, F-75008 PARIS
http://www.cigre.org

PS2-12

D2 Colloquium 2019

Cyber security standard and architectural assessment for a new digitalized power infrastructure

ROBERTA TERRUGGIA* GIOVANNA DONDOSSOLA+
RSE Ricerca sul Sistema Energetico
Italy

SUMMARY

The current power infrastructure is facing an evolution due to the integration of new distributed and intermittent energy resources: the operation strategies need to be rethought considering the challenges and the advantages provided by the generation and load flexible resources. In this evolving landscape 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 cyber security becomes a key point for the digitalization of the power grid required by the new control strategies. The connection of flexible resources involves some adaptations of the IT(Information Technology)/OT(Operational Technology) 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 before implementing the most appropriate setup.

This paper presents a methodology for the analysis of the cyber security requirements in terms of standard and architectural solutions necessary for the extension of existing power control infrastructures with new components and functionalities. The methodology is explained considering the cyber security aspects required for the integration, in a existent architecture, of a Regional Energy Management System with congestion management functionality addressed by the European H2020 project OSMOSE.

The security assessment methodology is based on the Cyber Security Evaluation Tool (CSET®) developed by the Department of Homeland Security to study the more important set of requirements identified by the security guidelines and standards, and related to architectural solutions. The methodology is applied to the evaluation of the cyber security posture of a smart grid monitoring and control infrastructure supporting a new congestion management functionality currently under specification. The congestion management is performed by a new Energy Management System (EMS) 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. The proposed methodology, by means of the CSET tool, allows to evaluate the cyber security guidelines and standards for the system under study and to identify the main weaknesses and prerequisites of the architecture comprising the key IT/OT components. The analysis includes the standard requirements considered relevant for the congestion management functionality implementation. Moreover, the main IT and OT assets are identified and the whole architecture evaluated in terms of pre-requisites (architectural requirements) of the network and security components. The focus of the analysis is on

* roberta.terruggia@rse-web.it

+ SC D2 Regular Member

the NISTIR 7628 guidelines for smart grid cybersecurity and on the architecture comprising the main information, communication and operational components required to perform the congestion management functionality. A sensitivity analysis is performed to compare different security setups. This approach allows to evaluate different solutions changing the analysis parameters to estimate the more appropriate configuration and set of requirements to address in the congestion management implementation. The results from the security assessment, presented in graphics and ranking tables, represent a valid support to the following implementation of the extended smart grid operation infrastructure by the utility. In general terms the analysis methodology can be applied for the design of architecture extensions realizing new functionalities, as in the case of the paper case study, but also for the periodic assessment of operational infrastructures in order to evaluate the best solutions to implement to enhance the current cyber security posture against the evolving threat landscape.

KEYWORDS

Smart Grid – Congestion Management - IT/OT - Cyber Security Assessment – Requirements

1 INTRODUCTION

The integration of new distributed and intermittent energy resources requires to rethink the current power infrastructure in terms of infrastructure and operation strategies adaptations: new component and communication technologies allow to enhance the grid operation and the control strategies have to consider the benefit offered by the flexibility that the generation and load resources can provide. This allows to obtain a more appropriate management of the power system considering the technical and economic plans. The new landscape highlights as the ICT (Information and Communication 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, prerequisite for the new control strategies, points out the paramount importance to address the cyber security aspects. The cyber security implemented into the infrastructure have to be enhanced considering the adaptation required by the connection of flexible resources. The assessment of the system in terms of cyber security requirements and implemented infrastructure solutions is a key process for the design of new applications and for the extension of an operational environment. The security posture of the solutions under analysis have to be compared in order to address the more appropriate setup. Several standards and guidelines define collections of requirements to guarantee the main cyber security objectives, but these lists are often generic and a deeper analysis is needed to refine this set in order to address the exact system under evaluation. Obviously this task cannot be performed manually, but needs to be supported by suitable tools. The assessment methodology proposed in this paper allows to evaluate the cyber security posture of an operational system enhanced with the new functions, the analysis is performed in terms of security requirements identifying the vulnerabilities and highlighting the main improvements required to guarantee a suitable level of security. The methodology proposes the use of a tool able to evaluate the compliance of the system under study with reference to a set of cyber security guidelines and standards. Moreover, the tool allows the detection of the main vulnerabilities and weaknesses of the ICT architecture comprising the key information, communication and operational components. The method presented in this paper is based on the Cyber Security Evaluation Tool (CSET®) [1] developed by the Department of Homeland Security to study the more significant set of requirements identified by the security standards and architectural solutions. The paper is structured as follows: first the congestion management case study is presented, then the methodological approach followed in the analysis is described. The assessment based on standards and architectures is then explained and some analyses results presented. Conclusive remarks are finally provided.

2 CASE STUDY

The security analysis addresses a case study developed by the OSMOSE European project [2] about a new congestion management functionality currently under specification. 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.

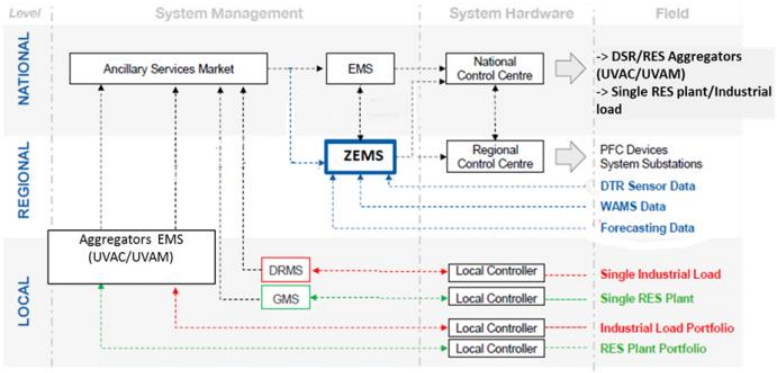

Figure 1: Component interactions for congestion management function [2]

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 flows at the boundaries of the controlled electrical zone. 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 1 presents an overview of the main components and their interactions for the execution of the congestion management function.

3 METHODOLOGICAL APPROACH

The cyber security assessment of a system can be performed following specific standards and guidelines, where the main requirements are identified. The list of security requirements resulting from the simple application of these reference documents, has to be refined: for example in this analysis the NISTIR 7628 guideline [3] is considered. From the application of the NISTIR 7628 methodology to the case at hands, a first set of security requirements can be derived. In cases, such as the congestion management in the sub-transmission grid, where several actors exchange information, the obtained set contains almost all the NISTIR requirements without a specialization. On the other hands some of the excluded requirements could be useful for the specific system under analysis. It is clear that the plain application of the guideline is not reliable enough, but represents a raw basis for the assessment execution. The refinement of this list cannot be performed manually, but needs a tool support helping to steer the selection in a more systematic way. Moreover the requirements coming from the NISTIR address only a high-level architecture, where several architectural and implementation details, that are important for the assessment, are left out.

The security assessment of the congestion management implementation requires the adoption of an appropriate tool. To achieve this goal the Cyber Security Evaluation Tool (CSET®) developed by the Department of Homeland Security has been selected. The CSET 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 can be performed to compare different security setups. This approach allows to evaluate various solutions changing the analysis assumptions to estimate the more appropriate set of security requirements to address.

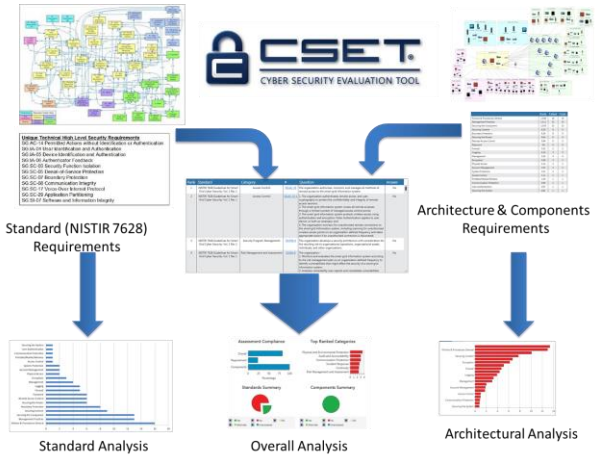

Figure 2: The proposed approach

The approach followed by the analysis is represented in Figure 2. Two independent assessment steps are performed: the standard assessment and the architectural assessment. These are then combined in an overall assessment in order to obtain a complete set of security requirements.

4 CYBER SECURITY ASSESSMENT

4.1 Standard assessment

The CSET tool allows to perform the assessment selecting different standards and guidelines. Some of them are related to general requirements of cyber security in IT context, others are more specific for industrial control environments. Considering the smart grid domain, in this analysis the NISTIR 7628 has been selected for the application of CSET standard assessment in order to evaluate the main cyber security requirements of the case study. NISTIR 7628 is a document that presents a methodological 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 cyber risks and identifying and applying appropriate security requirements. The CSET standard assessment can be performed following the exact text formulation from the standard or by means of more customer oriented questions. Indeed, the assessment based on the selected standard (or different standards in case of more complex analyses) can be completed following a question-based approach where simple questions are answered or using a requirements-based approach, where the exacting wording from the standard is applied. In the following analysis the second option has been chosen.

4.2 Architecture assessment

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 whole 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. Moreover, the CSET analysis run 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 remedial actions in order to make the whole system more secure. Figure 3 presents the architecture derived from the case study 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 sites (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 3). The communications with them are performed through VPNs (Virtual Private Networks) connecting through specific access points to the control network. 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 mode.

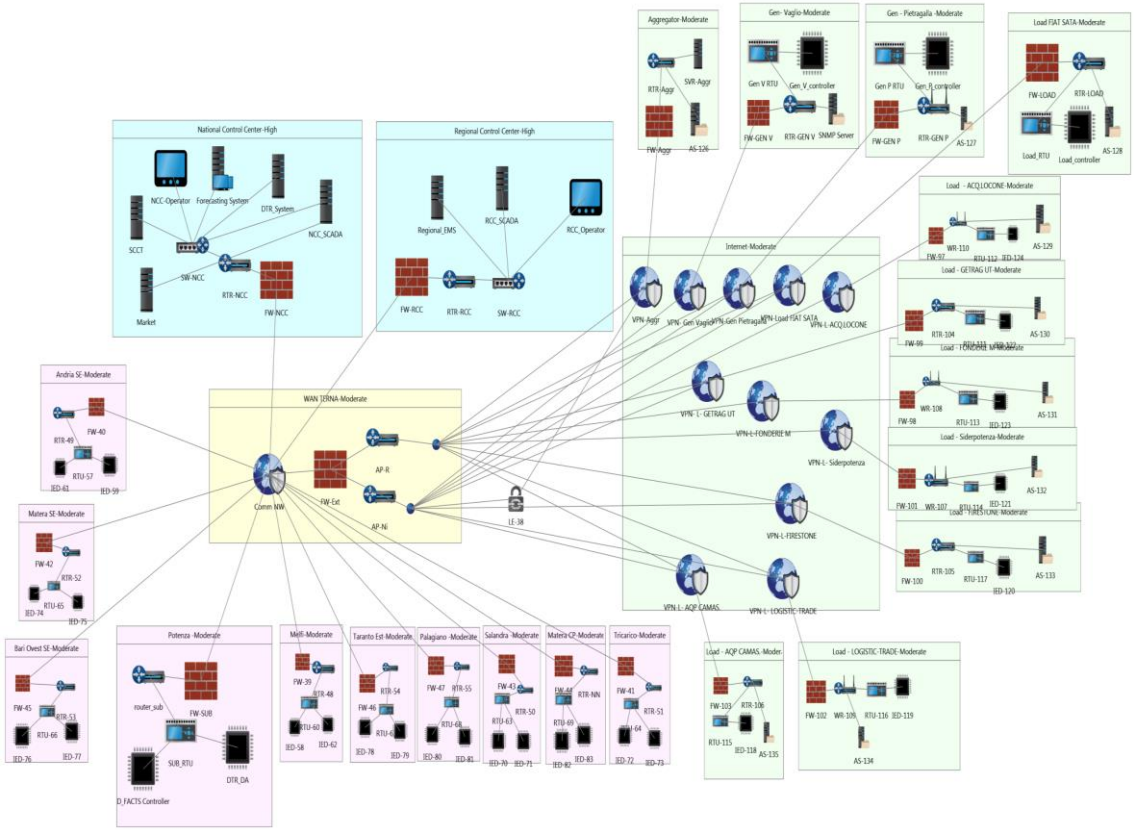

Figure 3: Case study architecture

5 CASE STUDY SECURITY EVALUATION

The focus of the analysis is on the NISTIR 7628 guidelines for smart grid cybersecurity and on the architecture comprising the main information, communication and operational components required to perform the congestion management functionality. In this study the analysis approach depicted in Figure 2 is addressed, where the standard and architectural analyses are performed independently and then combined in an overall run. 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.

5.1 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 information exchanges. 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 scopes. 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 first set of high-level requirements. This set will be enhanced using the CSET tool. CSET evaluates the compliance to the NISTIR 7628 guideline considering the questions with positive answer. In the analysis the requirements from the guideline application to the use case actors and interfaces are set as satisfied in the assessment phase. This is the basis that will be improved taking into account the CSET evaluation results. 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 among “Low”, “Medium”, “High” and “Very High”. The selection of the levels impacts the number of requirements that need to be satisfied. In the following graphs some scenarios considering different levels of the C-I-A objectives are considered and analysed. In Figure 4 left side the lowest levels of security is considered. The graph depicts the percentage of compliance for each requirement family. It is possible to note as the set coming from the literal application of the NISTIR 7628 guideline allows to obtain the whole compliance for almost all the families. The opposite situation is achieved from the analysis with results in Figure 4 right side.

Figure 4: Case study NISTIR 7628 analysis L-L-L (left side) and VH-VH-VH (right side)

Here all the C-I-A objectives are set to "Very High". This is the most restrictive case in terms of cyber security requirements. The previous ones are limit cases, useful to understand the boundaries of the analysis. 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. In Figure 5 it is possible to observe that only some families are fully satisfied, some ones else as for example "Access Control" and "Smart grid information system and communication protection" have a compliance of 82% and 86% so it is necessary to extend the set of requirements coming from the NISTIR 7628 application with additional requirements not included until now in the analysis as for example SG.SC-4 Information Remnants, SG.SC10 Trusted Path and SG.SC27 Heterogeneity.

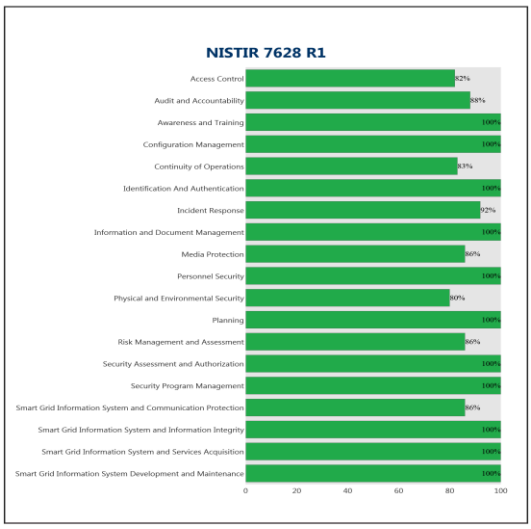

Figure 5: Case study NISTIR 7628 analysis L-M-M

5.2 Architecture assessment

With reference to the congestion management case study and its architecture presented in the previous section, an analysis of the infrastructure weaknesses and of the more significant security requirements at component level is presented.

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 highlights where there could be security failings that need further attention in the design. Moreover, the tool provides some suggestions about how to mitigate the weaknesses. In Figure 6 the infrastructure diagram of the case study under analysis is depicted. It is similar to Figure 3, 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.

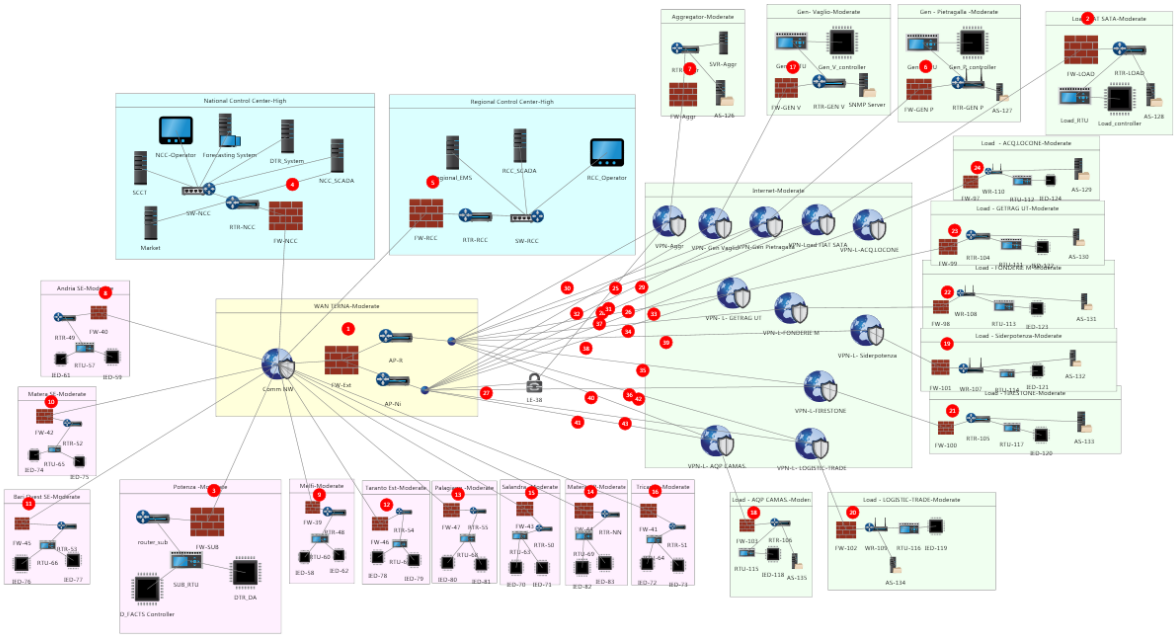

Figure 6: ICT Architecture with identified weaknesses

In addition each circle is an active link that can be opened in order to explore the specific suggestion. An example is reported in Figure 7 where is highlighted the requirement to include an Intrusion Detection System or an Intrusion Prevention System to enhance the firewall capability for the communication between the internal wide area network and the external public network.

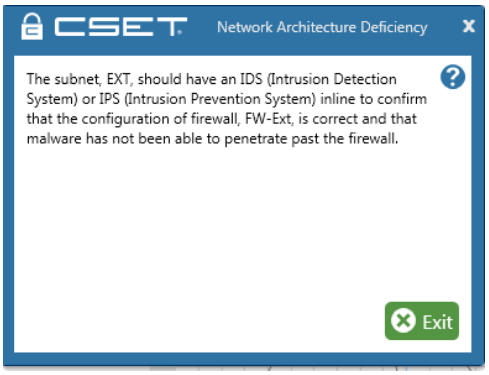

Figure 7: Example of discovered Network Architecture Deficiency

Furthermore, it is important to identify the main architectural requirements significant for the case study implementation. For this reason the infrastructure analysis is completed with specific architectural requirements. In order to address this assessment, it is essential to consider a baseline context in terms of security configuration of the architectural components and communications, and applied policies. Therefore some security assumptions are considered and listed grouped by category in Table I taking into account minimal security measures implemented in the infrastructure.

TABLE I: ARCHITECTURAL ASSUMPTIONS

Category	Assumption
Access Control	Common user accounts are given limited privileges
Account Management	Mechanism for managing and monitoring accounts are in place (e.g. login monitoring, unused accounts, groups and databases removed)
Boundary Protection	The communication are protected with public facing servers are in DMZ, firewall rules reviewed and implemented for control network communications
Firewall	No critical traffic is restricted and ports reviewed an closed if not necessary, withelisting is implemented and Denial of Service (DoS) protections are activated
Management Practices	The account are managed enforcing the remote access policies, operational processes to maintain security are regularly performed, clock synchronization, updates and anomaly detection implemented
Password	Policies for password management are in pace (default password changed, strong admin and user passwords modified at regular interval, no password reusing, all accounts are protected with passwords and the devices keeps the password in a secure encrypted format
Policies & Procedures General	The company installs anti malware software, remote access users require to re-authenticate their credentials, firewall configurations are backing up and inactive administrator sessions locking out
Remote Access Control	Remote access is restricted to secure means only and insecure ones are prohibited, disconnected after 30 minutes of inactivity, white lists are in place.
Securing Content	Info protection methods are implemented to restrict and secure sensitive and personal information
Securing the Components	The system integrity is guarantee by means of turning off the service and processes not required by the application, all sample applications, toolkits SDKs and unused virtual directory are removed, an Uninterruptible Power Supply (UPS) to minimize the impact of power loss implemented, portable media are disabled or limited, unneeded networking features disabled and Ip source routing disallowed
Securing the router	The communications are protected disallowing the IP directed broadcast, router user account and router remote access restricted (only SSH), routers use authentication services for all user authentications
User Authentication	The system utilizes an authentication mechanism such as Active Directory, LDAP or a Kerberos server

Considering the assumptions made for the assessment session, from the analysis run it is possible to obtain a set of further requirements. Table II presents the list of additional requirements relevant for the congestion management function considering the above assumptions. Each requirement is identified by an "Id" composed by the category and the reference number given by the CSET tool.

TABLE II: CASE STUDY ARCHITECTURAL ANALYSIS

Id	Category	Name	Description
ARCH-BP-06	Boundary Protection	ICMP traffic filtering	All incoming and outgoing ICMP traffic have to be denied except where specifically permitted by the organization
ARCH-CP-01	Communication Protection	VLAN usage	Private VLANs, known as protected ports, have to be used to secure sensitive communication over public or unsecure circuits
ARCH-EN-03	Encryption	Client - server communication encryption	Communication between clients and the terminal server have to be encrypted
ARCH-EN-03	Encryption	Node to node communication encryption	Data communications to and from the node have to be encrypted
ARCH-LO-01	Logging	Event logging	Events, such as failed login attempts and failed file system actions, have to be logged
ARCH-LO-02	Logging	Security threat notification	System administrators have to be automatically notified of potential security threats, e.g., failed login attempts, failed file system activity, and malformed URL requests
ARCH-LO-03	Logging	Secure log storage	Logs have to be archived securely on another host for offline analysis
ARCH-LO-04	Logging	Connection logging	All incoming connections have to be logged
ARCH-LO-05	Logging	Authentication event logging	Authentication and administrative events, including enabling and disabling logging, have to be recorded
ARCH-MN-01	Management	System partitioning	The Operating System (OS) and applications, data and database, and logs have to be loaded on separate logical or physical partitions
ARCH-MN-03	Management	Access rule management	Access rules have to be added, modified, and deleted as business needs change
ARCH-MP-05	Management Practices	Test and development servers segregation	Test and development servers have to be located on a different network segment than the production servers
ARCH-MP-09	Management Practices	Database segregation	The database have to be hosted on a physical or virtual separated and dedicated server
ARCH-MP-10	Management Practices	Two factor authentication	System access have to require two factor authentication
ARCH-PP-01	Policies & Procedures General	Session locking	The company have and enforce a policy for locking out inactive user sessions
ARCH-PP-03	Policies & Procedures General	Software and data back up	The company have and enforce a policy for backing up critical software and data
ARCH-SC-01	Securing Content	Code review	Code reviews performed by a change committee and/or peer group have to ensure there are no security or performance issues
ARCH-SC-02	Securing Content	Application error content	Application errors have to be return a generic message rather than a detailed error
ARCH-SC-03	Securing Content	Third-party code review	Third-party code and applications have to be reviewed and approved by an authorized manager or committee
ARCH-SC-05	Securing the Component	Scheduled activitie review	Passwords or other sensitive server information have to be removed from scheduled jobs, scripts, or queries (particularly those in plain text format)
ARCH-SC-06	Securing Content	Sensitive content segregation	Sensitive content have to be isolated from other content
ARCH-SP-01	System Protection	Intrusion Prevention	The company have to employ Intrusion Prevention Systems (IPSs)
ARCH-SP-02	System Protection	Host-based Intrusion Detection	Host-based Intrusion Detection Systems (IDSs) have to be used to alert administrators of anomalies
ARCH-SS-01	Securing the System	Time synchronization	The device have to sync system time to an accurate and reliable clock

5.3 Overall analysis

CSET provides the ability to perform an overall analysis where both standard and architectural requirements are considered together. The NISTIR 7628 requirement categories are similar to the architectural ones, so it is possible to identify some meta-categories in order to obtain a unique list of requirements. All the requirements are ranked and classified as a unique set. This allows to obtain a global view of the security posture of the system and highlights the point of weakness that need to be improved in terms of security requirements.

6 CONCLUSIONS

This paper presents a methodology for the assessment of the cyber security posture in terms of standard and architecture requirements. The proposed approach goes beyond the simple extraction of the list of requirements obtained by the application of standards or guidelines, but allows a refinement that it is essential to address the system under analysis. The methodology is presented considering a selected case study addressing the infrastructure extensions needed for the inclusion in the operational system of new functionalities, in this case the congestion management function. The paper presents some sample analysis results, but the methodology itself has a general validity and may be applied to different scenarios.

From the standard assessment a consolidated list of high-level requirements has been obtained considering the peculiarity of the case study and the security assurance level required. This list has been enhanced with the identification of specific architectural requirements. Starting from some cyber security assumptions, the architectural assessment provided a list of detailed requirements to accomplish in order to make the congestion management functionality implementation more secure. Moreover, the architectural and component analysis highlighted some infrastructure weaknesses to be filled in. Finally the overall analysis allows to obtain a comprehensive view of the requirements and security measures to implement. In particular the access control and communication protection resulted as the highest priority requirements for the congestion management case study.

As long as all the infrastructural details are known and represented correctly, the run results represent a valid support to the following security implementation of the congestion management 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.

7 BIBLIOGRAPHY

[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