Study Committee D2

Information Systems and Telecommunication

Paper 10794_2022

HOW TO ASSESS THE CYBERSECURITY POSTURE OF UTILITY INFRASTRUCTURES? A CASE STUDY FROM THE OSMOSE PROJECT

Giovanna DONDOSSOLA[1], Roberta TERRUGGIA[1], Andrea FOSCHINI[2], Luca ORRÙ[2], Giuseppe LISCIANDRELLO[2], Francesco SILLETTI[2]

[1]RSE S.p.A., [2]TERNA S.p.A.

Motivation

- assess the **cybersecurity posture** of EPU critical infrastructures
- identify **prioritised requirements** for a given Security Assurance Level (in terms of Confidentiality, Integrity and Availability)
- check if the integration in the existing architecture of new ICT systems requires new cybersecurity controls to satisfy the Security Level assigned to the entire system

Method/Approach

1. Standard compliance analysis

Inputs

- Reference standard: e.g. **NIST 800-53**
- **Security Assurance Level** (CIA) : e.g. LMM

Outputs

- Prioritised requirement categories
- **Ranked requirements**

2. Architecture analysis

Inputs

- **ICT architecture, asset categories**
- **Criticality levels** of security domains
- Satisfied security controls

Outputs

- Network warnings
- Ranked control categories
- **Percentage of satisfied/missing controls**
- Cybersecurity Test Plans

3. Scalability Analysis

Inputs

- Results from standard compliance analyses
- Results from architecture analyses

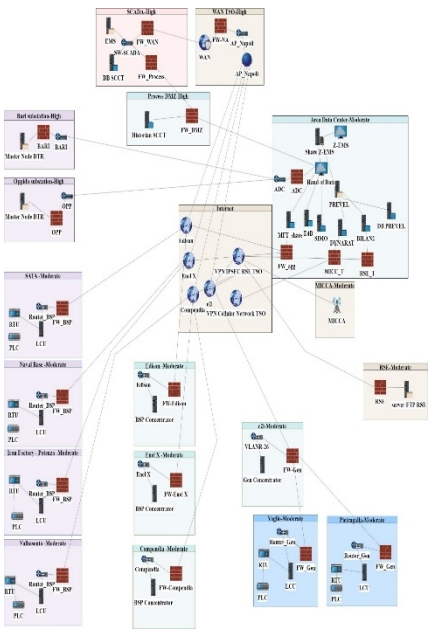
Outputs

- **Quantitative indicators**

Object of investigation

- H2020 European Project: **OSMOSE** (Optimal System-Mix Of flexibility Solutions for European electricity)
- WP 5 (leaded by Terna) on the **congestion management** in the Italian transmission grid
- The congestion management is performed by a **Zonal Energy Management System** that optimizes the use of energy resources connected in a defined geographical zone with periodic updates of the dispatching plans with a 3 hours ahead time-horizon, involving flexible loads and renewable generators
- Extensions to the ICT architecture: new interactions with external actors and the installation of additional components have been analysed under the cyber security perspective
- Involved Areas: TSO control center, TSO substations, Wind Generation Plants, Industrial Loads

Experimental setup



OSMOSE -Demo 5 network diagram

Study Committee D2

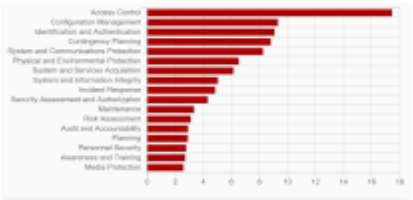
Information Systems and Telecommunication

Paper 10794_2022

HOW TO ASSESS THE CYBERSECURITY POSTURE OF UTILITY INFRASTRUCTURES? A CASE STUDY FROM THE OSMOSE PROJECT continued

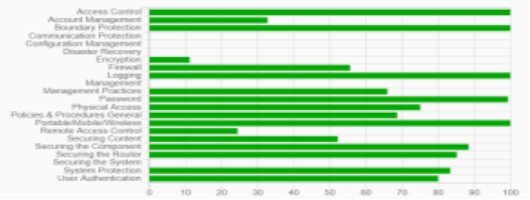
Assessment results

1. Standard compliance analysis



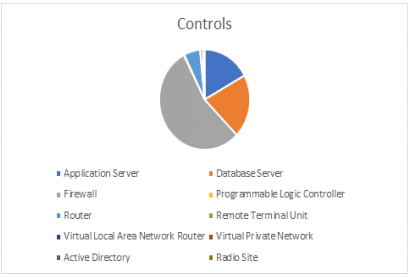
NIST 800-53 cybersecurity controls (SAL-LMM)

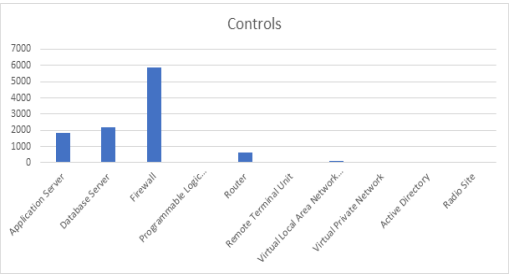
2. Architecture analysis



Percentage of satisfied controls (Intermediate Protection)

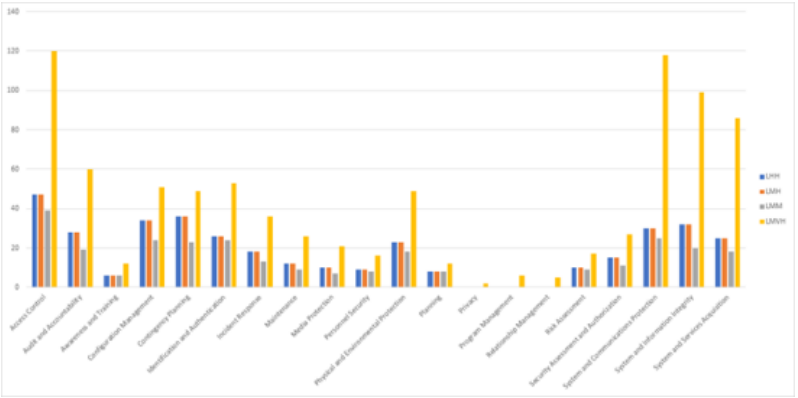
2. Architecture analysis





Percentage of Controls distribution (left) and Number of Controls (right)

3. Scalability analysis



Number of Requirements per category (4 SALs)

Study Committee D2

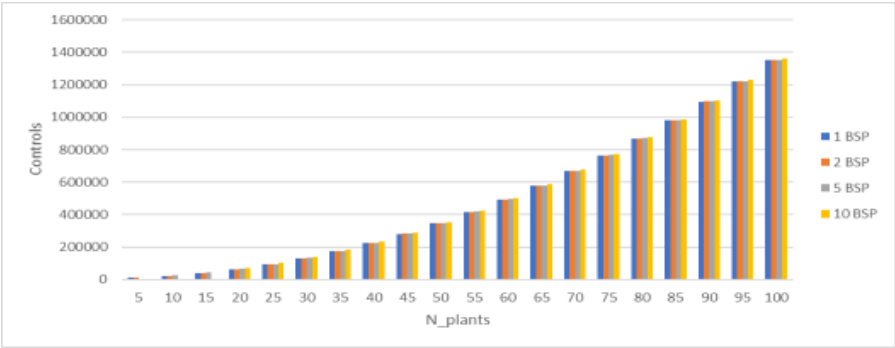
Information Systems and Telecommunication

Paper 10794_2022

HOW TO ASSESS THE CYBERSECURITY POSTURE OF UTILITY INFRASTRUCTURES? A CASE STUDY FROM THE OSMOSE PROJECT continued

Assessment results (cont.)

3. Scalability analysis



Number of Controls varying the Number of Plants (granularity 5 Plants)

Discussion

- The poster presents a security assessment methodology based on the CSET tool and applied to the Demo5 architecture of the OSMOSE European project
- From the standard compliance analysis, a set of prioritized NIST 800-53 security requirements has been derived together with the compliance with given Security Assurance Levels
- From the architecture analysis, the security posture in terms of security controls has been assessed and missing security controls have been identified
- A structured Security Test Plan has been generated based on the security controls from the architecture analysis
- A scalability analysis of the methodology has been performed by defining specific indicators, such as Number of Requirements varying the SAL, Number of Controls varying the Number of Plants
- The results from the scalability analysis showed that the Number of Controls increases quadratically with the number of connected assets

Conclusion

- Given the targets fixed by the energy transition an increasing amount of flexible energy resources are and will be connected to power grids
- Grid observability and controllability require to extend existing ICT infrastructures with new systems and interfaces
- Electric Power Utilities are struggling with the need of adopting suitable methodologies for continuously assessing the cybersecurity posture of their critical infrastructures
- The security assessment methodology presented in the poster exploits the CSET tool features to check the sensitivity of the security requirements and controls varying parameters such as the assurance level and the architecture scale
- The peculiarities of the methodology are a valid support for the application of a graded approach in improving the security maturity level within an organization

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 of the OSMOSE project