Guidelines for Developing a Power-Grid Cybersecurity Database in Europe

George-Călin Seriţan
Department of Measurements, Electrical Apparatus and Static Converters
University Politehnica of Bucharest
Bucharest, Romania
george.seritan@upb.ro

Bogdan-Adrian Enache
Department of Measurements, Electrical Apparatus and Static Converters
University Politehnica of Bucharest
Bucharest, Romania
bogdan.enache2207@upb.ro

Radu Porumb
Electrical Power Systems Department
University Politehnica of Bucharest
Bucharest, Romania
radu.porumb@upb.ro

Daniel Balaci
Network Operation, Maintenance and Development Department,
Transelectrica S.A.
Bucharest, Romania
daniel.balaci@transelectrica.ro

Irina Clima
Department of Digitalization
Societatea Energetica Electrica S.A.
Bucharest, Romania
irina.clima@electrica.ro

Cristinel-Bogdan Bărbulescu
Department of Digitalization
Societatea Energetica Electrica S.A.
Bucharest, Romania
cristinel.barbulescu@electrica.ro

***Abstract*— As the interconnectivity of power grids continues to expand, their susceptibility to cyber threats has also risen sharply. In order to counteract these risks, it's crucial to embrace trustworthy communication protocols and standards that incorporate stringent security safeguards. One feasible approach to confront the escalating cyber threats is creating a cybersecurity database specifically designed for power grid systems. This paper will examine the advantages and challenges of creating such a database and potential strategies for overcoming these challenges.**

Keywords—cybersecurity, power grid, database, database methodology

I. Introduction

The modern power grid is not an isolated island. More and more technologies are being developed and implemented to increase its functionality. With every step, one thing remains constant an increased number of communication devices are now included in the power grid. They influence not only the operation of the grid but also its risk of being targeted by a cybersecurity event [1].

With the adoption of the European Network of Transmission System Operators (ENTSO-E) Agreement on International Cooperation [2], 42 European Transmission System Operators (TSO) from 35 countries are now interconnected, forming one giant power grid spread all over Europe. In this context, one cybersecurity event in one part of the network could negatively affect the entire network.

Now, more than ever, cyber events' increasing scale and impacts on the power grid raise significant concerns [3]. However, information covering threat actors, motives, the technology used, or classified effects is scarce. Several Vulnerability Notes and Alerts are dedicated to power-grid equipment but have limited circulation and require time and effort to access them. Actual cybersecurity events in a power grid can be found on the Industrial Cybersecurity Incidents Database [4]. However, this also needs more information focused more on the targeted company/operator rather than on the nature of the event or the technology involved.

This paper presents and analyses the initial steps to develop a dedicated power-grid cybersecurity database. Because there is no testing methodology available for power-grid cybersecurity and considering its specific needs, the starting points of the study will be the Open-Source Security Testing Manual, Web Security Testing Guide, IEC 60870-5-104, and IEC 61850 standard. These will be analysed and tailored to fit the power grid's nature. Besides this, an extensive literature survey will be done, and exporters from the Romanian TSO and Distribution System Operators (DSO) will be interviewed.

The main contributions of the paper are:

- Extracting the characteristics of a cybersecurity power-grid database considering the available literature and especially the IEC 60870-5 communication standard (Section 2);
- Performing a comparative study between multiple database-developing methodologies and proposing the best suited for cybersecurity events (Section 3);
- Developing a conceptual model for a cybersecurity power grid database (Section 4).

II. Characteristics of a Cybersecurity Database for Power-Grid

A dedicated cybersecurity database would enable centralised monitoring and analysis of potential threats and vulnerabilities within the power grid infrastructure [5 - 8]. This would facilitate timely detection and response to cyberattacks and reduce the potential impact on grid operations. While this concept is not new, it would encourage more effective risk management by enabling organisations to assess and prioritise vulnerabilities based on real-time threat intelligence, ultimately improving the overall security posture of power grids.

Based on the literature survey done [1-3], [5-10], the unique features of a cybersecurity database for power-grid are drawn from three key aspects:

- Focus on power grid infrastructure;
- Industry-specific threat intelligence;
- Regulatory compliance.

First, database development should consider the unique aspects of power grid infrastructure, including power

generation, transmission, and distribution systems, as well as the various communication protocols and devices used in grid operations. Second, only industry-specific threat intelligence, i.e. vulnerabilities in Supervisory Control and Data Acquisition (SCADA) systems, Intelligent Control systems (ICS) components, and power grid-specific protocols like IEC 61850, DNP3, and Modbus, should be considered. Lastly, the collected information should help organisations monitor, assess, and demonstrate compliance with their specific requirements. In this paper, the focus will be only on European legislation compliance.

Based on these pillars, all the information that would be included in the database should fall under at least one of the categories:

- Grid-Specific Vulnerabilities, such as vulnerabilities affecting control systems, substations, and energy management systems.
- Network Topology and Configurations, such as devices, communication protocols, and network topology, to facilitate vulnerability assessments and incident response planning.
- Security Policies and Procedures: The database should store information on the security policies, procedures, and best practices implemented by power grid operators to protect their infrastructure.
- Incidents and Attack Vectors: The database should contain records of past cyberattacks and incidents affecting power grids, including the tactics, techniques, and procedures (TTPs) employed by threat actors and the affected systems and infrastructure. Also, in this category, all the information about planned pen tests performed by involved actors in the energy sector should be considered.

Particular attention should be given to the IEC 60870-5 standard, which focuses on transmission protocols between control centres, substations, and Remote Terminal Units (RTUs) within power grids. Moreover, the IEC 60870-5-104 defines the Application Service Data Units (ASDUs) and the Application Protocol Data Units (APDUs) for SCADA systems over TCP/IP networks.

Despite its potential benefits, implementing the IEC 60870-5-104 standard for cybersecurity in power grids can present several challenges [11-13]. Many power grids are still using older, proprietary communication protocols that may need to be upgraded to support IEC 104 and retrofitting these legacy systems can take time and effort. Also, ensuring interoperability between devices from different vendors that support the IEC 104 standard can be complex due to variations in implementation and interpretation of the standard [14], [15]. All this corroborating and considering the dynamic nature of cyber threats means that more than relying solely on the IEC 104 standard may be required.

Several measures to mitigate these problems were presented in the literature and will be implemented in the proposed database. So, enhancing cybersecurity for IEC 60870-5-104 should consider the following:

- Secure Authentication Mechanisms: The standard supports secure authentication mechanisms, such as challenge-response authentication and digital signatures, to prevent unauthorised access to critical systems.
- Data Integrity and Confidentiality: The IEC 104 protocol can be combined with encryption algorithms like Advanced Encryption Standard (AES) or VPN tunnels to ensure the confidentiality and integrity of sensitive data transmitted between devices.
- Role-Based Access Control: The standard allows for implementing role-based access control (RBAC), which helps restrict user access to specific functions and data within the SCADA system based on their roles and responsibilities.
- Intrusion Detection and Prevention: Using IEC 104 allows for integrating intrusion detection and prevention systems (IDPS) to monitor network traffic, identify potential threats, and take appropriate action to prevent unauthorised access or system compromise.

Analysing the unique aspects of a cybersecurity database led to identifying three major challenges.

- Interoperability and Integration: Power grid systems often comprise various devices, protocols, and technologies. Ensuring interoperability and seamless integration of the cybersecurity database with existing power grid infrastructure can be challenging.
- Real-Time Data Processing: Power grid operations require real-time data processing and analysis for timely threat detection and response. A cybersecurity database for power grids must handle large volumes of data and maintain high-performance levels under varying loads.
- Physical Security Considerations: Unlike a regular cybersecurity database, a power grid-focused database must also consider the physical security aspects of grid infrastructure, as physical attacks or natural disasters can significantly impact grid operations and security.

These challenges can be overcome by adopting a collaborative approach, leveraging existing frameworks, building on open standards, and investing in advanced technologies, ultimately contributing to a more secure and resilient power grid infrastructure.

III. Database Developing Methodologies

Database development methodologies are essential in creating and maintaining robust, efficient, and reliable database systems. These methodologies provide a structured approach to designing, building, and managing databases to meet the organisation's and its users' needs. Starting from well-known strategies, three significant approaches will be analysed in the context of cybersecurity for power grids, and recommendations for different implementation scenarios will be issued.

A. The Waterfall Model

The Waterfall model – Fig. 1, is a traditional, linear methodology that follows a sequential process, starting with requirements analysis and concluding with system maintenance [16]. This approach best suits small, well-defined projects with precise and stable requirements. The stages in the Waterfall model are requirements analysis,

system design, implementation, testing, deployment, and maintenance.

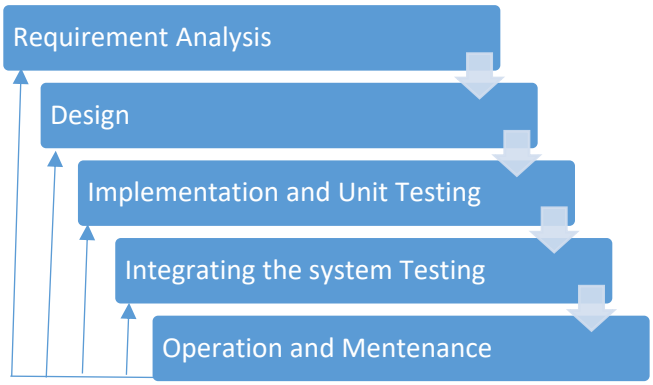

Fig. 1. The waterfall model [14]

The advantages of this methodology lie in its accessibility to understand and manage due to its linear structure and clear milestones and deliverables for each stage. On the other hand, its inflexibility makes it unsuitable for projects with evolving requirements. Also, it can lead to late detection of issues due to the sequential nature of the process.

B. Agile Model

The Agile model – Fig. 2, is an iterative and incremental approach to database development [17]. Agile methodologies, such as Scrum and Extreme Programming (XP), prioritise flexibility, collaboration, and continuous improvement. Developers work on small, manageable tasks in short iterations called sprints, allowing for rapid adaptation to changes in requirements or user feedback.

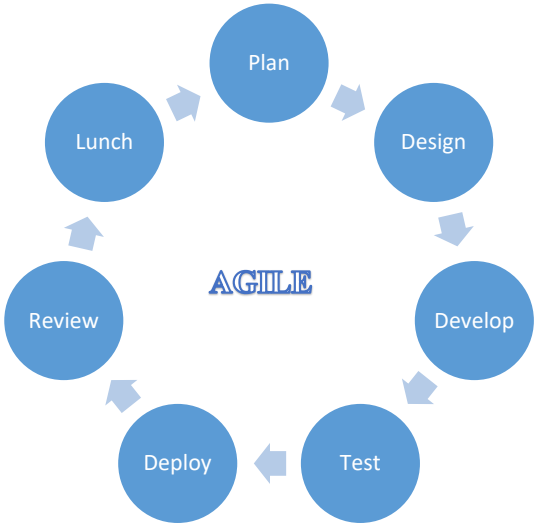

Fig. 2. The Agile Model

Unlike the waterfall model, this methodology is more adaptable to changing requirements and priorities. Also, it increases collaboration and communication among team members and offers early and continuous delivery of functional software components. On the other hand, it requires a high level of stakeholder commitment and involvement and could be more predictable regarding project timeline and cost.

C. The Spiral Model

The Spiral model – Fig. 3, combines Waterfall and Agile methodologies elements, emphasising risk analysis and iterative development [18]. The process consists of four quadrants: identifying objectives, evaluating risks, developing, and testing the system, and planning the next iteration. This methodology is well-suited for large-scale projects with complex and uncertain requirements.

Fig. 3. The spiral model

This methodology emphasises risk management and mitigation, leading to its ability to adapt to changing requirements while maintaining a structured approach. It is well suited for large-scale and complex projects. Its major drawback is that it requires a high level of expertise in risk management which is scarce for cybersecurity experts and can be more difficult and time-consuming than other methodologies.

Choosing the proper methodology for creating a cybersecurity database can be a burden. Considering the project size and complexity, a flexible and iterative approach, such as Agile or Spiral, takes the lead. Still, a Waterfall approach may be appropriate if requirements are well-defined and stable. After carefully considering the significant risks involved, the Spiral methodology, which focuses on risk analysis and mitigation, is the best alternative.

IV. Database Conceptual Model

After the methodology for a cybersecurity database is established, the next step is to develop a conceptual model. This model is more like a four steps action plan that leads to database development. The main aspects are:

- Identifying Stakeholders
- Defining the Scope and Objectives
- Identifying Data Entities and Attributes
- Establishing Relationships and Constraints

The first step in developing a conceptual model is identifying stakeholders, such as utility companies, power grid operators, cybersecurity experts, and regulatory bodies. Their input and requirements will shape the design of the database. After this step, establishing the scope and objectives of the cybersecurity power grid database is crucial to ensure it

meets the needs of its users. Key objectives include threat detection and monitoring, vulnerability assessment, risk management, and regulatory compliance. The next step is to identify the data entities and attributes that will be included in the database. These could include threat intelligence, vulnerability information, incident reports, network configurations, and security policies. Finally, the relationships between data entities and any constraints on these relationships should be defined to ensure data consistency and integrity within the database.

The key components of a cybersecurity power grid database conceptual model are:

- Threat Intelligence: This component encompasses data related to known cyber threats and potential vulnerabilities in power grid systems. Attributes could include threat actor information, attack vectors, targeted systems, and mitigation strategies.
- Vulnerability Information: This component includes data on vulnerabilities identified within power grid infrastructure, such as software flaws, misconfigurations, and hardware weaknesses. Attributes include vulnerability descriptions, severity ratings, affected systems, and remediation guidance.
- Incident Reports: This component comprises data on cybersecurity incidents within power grid systems, providing valuable insights into the tactics and techniques employed by threat actors. Attributes could include incident timestamps, attack methods, impacted systems, and response actions taken.
- Network Configurations: This component contains data on the network architecture and configurations of power grid systems, such as devices, communication protocols, and network topology. This information is critical for vulnerability assessments and incident response planning.
- Security Policies and Procedures: This component includes data on the security policies, procedures, and best practices implemented by power grid operators to protect their infrastructure. Attributes could consist of policy descriptions, implementation guidelines, and compliance status.

The conceptual model can establish relationships between these components and provide a foundation for a cybersecurity power grid database that supports effective threat detection.

V. Conclusions

Developing a cybersecurity database specifically for power grids presents numerous advantages, including centralised monitoring and analysis, enhanced information sharing, improved risk management, and streamlined regulatory compliance. However, challenges such as data privacy and confidentiality, data quality and standardisation, interoperability and integration, scalability and performance, and maintenance and updates must be addressed. These challenges can be overcome by adopting a collaborative approach, leveraging existing frameworks, building on open standards, and investing in advanced technologies, ultimately contributing to a more secure and resilient power grid infrastructure.

This paper presents the first steps towards developing such a database and its characteristics, i.e. focus on power grid infrastructure, industry-specific threat intelligence, and regulatory compliance. Based on the complexity analysis, the implementation methodology should be found on the Spiral design, which focuses on risk analysis and mitigation. The conceptual model for such a database should be based on the following vital components identifying stakeholders, defining the scope and objectives, identifying data entities and attributes and establishing relationships and constraints.

Acknowledgment

This work was supported by the PN-III-P3-3.6-H2020-2020-0202, internal ID 220214299, support program rEsilient and seLf-healed EleCTRical pOwer Nanogrid (ELECTRON), EU H2020 SU-DS04-2018-2020 grant.

References

[1] Krause, T., Ernst, R., Klaer, B., I. Hacker, "Cybersecurity in power grids: challenges and opportunities" in Sensors, 21, (18), 6225, 2021.

[2] " ENTSO-E Vision: A Power System for a Carbon Neutral Europe", 2022, https://vision.entsoe.eu. (accessed on 10.05.2023).

[3] Desarnaud G. "Cyberattacks and energy infrastructure – Anticipating risk", Ifri, 2017, https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf.

[4] Industrial cybersecurity database, https://hub.tisafe.com , (accessed on 10.05.2023).

[5] Cardenas, D.J.S.; Hahn, A.; Liu, C.C, "Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations", in IEEE Access, 2020, 8, 61161–61173.

[6] Krishna, R. R., Priyadarshini, A., Jha, A. V., Appasani, B., Srinivasulu, A., & Bizon, N. "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions" in Sustainability, 2021, 13(16), 9463.

[7] Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. "Challenges and Opportunities in Securing the Industrial Internet of Thing" in IEEE Trans. Ind. Inform. 2020, 17, 2985–2996.

[8] Oproescu, Mihai, et al. "Theory or practice-new trends in Engineering Career." 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE, 2022.

[9] Sun, C. C., Hahn, A., & Liu, C. C. "Cyber security of a power grid: State-of-the-art", International Journal of Electrical Power & Energy Systems, 99, 2018, pp. 45-56.

[10] Sahoo, S., Dragičević, T., & Blaabjerg, F. "Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities.", IEEE Journal of Emerging and Selected Topics in Power Electronics, 9(5), 2019, pp.5326-5340.

[11] Appasani, B.; Mishra, S.K.; Jha, A.V.; Mishra, S.K.; Enescu, F.M.; Sorlei, I.S.; Bîrleanu, F.G.; Takorabet, N.; Thounthong, P.; Bizon, N. "Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions" in Sustainability 2022, 14, 8801.

[12] Jarmakiewicz, J., Parobczak, K., & Maślanka, K. "Cybersecurity protection for power grid control infrastructures" in International Journal of Critical Infrastructure Protection, 2017, 18, 20-33.

[13] Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems" in IEEE Access 2019, 7, 46595–46620

[14] R. Barbosa, R. Sadre and A. Pras, "Flow whitelisting in SCADA networks" in International Journal of Critical Infrastructure Protection vol. 6(3-4), pp. 150–158, 2013.

[15] Ackermann, P. Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems; Packt: Birmingham, UK, 2017.

[16] Connolly, T., & Begg, C. Database Systems: A Practical Approach to Design, Implementation, and Management, Pearson , 2014.

[17] Ambler, S. W., & Sadalage, P. J.Agile Database Techniques: Effective Strategies for the Agile Software Developer, John Wiley & Sons, 2012.

[18] Watt, A. Database Design - 2nd Edition, BCCampus, 2014.