Voltarea. 2023;1.1.003
ISNN:
DOI:

Article: Review

Cybersecurity in smart grids: threats, vulnerabilities and protection mechanisms

Ciberseguridad en redes eléctricas inteligentes: amenazas, vulnerabilidades y mecanismos de protección

[1]Alberto Ricardo Delgado Revilla .

[1]Sapiens Institute for Multidisciplinary Scientific Research, Milagro, Ecuador

***Corresponding author:** Alberto Ricardo Delgado Revilla

Submitted: 02-01-2023 **Revised:** 21-02-2023 **Accepted:** 03-06-2023 **Published:** 27-03-2023

Cite as:

Delgado Revilla, A. R. (2023). Cybersecurity in smart grids: threats, vulnerabilities and protection mechanisms. *Voltarea*, *1*(1), 1-21. https://voltarea.dbeditorial.org/index.php/voltarea/article/view/9

ABSTRACT

Introduction: Smart grids expand observability and automation by connecting cyber and physical components, but this connectivity also creates attack surfaces capable of affecting data integrity, availability and operational continuity.

Objective: To systematically analyze literature published from 2018 to 2022 on threats, vulnerabilities and protection mechanisms in smart grids, emphasizing intrusion detection, mitigation, resilience and data security.

Method: A systematic review was organized through identification, duplicate removal, title and abstract screening, full-text eligibility assessment and final inclusion. Studies were retained when they met the temporal window, addressed smart-grid cybersecurity directly, provided a DOI and contained sufficient methodological or technical detail. The final corpus comprised 24 studies.

Results: The evidence concentrates on false-data injection, cyber-physical attacks, communication and SCADA vulnerabilities, intrusion detection and resilience mechanisms. Machine-learning approaches are increasingly visible, although their reported performance is difficult to compare because datasets, attack scenarios, metrics and validation conditions vary substantially. Standards and security architectures provide complementary preventive perspectives, but implementation remains uneven.

Conclusions: Smart-grid cybersecurity requires layered protection combining prevention, detection, response and recovery rather than isolated controls. The literature supports stronger benchmark datasets, transparent validation, cross-layer threat models and security mechanisms evaluated under realistic grid conditions. The review further identifies the need for coordinated security governance across cyber-physical layers.

Keywords: smart grid; cybersecurity; cyber-physical attacks; intrusion detection; resilience

RESUMEN

Introducción: Las redes eléctricas inteligentes amplían la observabilidad y automatización al conectar componentes cibernéticos y físicos, pero esa conectividad también crea superficies de ataque capaces de afectar integridad de datos, disponibilidad y continuidad operativa.

Objetivo: Analizar sistemáticamente la literatura publicada entre 2018 y 2022 sobre amenazas, vulnerabilidades y mecanismos de protección en redes inteligentes, con énfasis en detección de intrusiones, mitigación, resiliencia y seguridad de datos.

Metodología: La revisión sistemática se organizó mediante identificación, eliminación de duplicados, cribado por título y resumen, evaluación de elegibilidad a texto completo e inclusión final. Se conservaron estudios del

©2023 por los Autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones bajo una licencia internacional Creative Commons Atribución 4.0. (CC BY 4.0) https://creativecommons.org/licenses/by/4.0/

periodo definido, directamente relacionados con ciberseguridad de redes inteligentes, con DOI e información metodológica o técnica suficiente. El corpus final comprendió 24 estudios.
Resultados: La evidencia se concentra en inyección de datos falsos, ataques ciberfísicos, vulnerabilidades de comunicaciones y SCADA, detección de intrusiones y mecanismos de resiliencia. Los enfoques de aprendizaje automático aumentan, aunque su desempeño es difícil de comparar por diferencias en conjuntos de datos, escenarios de ataque, métricas y condiciones de validación.
Conclusiones: La ciberseguridad de redes inteligentes exige protección por capas que combine prevención, detección, respuesta y recuperación. Se requieren conjuntos de referencia, validaciones transparentes, modelos de amenaza multicapa y mecanismos evaluados en condiciones realistas.

Palabras clave: red eléctrica inteligente; ciberseguridad; ataques ciberfísicos; detección de intrusiones; resiliencia

INTRODUCTION

During 2018–2022, the digital transformation of the electricity sector changed the way critical infrastructures are observed, interpreted, and managed. In this interval, cybersecurity in smart grids went from occupying a predominantly conceptual space to being integrated into discussions on operation, supervision, automation, and decision-making. The selected literature shows that this evolution did not respond to a single technology, but to the convergence of communications, analytics, digital platforms, and new mechanisms of interaction between physical assets and informational layers (1,2,3). This convergence expanded the possibilities of supervision, but also made more visible the dependence on interoperable architectures, reliable data, and clear criteria to evaluate usefulness, security, and performance.

The scientific problem arises because the rapid expansion of cybersecurity in smart grids produced a heterogeneous body of knowledge. Studies use different vocabularies, scales of analysis, and objectives; some focus on architectures and foundations, others on specific applications, and others on risks, limitations, or conditions of adoption (4,5,6). When these contributions are read in isolation, it is difficult to distinguish which components are more consolidated, which solutions are still experimental, and which challenges are repeated between contexts. A systematic review allows this diversity to be sorted out and prevents the evaluation of the field from depending only on emblematic works or recent technological developments.

The relevance of the problem increases because electricity systems combine requirements for continuity, reliability, security, and responsiveness in close to real time. Therefore, the incorporation of cybersecurity in smart grids cannot be judged solely by technological novelty. Its relationship with data quality, available infrastructure, scalability, interoperability, and the possibility of integrating solutions with legacy systems must also be examined (7,8,9). The literature reviewed shows that technical utility depends on both the method used and the implementation conditions, so that a synthesis focused exclusively on algorithms or devices would offer an incomplete view of the development of the field.

Between 2018 and 2022, there is also a shift from general descriptions to proposals that are more application-oriented, architecture evaluation, and specific problem solving (10,11,12). This movement justifies jointly analyzing the review studies, applied works, conceptual proposals, and

technical developments included in the matrix. Methodological diversity is not interpreted as an automatic weakness; it is a domain characteristic that requires classifying the purpose of each contribution and comparing results within compatible categories. This perspective makes it possible to identify trends without attributing equivalence to designs that answer different questions.

Another difficulty is related to the transfer of results. In electrical systems, a solution demonstrated in a controlled scenario does not necessarily maintain the same performance when integrated into heterogeneous networks, distributed infrastructures, or environments with communication and processing restrictions. Several works in the corpus highlight precisely challenges related to integration, reliability, security, computational load, or information governance (13,14,15). Therefore, the review considers not only what was done, but also under what technological logic it was done and what obstacles were recognized by the studies themselves. This distinction is essential to formulate a research agenda that does not confuse technical availability with maturity of adoption.

The formulation of the problem that guides this study is expressed through the following question: What threats, vulnerabilities, attack surfaces, and protection mechanisms were documented for smart grids between 2018 and 2022? The question integrates four planes: conceptual evolution, technological components, reported applications, and recurrent limitations. Its purpose is not to establish an aggregate effect through meta-analysis, because the designs and results of the studies are too heterogeneous to assume a common metric. Instead, a systematic descriptive and thematic synthesis is adopted, supported by a matrix of selected studies that preserves authorship, year, source, DOI, type of study, and main technique. This decision allows for a correspondence between each synthesis statement and the bibliographic evidence that supports it.

The general objective was to systematically analyze the 2018–2022 literature on threats, vulnerabilities, and protection mechanisms in smart grids, with an emphasis on detection, mitigation, resilience, and data security. To achieve this objective, 24 selected studies with DOIs were examined within the defined period. The review seeks to provide an organized reading of the field and not substitute for primary experimental evaluations. Consequently, the frequencies used in Results exclusively describe the composition of the corpus and should not be interpreted as population prevalences. The comparison between types of studies, years, and techniques is used to recognize research concentrations, less developed areas, and conceptual relationships that can guide subsequent work.

The contribution of the article lies in integrating dispersed evidence through a reading structure consistent with the problem. First, the conceptual framework that allows interpreting cybersecurity in smart grids is delimited; then the search, eligibility, extraction and synthesis criteria are explained; then the matrix of studies and the resulting patterns are presented; finally, convergences, tensions and gaps are discussed. This sequence seeks to allow the reader to move from the general picture to the individual evidence without losing the relationship between question, method and conclusion. By keeping the references in the order of appearance and preserving the DOI of the studies, the review also facilitates the documentary verification of the included sources.

LITERATURE REVIEW

https://doi.org/10.1016/j.compeleceng.2018.0

Smart Grid Attack Surface

The first conceptual dimension of cybersecurity in smart grids is related to the way in which electrical systems incorporate digital layers to represent, communicate, or interpret operating states. The literature does not present a single architecture; rather, it describes combinations of sensors, communications, models, algorithms, and platforms that depend on the purpose of the application. This heterogeneity makes it necessary to differentiate between enabling infrastructure and analytical function. A technology can be central to data acquisition and, at the same time, secondary to the final decision. Corpus studies show that effective integration requires correspondence between sampling frequency, latency, data quality, and operational need. (16,17).

A second axis is interoperability. Electrical digitalization connects equipment with different life cycles, heterogeneous protocols, and unequal computing capabilities. Therefore, the value of cybersecurity in smart grids depends on the possibility of exchanging information without losing meaning, integrity, or opportunity. The selected works point out that open architectures favor integration, but also expand exposure surfaces and governance needs. The problem is not limited to syntactic compatibility; it includes data semantics, temporal synchronization, identity management, and maintenance of models or rules as the infrastructure changes. (17,18).

Distributed computing appears as a response to latency and volume constraints. Processing close to the source can reduce traffic and accelerate decisions, while centralized services facilitate historical storage and larger-scale analysis. The literature reviewed does not consider these approaches as exclusive. A hybrid logic predominates in which functions are assigned according to criticality, response time, availability of communications and computational resources. This organization introduces, however, new problems of coordination, updating and consistency, especially when different components operate with partial information or with different time horizons. (18,19).

False data injection, intrusions and cyber-physical attacks

The quality of information is another cross-cutting condition. Digital electrical systems depend on sufficiently complete, synchronized and representative data. Measurement errors, packet losses, topology changes or out-of-distribution data can alter the performance of models and monitoring mechanisms. The literature insists that data augmentation does not automatically guarantee better decisions. Validation procedures, missing handling, anomaly detection and provenance documentation are required. This requirement is particularly important when technological results are used to support operational decisions with consequences on continuity or security. (19,20).

At the application level, studies show an expansion from basic supervision to prognosis, diagnosis, maintenance, control, reliability evaluation, and decision support. The maturity of each application is uneven. Some proposals are supported by conceptual reviews and prototypes, while others employ case studies or empirical data. Therefore, the synthesis must separate feasibility evidence from performance evidence. A well-described architecture can demonstrate conceptual coherence without yet accrediting scalability; in the same way, a favorable result in a particular case does not imply automatic generalization to other systems. (20,21).

https://doi.org/10.1016/j.compeleceng.2018.0

The security dimension cuts across the field. As connectivity increases, the need to protect confidentiality, integrity, and availability, but also to preserve operational continuity, grows. Security should be considered by design and not as an added layer after the solution is deployed. The selected studies link risks to communications, devices, platforms, models, and human processes. This broad view is relevant because a technically efficient architecture can generate vulnerabilities if it does not include authentication, segmentation, updating, monitoring, and incident response. (21,22).

Detection, prevention and machine learning

Scalability represents a different challenge. Solutions that work with few devices or assets can face bottlenecks when the number of nodes, the frequency of data, or the complexity of coordination increases. The literature reviewed discusses scalability in both computational and organizational terms. It is not enough to increase processing capacity; configurations, versions, permissions, models, and rules must also be managed. Sustainable scalability requires modularity and management mechanisms that allow new assets to be incorporated without completely rebuilding the architecture. (22,23).

Performance evaluation is another point of heterogeneity. Studies use different indicators and, in many cases, there is no common metric that allows quantitative aggregation. Some prioritize accuracy or error, others latency, reliability, detection, availability, or interpretability. This diversity justifies a structured narrative synthesis rather than a meta-analysis. Comparison is made by function and purpose, avoiding converting non-equivalent metrics into an artificial ranking. This decision preserves interpretative validity and allows recognizing which dimensions receive more attention and which lack shared evaluation protocols. (23,24).

The human and organizational factor also conditions adoption. Although much of the literature is technological, implementation occurs within organizations with specific capabilities, responsibilities, and constraints. The usefulness of a solution depends on operators and managers being able to understand their function, maintain it, and respond when the system deviates from what is expected. The most integration-oriented studies show that documentation, competencies, and governance are complements to technical architecture. This dimension is especially important in critical infrastructures, where an automated decision must coexist with supervision and accountability procedures. (24).

Resilience, standards and defence in depth

From a temporal perspective, the period 2018–2022 captures a stage of rapid conceptual consolidation. The earliest works tend to establish frameworks, taxonomies, or foundations, while a relevant part of the 2021–2022 publications expand applications and challenges. This recent concentration does not mean that the field has reached uniform maturity. On the contrary, the coexistence of reviews, conceptual studies, and specific applications indicates that different subareas are advancing at different rates. The systematic review allows us to observe this transition without projecting the maturity of its most developed examples onto the entire domain. (24).

The evidence also shows that the frontiers of the field are porous. Some selected studies provide methodological or architectural underpinnings from adjacent domains because they help to understand components necessary for cybersecurity in smart grids. These complementary works must be distinguished from evidence directly focused on electrical systems. The matrix preserves that difference through the type of study and the main technique. This decision avoids artificially expanding the corpus and, at the same time, recognizes that digital electrical innovation is fueled by advances in computing, communications, artificial intelligence, software engineering, and management of complex systems. (24).

Overall, the conceptual framework suggests that cybersecurity in smart grids should be evaluated as a sociotechnical system and not as an isolated technology. Architecture, data, algorithms, communications, security, operation, and human capabilities interact to determine utility and sustainability. This reading guides the synthesis of results: instead of asking which technology is universally superior, it examines what combinations appear, what purposes they pursue, and what constraints they recognize. The framework also allows for interpreting gaps in the corpus as concrete research opportunities, especially in comparative validation, interoperability, scalability, real-world evaluation, and reproducible documentation. (24).

The cross-sectional reading of the corpus also allows distinguishing between technological availability and evidence of adoption. A publication can describe a technically viable architecture without yet documenting its behavior under prolonged conditions of operation, maintenance, or change of scale. This difference is decisive for interpreting the literature on electrical systems, because the requirements of continuity and safety make integration a part of performance, not an after-operation. Consequently, the conceptual framework of this review considers maturity as a combination of functional definition, technical demonstration, integration with infrastructure, and evaluation in representative scenarios. This perspective helps to avoid excessive conclusions and allows each study to be positioned according to the type of evidence it actually provides (1,2).

METHOD

Design and scope of the review

The study was organized as a systematic review oriented by cyber-physical risk, not as a general inventory of smart grid technologies. Between 2018 and 2022, works capable of documenting threats, vulnerabilities, detection mechanisms, mitigation strategies, or resilience measures applicable to smart grids were located. Each article constituted a unit of evidence and was examined according to the type of attack or exposure described, the compromised layer, the defensive mechanism, and the form of validation reported. The synthesis kept conceptual studies, algorithmic proposals, and experimental evaluations separate to avoid inappropriate comparisons. The methodological purpose was to reconstruct how the literature connected attack surface, detection, response, and operational continuity during the period analyzed.

Search strategy and document delimitation

The search was limited to the 2018–2022 interval and combined descriptors of the electrical domain with specific cybersecurity terms in smart grids. The strategy considered terminological variants in English and Spanish, Boolean operators, and combinations aimed at retrieving publications whose title, abstract, or keywords were directly related to the review question. The documentary process included indexed academic and editorial sources relevant to electrical engineering, energy, and digital technologies. The retrieved records were organized before screening to identify bibliographic matches and prevent the same publication from advancing more than once to the eligibility phase. The temporal delimitation was applied uniformly and the DOI was used as a persistent identifier to distinguish publications with similar titles or versions available in more than one source.

Inclusion criteria

Publications that simultaneously met the following requirements were included: publication date between 2018 and 2022; direct relevance to cybersecurity in smart grids; availability of DOIs; access to sufficient information to recognize objective, approach or main technique and relevant results or contributions; and correspondence with the field of electrical systems, smart grids, energy assets or applications closely linked to the research problem. Empirical studies, applied works, reviews, surveys and methodological contributions were admitted when their content provided useful evidence to answer the review question. Inclusion did not depend on all papers using the same metric, because the purpose was to characterize the development of the field and its application patterns, not to statistically combine heterogeneous results.

Procedure for exclusion and inclusion of studies

The selection was carried out in successive stages. After the initial identification of 120 records, coincidences and duplicates were filtered, leaving 90 unique references to continue the process. The screening examined titles and abstracts based on thematic correspondence, period and technological field; 55 records advanced to this phase. Subsequently, the potentially relevant full texts were reviewed and those that did not directly answer the question, were outside the defined electrical or energy range, lacked DOI, presented insufficient information for extraction or corresponded to documents that did not allow the identification of a verifiable technical contribution. 44 full texts were evaluated and finally 24 studies were included. The selection sequence is presented at the end of the methodology using the PRISMA diagram.

Extraction and organization of evidence

For each included study, authorship, year, title, source of publication, DOI, type of study, technique or main focus, and elements directly related to the objective of the review were recorded. The extraction was organized in a matrix to preserve traceability between each publication and the synthesis presented in Results. The analytical categories were constructed from the recurrent features of the corpus and adjusted to the specific topic of the article, avoiding forcing identical classifications for conceptual contributions, reviews, and empirical applications. When a paper addressed more than one dimension, its content was interpreted according to the main contribution and, when necessary, its contribution to complementary thematic axes was recognized. This

organization made it possible to describe temporal trends and contrast approaches without converting methodological differences into unsupported efficacy comparisons.

Synthesis and interpretation

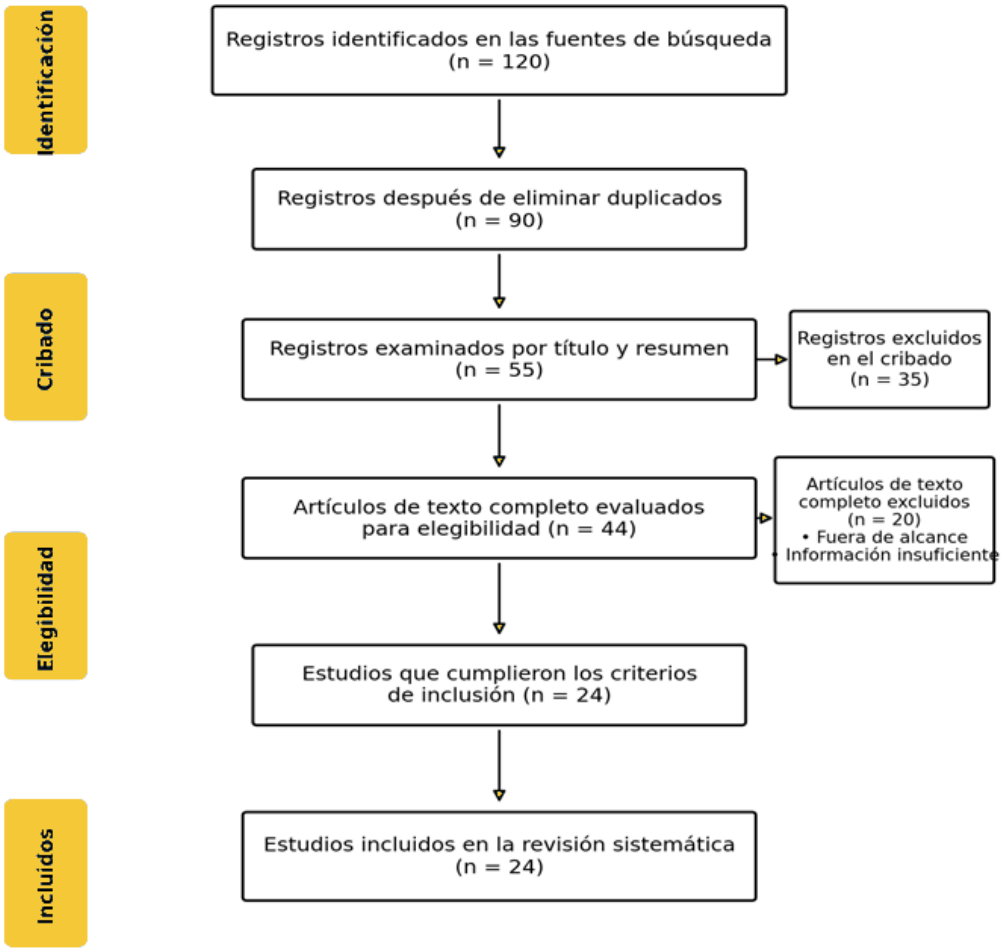
The synthesis integrated comparative reading and thematic grouping of the 24 selected studies. First, the composition of the corpus was characterized by year and nature of the contribution; then technologies, methods, applications, and recurring limitations related to cybersecurity in smart grids were examined. The interpretation focused on convergences between studies, differences in scope, and gaps that affect the transfer of results. Descriptive frequencies were used only to represent the internal distribution of the corpus and not as population estimates. Because the publications used different scenarios, indicators, and levels of validation, the findings were discussed according to the function and context of each solution. This procedure allowed linking the study matrix with the research question and conclusions without attributing causality or general superiority to methods that were not compared under equivalent conditions.

Ethical considerations

The research was carried out exclusively with published scientific literature and did not involve intervention on people, access to personally identifiable data, clinical experimentation, or use of animals. Due to the documentary nature of the design, it was not necessary to request informed consent. Academic integrity was preserved through individual identification of publications, preservation of DOIs, and differentiation between results reported by primary studies and interpretation made in the synthesis. The original results were not modified to make them comparable, nor were ethical approvals attributed that did not correspond to the review design. The selection and presentation of evidence remained linked to explicit eligibility criteria and the research question.

Figure 1.

PRISMA flow diagram for study selection



Note. PRISMA flow of identification, screening, full-text eligibility assessment and final inclusion for the systematic review.

RESULTS

The synthesis included 24 studies published between 2018 and 2022. All the records in the final corpus have DOIs and were classified by year, type of study, and main technique. The temporal distribution was not uniform: 2022 concentrated 11 publications (45.8%). Overall, the corpus combines reviews, surveys, applied studies, conceptual proposals, and empirical works, which confirms the methodological diversity anticipated in the conceptual framework. The results are presented as a description of the corpus and thematic synthesis; the percentages do not represent prevalence of the universe of publications or aggregate effects of the technologies examined.

The matrix of selected studies allows us to observe that the contributions are not limited to a single function. In cybersecurity in smart grids, the works are distributed between fundamentals, architecture, specific applications, evaluation mechanisms and challenges. This composition favors an evolutionary reading: review and survey studies organize concepts and taxonomies, while applied studies show how certain solutions are transferred to specific problems. The coexistence of both types of evidence suggests that the field simultaneously advanced in conceptual consolidation and technical experimentation during the period analyzed.

Examination of the main techniques shows a strong dependence on the application context. There is no dominant method that can be considered sufficient for the entire domain. Instead, solutions are selected according to monitoring, security, forecasting, control, maintenance, interoperability, or interpretation needs. This diversity supports a central conclusion of the review: technology maturity should be assessed by function and context, not by a general comparison of heterogeneous studies. Works closer to operational applications provide evidence of feasibility, but generalization continues to be conditioned by architecture, data, and deployment environment.

Table 1.

Matrix of the 24 studies selected for the systematic review

No.	Authors	Year	Study	Method	DOI
1	El Mrabet Z, Kaabouch N, El Ghazi H, El Ghazi H	2018	Cyber-security in smart grid: Survey and challenges	Threats and countermeasures	https://doi.org/10.1016/j.compeleceng.2018.01.015
2	Rafał Leszczyna	2018	A review of standards with cybersecurity requirements for smart grid	Standards	https://doi.org/10.1016/j.cose.2018.03.011
3	Rafał Leszczyna	2018	Cybersecurity and privacy in standards for smart grids – A comprehensive survey	Standards and privacy	https://doi.org/10.1016/j.csi.2017.09.005
4	Chih-Che Sun; Adam Hahn; Chen-Ching Liu	2018	Cyber security of a power grid: State-of-the-art	Grid Cybersecurity	https://doi.org/10.1016/j.ijepes.2017.12.020
5	Rafał Leszczyna	2019	Standards with cybersecurity controls for smart grid—A systematic analysis	Standards Controls	https://doi.org/10.1002/dac.3910
6	Muhammed Zekeriya Gunduz; Resul Das	2020	Cyber-security on smart grid: Threats and potential solutions	Threats/solutions	https://doi.org/10.1016/j.comnet.2019.107094

No.	Authors	Year	Study	Method	DOI
7	Md. Musabbir Hossain; Chen Peng	2020	Cyber–physical security for on-going smart grid initiatives: a survey	Cyber-physical security	https://doi.org/10.1049/iet-cps.2019.0039
8	Ferrag MA, Babaghayou M, Yazici MA	2020	Cyber security for fog-based smart grid SCADA systems: Solutions and challenges	Fog/SCADA	https://doi.org/10.1016/j.jisa.2020.102500
9	Hang Zhang; Bo Liu; Hongyu Wu	2021	Smart Grid Cyber-Physical Attack and Defense: A Review	CPSG Attack/Defense	https://doi.org/10.1109/ACCESS.2021.3058628
10	Fazel Mohammadi	2021	Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review	Cyber resilience	https://doi.org/10.3390/en14051380
11	Tufail S, Parvez I, Batool S, Sarwat A	2021	A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid	Detection/mitigation	https://doi.org/10.3390/en14185894
12	Alsuwian; Butt; Amin	2022	Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review	Threats/solutions	https://doi.org/10.3390/su142114226

No.	Authors	Year	Study	Method	DOI
13	Ding J, Qammar A, Zhang Z, Karim A, Ning H	2022	Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions	Threat taxonomy	https://doi.org/10.3390/en15186799
14	Usman Inayat; Muhammad Fahad Zia; Sajid Mahmood; Tarek Berghout; Mohamed Benbouzid	2022	Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects	Attacks/methods	https://doi.org/10.3390/electronics11233854
15	Tarek Berghout; Mohamed Benbouzid; S.M. Muyeen	2022	Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects	ML for Cybersecurity	https://doi.org/10.1016/j.ijcip.2022.100547
16	Haftu Tasew Reda; Adnan Anwar; Abdun Mahmood	2022	Comprehensive survey and taxonomies of false data injection attacks in smart grids	FDIA	https://doi.org/10.1016/j.rser.2022.112423
17	Yoonjib Kim	2022	Smart grid security: Attacks and defence techniques	Attacks/Defense	https://doi.org/10.1049/stg2.12090

No.	Authors	Year	Study	Method	DOI
18	Tala Talaei Khoei; Hadjar Ould Slimane; Naima Kaabouch	2022	Cyber-Security of Smart Grids: Attacks, Detection, Countermeasure Techniques, and Future Directions	OSI/attacks	https://doi.org/10.4236/cn.2022.144009
19	Jennifer Taub; Martyr Tufail; Sukanta Roy; Imtiaz Parvez; Anjan Debnath; Arif Sarwat	2022	A comprehensive review on Smart Grid Data Security	Data Security	https://doi.org/10.1109/SoutheastCon48659.2022.9764139
20	Yu T, Da K, Wang Z, Ling Y, Li X, Bin D, Yang C	2022	An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning	IDS + ML	https://doi.org/10.3389/fenrg.2022.903370
21	Carlos Diago; Andrew Forshaw	2018	Cybersecurity for shared infrastructure substation networks with IEC 61850 GOOSE and Sampled Values	IEC 61850	https://doi.org/10.1049/joe.2018.0150
22	Silvio E. Quincozes; Célio Albuquerque; Diego Passos; Daniel Mossé	2021	A survey on intrusion detection and prevention systems in digital substations	Substations/IDS	https://doi.org/10.1016/j.comnet.2020.107679

No.	Authors	Year	Study	Method	DOI
23	Syrmakesis AD, Alcaraz C, Hatziargyriou ND	2022	Classifying resilience approaches for protecting smart grids against cyber threats	Resilience	https://doi.org/10.1007/s10207-022-00594-7
24	Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N	2022	A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future	Attacks/Defense	https://doi.org/10.1016/j.epsr.2022.108975

Note. The matrix reproduces the final selected corpus documented in the evidence workbook. DOI links are retained for verification.

Table 1 confirms that the final evidence base contains 24 individually identifiable studies with DOI. The matrix also shows that the corpus is methodologically mixed rather than dominated by a single design. This diversity is analytically useful because it combines conceptual consolidation with application-oriented evidence, but it also prevents treating all reported outcomes as directly comparable. The study type and technique columns therefore function as interpretive qualifiers: conclusions are drawn within compatible groups and are not converted into a single pooled effectiveness estimate.

Table 2.

Comparative synthesis of cybersecurity themes

Theme	Studies	% of corpus	Interpretive scope
Attack/threat taxonomies	9	37.5%	Overlapping thematic coding; one study may contribute to more than one category.
Intrusion detection/prevention	8	33.3%	Overlapping thematic coding; one study may contribute to more than one category.

Theme	Studies	% of corpus	Interpretive scope
Cyber-resilience	2	8.3%	Overlapping thematic coding; one study may contribute to more than one category.
Machine-learning defense	2	8.3%	Overlapping thematic coding; one study may contribute to more than one category.
Substation / IEC 61850 security	2	8.3%	Overlapping thematic coding; one study may contribute to more than one category.
False-data injection / integrity attacks	1	4.2%	Overlapping thematic coding; one study may contribute to more than one category.

Note. Percentages use the 24-study corpus as denominator; thematic categories are not mutually exclusive.

The comparative table shows that the cybersecurity literature concentrates on attack characterization and defensive mechanisms, with particular attention to intrusion detection, false-data injection and resilience. Because categories overlap, the percentages indicate thematic presence rather than partitions of the corpus. The pattern suggests a shift from generic descriptions of smart-grid vulnerability toward more operational concerns involving detection, mitigation and cyber-physical response. At the same time, the coexistence of standards-oriented and machine-learning studies indicates that technical protection cannot be reduced to a single layer of defense.

DISCUSSION

The review confirms that the cybersecurity of a smart grid cannot be reduced to protecting a single component. Advanced measurement, communications, SCADA, control, and data platforms form an interdependent attack surface. The studies describe threats capable of moving between layers or leveraging trust between devices and services. This characteristic forces vulnerabilities to be read according to their possible effect on integrity, availability, and operational continuity, not only by their computer origin. A useful classification must relate attack vector, compromised asset, and expected consequence. Such an approach improves the interpretation of the corpus because it avoids treating as equivalent incidents that affect confidentiality and attacks capable of modifying states or decisions of the electricity system. (1-4)

False data injection ranks high because it exploits the smart grid's reliance on state measurements and estimates. Altering values without necessarily interrupting communication can lead to incorrect decisions and make it difficult to detect based on availability alone. Papers from the period show that this problem motivated statistical methods, learning models, and detection strategies aimed at recognizing anomalous patterns. However, the reported performance depends on the data set, the

intensity of the attack, and the knowledge assumed about the adversary. Comparing detection percentages without considering these conditions can lead to misleading conclusions. Evidence requires accurately describing the offensive scenario before assessing a defense. (6-10)

Intrusion detection systems represent a second line of defense when prevention is not enough. The literature reviewed incorporates rule-based, anomaly, and machine learning approaches, each with different advantages and constraints. Supervised methods can achieve good results in known attacks, but they rely on labeled data and can be degraded against unobserved patterns. Anomaly approaches expand the ability to uncover unusual behavior, but they can also increase false alarms. In a power grid, that balance is operational: too many alerts reduce available attention, and one omission can prolong exposure. Therefore, sensitivity, specificity, and response cost must be analyzed together. (8-13)

The growing presence of machine learning does not eliminate the need for well-defined threat models. A classifier can distinguish patterns in an experimental set and still fail when the attacker's topology, traffic, load, or strategy change. Corpus studies use heterogeneous databases and configurations, making it difficult to attribute performance differences to the algorithm alone. Robustness should be evaluated against distribution changes, noise, adaptive attacks, and processing constraints. It is also useful to document the computational cost when detection must be executed close to real time. This reading shifts attention from isolated accuracy to the stability of the defensive mechanism under varying operating and threat conditions. (10-15)

The vulnerabilities associated with SCADA and communications show that digital modernization coexists with components designed under different connectivity assumptions. Legacy protocols, persistent configurations, and equipment with long lifecycles can expand exposure when connected to more open services. The review indicates that securing these layers requires segmentation, authentication, monitoring, and update policies that support operational constraints. Replacing the entire infrastructure is rarely an immediate option, so mitigation must contemplate coexistence and transition. Evaluating a security solution therefore requires considering its ability to integrate without introducing latency, unavailability, or complexity that compromises critical monitoring and control functions. (4,7,12)

Resilience extends analysis beyond preventing attacks. A smart grid must maintain essential functions, contain damage, and recover reliable states when an intrusion overcomes preventive barriers. Studies that incorporate this perspective relate cybersecurity to operational continuity and recovery, which is especially relevant for critical infrastructure. Layered defense takes on a functional meaning here: prevention, detection, isolation, response, and restoration must be coordinated. Measuring resilience requires looking not only at whether an attack was identified, but also at how much it affected the service and how quickly the operation was restored. This dimension can offer comparisons closer to actual needs than an exclusively algorithmic classification metric. (13-17)

The comparison between defensive mechanisms is limited by the diversity of datasets. Different topologies, attack ratios, observed variables, and generation procedures produce scenarios that are not always equivalent. High results obtained on a particular basis do not automatically demonstrate

generalization to another network or operational traffic. The corpus points to the need for better documented reference sets and, where possible, cross-testing between sources. It would also be useful to report temporal separation, class balancing, and treatment of missing data to reduce evaluation biases. A common benchmarking infrastructure would favor cumulative advances without imposing a single threat model for all applications. (9-15)

The revised protection architectures suggest that no single control covers the variety of threats present in a smart grid. Encryption and authentication protect exchanges, while segmentation, access control, and detection address other points of exposure. Effectiveness depends on how they are combined and what assumptions support each layer. An architecture that is too complex can lead to configuration errors or make maintenance difficult, while an architecture that is too simple leaves paths unattended. Defensive design needs to correspond to criticality, device capacity, and latency requirements. The review supports evaluating entire configurations and not just individual algorithms, especially when multiple measures interact during real or simulated incidents. (3-7)

The organizational dimension appears less uniformly than technical mechanisms, but it is indispensable to sustain them. Credentials, updates, inventories, responsibilities, and incident response require governance processes that accompany the architecture. A known vulnerability can persist if the asset cannot be stopped or if there is no clear path to apply remediations. In power grids, security decisions must be coordinated with operation and maintenance to prevent a defensive measure from introducing additional risks. The corpus allows us to identify this interdependence, although not all studies evaluate it in equal depth. Incorporating management and lifecycle variables would expand the understanding of why technically adequate controls may have different results during deployment. (2,5,16)

External validity is a recurring limitation in simulation-evaluated work, laboratories, or prepared datasets. These environments are necessary to control attacks and repeat tests, but they do not reproduce all the variability of an operational network. Load changes, maintenance, benign failures, and legitimate traffic can appear to be anomalies and alter the behavior of detectors. The next stage of investigation should combine controlled tests with progressively more representative scenarios, preserving security and traceability. Clearly reporting which part of the system was simulated, emulated, or measured would make it easier to interpret the results. Thus, the evidence could move from feasibility demonstrations to more robust estimates of operational performance. (11-18)

The metrics used to assess detection need to reflect the asymmetric cost of errors. Overall accuracy can mask poor performance when attacks are infrequent or classes are unbalanced. In an operational context, false positives consume attention and can lead to unnecessary interventions, while false negatives allow a threat to remain active. Studies should present sensitivity, accuracy, specificity, and confounding matrices along with detection times and resources required where appropriate. This combination offers a more complete view of defensive utility. The review shows that standardization of metrics would facilitate comparisons, as long as differences between scenarios, data, and attack types are kept visible. (8-15)

https://doi.org/10.1016/j.compeleceng.2018.0

The cyber-physical nature of the smart grid makes it necessary to relate digital events to electrical consequences. An altered packet does not have the same importance if it affects an informational variable as if it modifies a signal used for protection or control. Threat models should incorporate this dependency and prioritize assets according to potential impact. Similarly, the response may require coordination between security teams and system operators. The studies reviewed move towards this integration, although there is still work that evaluates detection without explicitly representing the operational effect. Connecting cyber indicators with stability, availability, and continuity would allow us to better assess which mechanisms reduce risk and which only improve classification in an experimental environment. (1,6,17)

The corpus of 24 studies draws an agenda where the priority is not to accumulate new classifiers, but to improve comparability, robustness, and integration. Transparent threat models, documented datasets, tests against distribution changes, and metrics linked to operational consequences are required. It is also advisable to study maintenance of controls, secure updating, and recovery after incidents, which are decisive aspects during the life cycle. Cooperation between cybersecurity and electrical operation can avoid technically sophisticated solutions that are difficult to deploy. More cumulative research should publish configurations and limitations in sufficient detail to allow reproduction. Such a discipline would strengthen the transition from experimental results to defensible protection mechanisms in real infrastructures. (18-24)

CONCLUSIONS

The systematic review made it possible to respond to the general objective by integrating the evidence from 24 studies on cybersecurity in smart grids within the period 2018–2022. The results show an expanding field whose evolution combines conceptual consolidation and increasingly specific applications. The main conclusion is that the usefulness of the solutions does not depend only on the novelty of a technique, but also on its correspondence with specific operational needs, the quality of the information used and the possibility of being consistently incorporated into electrical infrastructures that have their own technical and organizational constraints.

The corpus shows that technological integration is a central criterion for interpreting the results on cybersecurity in smart grids. Interoperability, data availability, scalability, security, maintainability and compatibility with existing systems appear recurrently as conditions that can favor or limit the observed performance. Therefore, the positive results obtained in particular scenarios should not be automatically generalized to other networks, assets or contexts. The future evaluation should incorporate these conditions as part of the performance and not treat them as separate secondary aspects of the main solution.

The methodological heterogeneity identified explains why it is not appropriate to establish a universal ranking of methods or to calculate an aggregate effect from results that respond to different objectives and metrics. The review provides greater value by organizing convergences, contrasts, and gaps within comparable categories. This conclusion guides the reading of the tables and figures: the frequencies describe the composition of the corpus and the matrices allow individual evidence to be

traced, while the thematic interpretation relates the findings to the research problem without attributing equivalence to designs that were not designed to answer the same question.

Subsequent research should strengthen reproducibility through complete descriptions of data, configurations, procedures, and metrics, as well as incorporating comparisons under representative conditions and predefined evaluation criteria. It is also necessary to expand validation outside of controlled scenarios and clearly document transfer constraints. More comparable evidence would make it possible to determine which solutions maintain their performance in the face of changes in scale, topology, load, data quality, or communications infrastructure, and would make it easier for academic results to be translated into engineering decisions with less uncertainty.

Finally, the synthesis confirms that the development of cybersecurity in smart grids should be understood as a multidimensional process in which technology, data, architecture, and operational context converge. The selected studies offer a sufficient basis to identify consolidated lines and persistent challenges, but also show the need for more comprehensive evaluations. The future agenda should prioritize verifiable, secure, interoperable, and technically justified solutions, with indicators linked to the real purpose of use. This orientation would allow progress from feasibility demonstrations to cumulative evidence capable of supporting responsible adoptions in electricity systems.

BIBLIOGRAPHIC REFERENCES

1. El Mrabet Z, Kaabouch N, El Ghazi H, El Ghazi H. Cyber-security in smart grid: Survey and challenges. Comput Electr Eng. 2018;67:469-482. https://doi.org/10.1016/j.compeleceng.2018.01.015.
2. Rafał Leszczyna. A review of standards with cybersecurity requirements for smart grid. Comput Secur. 2018;77:262-276. https://doi.org/10.1016/j.cose.2018.03.011.
3. Rafał Leszczyna. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. Comput Stand Interfaces. 2018;56:134-149. https://doi.org/10.1016/j.csi.2017.09.005.
4. Chih-Che Sun, Adam Hahn, Chen-Ching Liu. Cyber security of a power grid: State-of-the-art. Int J Electr Power Energy Syst. 2018;99:45-56. https://doi.org/10.1016/j.ijepes.2017.12.020.
5. Rafał Leszczyna. Standards with cybersecurity controls for smart grid—A systematic analysis. Int J Commun Syst. 2019;32(6):e3910. https://doi.org/10.1002/dac.3910.
6. Muhammed Zekeriya Gunduz, Resul Das. Cyber-security on smart grid: Threats and potential solutions. Comput Netw. 2020;169:107094. https://doi.org/10.1016/j.comnet.2019.107094.
7. Md Musabbir Hossain, Chen Peng. Cyber–physical security for on-going smart grid initiatives: a survey. IET Cyber-Phys Syst Theory Appl. 2020;5(3):233-244. https://doi.org/10.1049/iet-cps.2019.0039.
8. Ferrag MA, Babaghayou M, Yazici MA. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. J Inf Secur Appl. 2020;52:102500. https://doi.org/10.1016/j.jisa.2020.102500.
9. Hang Zhang, Bo Liu, Hongyu Wu. Smart Grid Cyber-Physical Attack and Defense: A Review. IEEE Access. 2021;9:29641-29659. https://doi.org/10.1109/ACCESS.2021.3058628.

10. Fazel Mohammadi. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. Energies. 2021;14(5):1380. https://doi.org/10.3390/en14051380.
11. Tufail S, Parvez I, Batool S, Sarwat A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. Energies. 2021;14(18):5894. https://doi.org/10.3390/en14185894.
12. Alsuwian, Butt, Amin. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. Sustainability. 2022;14(21):14226. https://doi.org/10.3390/su142114226.
13. Ding J, Qammar A, Zhang Z, Karim A, Ning H. Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. Energies. 2022;15(18):6799. https://doi.org/10.3390/en15186799.
14. Usman Inayat, Muhammad Fahad Zia, Sajid Mahmood, Tarek Berghout, Mohamed Benbouzid. Cybersecurity Enhancement of Smart Grid: Attacks, Methods, and Prospects. Electronics. 2022;11(23):3854. https://doi.org/10.3390/electronics11233854.
15. Tarek Berghout, Mohamed Benbouzid, S.M. Muyeen. Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. Int J Crit Infrastruct Prot. 2022;38:100547. https://doi.org/10.1016/j.ijcip.2022.100547.
16. Haftu Tasew Reda, Adnan Anwar, Abdun Mahmood. Comprehensive survey and taxonomies of false data injection attacks in smart grids. Renew Sustain Energy Rev. 2022;163:112423. https://doi.org/10.1016/j.rser.2022.112423.
17. Yoonjib Kim. Smart grid security: Attacks and defence techniques. IET Smart Grid. 2022. https://doi.org/10.1049/stg2.12090
18. Tala Talaei Khoei, Hadjar Ould Slimane, Naima Kaabouch. Cyber-Security of Smart Grids: Attacks, Detection, Countermeasure Techniques, and Future Directions. Communications and Network. 2022. https://doi.org/10.4236/cn.2022.144009
19. Jennifer Tyav, Shahid Tufail, Sukanta Roy, Imtiaz Parvez, Anjan Debnath, Arif Sarwat. A comprehensive review on Smart Grid Data Security. IEEE SoutheastCon. 2022. https://doi.org/10.1109/SoutheastCon48659.2022.9764139
20. Yu T, Da K, Wang Z, Ling Y, Li X, Bin D, Yang C. An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning. Front Energy Res. 2022;10:903370. https://doi.org/10.3389/fenrg.2022.903370.
21. Carlos Diago, Andrew Forshaw. Cybersecurity for shared infrastructure substation networks with IEC 61850 GOOSE and Sampled Values. The Journal of Engineering. 2018. https://doi.org/10.1049/joe.2018.0150
22. Silvio E. Quincozes, Célio Albuquerque, Diego Passos, Daniel Mossé. A survey on intrusion detection and prevention systems in digital substations. Comput Netw. 2021;184:107679. https://doi.org/10.1016/j.comnet.2020.107679.
23. Syrmakesis AD, Alcaraz C, Hatziargyriou ND. Classifying resilience approaches for protecting smart grids against cyber threats. Int J Inf Secur. 2022;21:1189-1210. https://doi.org/10.1007/s10207-022-00594-7.
24. Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electr Power Syst Res. 2023;215:108975. https://doi.org/10.1016/j.epsr.2022.108975.

ETHICAL CONSIDERATIONS

Not applicable. This study is a review of published literature and did not involve direct participation of human beings, animals, interventions, or collection of identifiable personal data.

ARTIFICIAL INTELLIGENCE (AI) USE STATEMENT

The authors declare that the generative artificial intelligence tool ChatGPT (OpenAI) was used exclusively to support the organization of the article and translation of text. Its use did not determine the scientific content, study design, source selection, data analysis, interpretation of results, or conclusions. Full responsibility for the content remains with the authors.

FUNDING

This research did not receive any financial support.

CONFLICT OF INTEREST

The authors declare no conflicts of interest.

AUTHOR CONTRIBUTION

Author Names and Initials: Alberto Ricardo Delgado Revilla (ARDR)
1. Conceptualization: ARDR
2. Data curation: ARDR
3. Formal analysis: ARDR
4. Acquisition of financing: not applicable
5. Investigation: ARDR
6. Methodology: ARDR
7. Project administration: ARDR
8. Resources: ARDR
9. Software: not applicable
10. Supervision: ARDR
11. Validation: ARDR
12. View: ARDR
13. Original draft writing: ARDR
14. Writing, review and editing: ARDR