City Research Online

City St George's, University of London

Citation: Arsal, M., Kamel, T., Asad, H. & Khan, A. (2026). A Systematic Review of Cyber Risk Analysis Approaches for Wind Power Plants. Energies, 19(3), 677. doi: 10.3390/en19030677

This is the published version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/36926/

Link to published version: https://doi.org/10.3390/en19030677

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

energies

MDPI

Systematic Review

A Systematic Review of Cyber Risk Analysis Approaches for Wind Power Plants

Muhammad Arsal [1,*], Tamer Kamel [1,*], Hafizul Asad [2] and Asiya Khan [1]

[1] School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth PL4 8AA, UK; asiya.khan@plymouth.ac.uk
[2] School of Science and Technology, City St George's, University of London, London EC1V 0HB, UK; hafizul.asad@citystgeorges.ac.uk
* Correspondence: muhammad.arsal@plymouth.ac.uk (M.A.); tamer.kamel@plymouth.ac.uk (T.K.)

Abstract

Wind power plants (WPPs), as large-scale cyber–physical systems (CPSs), have become essential to renewable energy generation but are increasingly exposed to cyber threats. Attacks on supervisory control and data acquisition (SCADA) networks can cause cascading physical and economic impacts. The systematic synthesis of cyber risk analysis methods specific to WPPs and cyber–physical energy systems (CPESs) is a need of the hour to identify research gaps and guide the development of resilient protection frameworks. This study employs a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol to review the state of the art in this area. Peer-reviewed studies published between January 2010 and January 2025 were taken from four major journals using a structured set of nine search queries. After removing duplicates, applying inclusion and exclusion criteria, and screening titles and abstracts, 62 studies were examined for analysis on the basis of a synthesis framework. The studies were classified along three methodological dimensions, qualitative vs. quantitative, model-based vs. data-driven, and informal vs. formal, giving us a unified taxonomy of cyber risk analysis approaches. Among the included studies, 45% appeared to be qualitative or semi-quantitative frameworks such as STRIDE, DREAD, or MITRE ATT&CK; 35% were classified as quantitative or model-based techniques such as Bayesian networks, Markov decision processes, and Petri nets; and 20% adopted data-driven or hybrid AI/ML methods. Only 28% implemented formal verification, and fewer than 10% explicitly linked cyber vulnerabilities to safety consequences. Key research gaps include limited integration of safety–security interdependencies, scarce operational datasets, and inadequate modelling of environmental factors in WPPs. This systematic review highlights a predominance of qualitative approaches and a shortage of data-driven and formally verified frameworks for WPP cybersecurity. Future research should prioritise hybrid methods that integrate formal modelling, synthetic data generation, and machine learning-based risk prioritisation to enhance resilience and operational safety of renewable-energy infrastructures.

Keywords: cyber–physical systems; wind power plants; cybersecurity; threat modelling and assessment; cyber risk analysis; formal methods; machine learning

Check for updates

Academic Editor: Edmund Widl

Received: 24 November 2025
Revised: 2 January 2026
Accepted: 21 January 2026
Published: 28 January 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Throughout history, the use of wind energy has experienced fluctuations, transitioning from the old windmills of the past to the high-tech wind turbines found in modern wind

farms [1]. Due to the harmful environmental impact of fossil fuel-based energy sources, WPPs have become more popular in recent decades as they are cleaner, greener, and more sustainable. WPPs may consist of an array of large wind turbines positioned strategically to capture wind energy efficiently. The turbines' blades are designed to rotate when exposed to wind, generating kinetic energy that can be converted into electricity through generators. As the world is moving towards net zero, WPPs present the potential to emerge as essential contributors to global energy production. The higher capital cost of wind farms is a concern. However, their ongoing evolution towards greater efficiency reinforces their crucial role in building a greener future.

The increasing adoption of digital technology necessitates expanding networking capabilities, linking previously isolated components into broader communication networks [2]. This trend presents new kinds of challenges. Such new data flows for the complex interconnection of power grids and critical infrastructure raise significant security and safety concerns. Modern WPPs are thus perfect examples of CPS, combining information technology (IT) and operational technology (OT) layers that jointly govern sensing, communication, and control.

The importance of cybersecurity in wind energy systems is increasing due to their cyber–physical nature [3,4]. Current and emerging threats already exceed the industry's capacity to defend against them [5,6]. In recent years, numerous cyber intrusions and attacks have targeted wind energy systems [7]. These incidents highlight growing adversarial interest in this sector. A first-of-its-kind event happened on 5 March 2019, when a denial-of-service (DoS) attack disrupted communications for 12 h in Utah, USA [8]. DoS is a type of attack in which an attacker floods the communication channel so that legitimate transfer of data may halt for a specific period of time. It was a simple IT attack on an unpatched firewall. This temporarily reduced grid visibility to approximately 500 MW of the generating capacity across a dozen solar and wind power sites. It was the first time that a command centre in renewables lost visibility of its operational zone. While it was mostly an IT layer attack, it is an indicator that operations for such ICSs (industrial control systems) are at risk as digitisation increases. On 19 November 2021, Vestas—the world's largest wind turbine manufacturer—discovered a ransomware cyber attack. Ransomware is a type of attack in which attackers demand ransom (money or any privilege) whenever they gain control over some cyber or physical entity. The attackers illegally accessed sensitive and personal data from the IT servers and threatened to publish the stolen data [9]. Vestas confirmed that the stolen data had been leaked by the attackers and was potentially offered to third parties. Although there was no impact on operations, the Vestas stock price decreased by 4% due to loss of public confidence.

Other recent cases demonstrate the severity of the threat landscape and its political use cases. A major ViaSat (via satellite) attack forced nearly 5800 ENERCON wind turbines, representing 10 GW of total capacity, offline for almost two months when their satellite systems were attacked [10]. A ViaSat attack typically involves a targeted operation against satellite communication infrastructure (modems) that causes large-scale loss of connectivity rather than the theft of data. This attack happened at the same time as Russia invaded Ukraine. Moreover, a ransomware attack hit two German companies, namely Nordex Group SE and Deutsche Windtechnik. The attack on Nordex Group led the company to shut off its IT systems and remote communications to their wind turbines [11]. The cyber attack on Windtechnik similarly resulted in disabling remote access to 2000 wind turbines [12]. Even though the impact of these attacks on the wind farms and grid was limited, these attacks reveal how insecure these systems are in the face of rising cyber threats.

Although WPPs employ basic detection and protection mechanisms, denial-of-service and stealth attacks may render these defences ineffective by flooding communication

channels or spoofing sensor data. If an attacker manipulates measurements while control systems report normal operation, turbine controllers may continue unsafe actions during high wind or grid instability conditions. This can risk structural damage or cascading grid effects. Such attack scenarios highlight the immaturity of current defensive mechanisms. Moreover, adversaries can pursue long-term goals through espionage, for instance, as in the Chinese ScanBox campaign that profiled turbine operators in the South China Sea [13]. This malware is delivered via phishing emails. Once someone falls prey, it allows threat actors to profile victims and to deliver further carefully crafted malware to selected targets of interest. These examples collectively indicate that cybersecurity threats to WPPs are both realistic and becoming increasingly sophisticated.

While many of these incidents have primarily affected the IT layers of WPPs, which resulted in temporary communication disruptions. The risks to the OT layer could be even more critical. Without adequate protections, malicious activity could propagate into control logic, which would endanger both cyber and physical components of wind plants. Ultimately the stability of the electric grid would become compromised [14]. The wind energy sector will continue to be an attractive target, as many components still rely on legacy technologies that lack modern security updates. Table 1 shows these major cyberattacks on wind farms assets and defines their attack type and the impact it caused. It is noted that ransomware is the dominant attack type. Moreover, DoS and ViaSat attacks were also carried out to directly impact the communication and operations of WPPs. These different kinds of attacks on similar infrastructure reflect both the economic value and operational criticality of wind energy infrastructure.

Table 1. Cyber incidents affecting the wind energy sector.

Year	Organisation	Attack Type	Impact
2019	sPower	DoS	Temporary loss of communications and visibility to about 500 MW across a dozen solar and wind plants [8].
2021	Vestas	Ransomware	Shutdown of parts of internal IT infrastructure; compromise and later leak of internal and personal data [9].
2022	Enercon	ViaSat	Loss of remote monitoring and control for roughly 5800 wind turbines, totalling about 10–11 GW of capacity [10].
2022	Nordex Group	Ransomware	Company shut down IT systems and disabled remote access to managed turbines as a precaution [11].
2022	Deutsche Windtechnik	Ransomware	Remote monitoring connections to around 2000 turbines were switched off for 24–48 h; a full retake took several days [12].

Addressing such threats requires a comprehensive cyber risk analysis framework. It should be capable of identifying vulnerabilities and assessing the likelihood and potential impact of an incident. It can then guide risk management strategies. Cyber risk analysis thus forms the foundation of cyber resilience for WPPs. It encompasses three interrelated stages: (1) risk assessment (identifying and quantifying vulnerabilities and threats); (2) risk communication (the exchange of derived results from assessment among stakeholders); and (3) risk management (implementing mitigation measures such as intrusion detection and resilient control systems) [15]. The effectiveness of these stages depends on accurate modelling of the interactions between cyber and physical subsystems.

Although various cyber risk analysis frameworks have been proposed for CPS and the broader energy domain, the literature remains fragmented with respect to wind power

plants. Prior reviews often discuss general CPS risk analysis or renewable energy security but fail to capture the unique control architectures, environmental constraints, and distributed nature of WPPs. Unlike solar and PV systems, the dynamics of WPPs are not purely electrical but arise from a delicate interplay between electrical and mechanical processes. Their protection mechanisms also differ, incorporating coordinated electrical and mechanical safeguards. Any compromise in WPP would not merely affect grid parameters but might harm wind turbines themselves and staff or personnel nearby. Furthermore, existing work often lacks explicit comparison of cyber risk analysis methods. It also lacks formal treatment of safety–security interdependencies and quantitative evaluation of their applicability to the wind power sector. A systematic review is therefore needed to consolidate evidence, identify methodological trends, and highlight research gaps specific to WPPs.

This paper therefore presents a PRISMA-aligned systematic review of cyber risk analysis approaches relevant to wind power plants. The PRISMA checklist of this review is provided in PRISMA 2020 checklist table (Supplementary Materials). This review covers the literature in peer-reviewed journals and conferences from January 2010 to January 2025. It targets studies that propose or discuss methods and frameworks that are applicable to the evaluation of cyber risk of WPPs. This review was carried out using an explicit search strategy (see Section 3), predefined inclusion/exclusion criteria, and a transparent screening process that yielded the final corpus analysed in this manuscript. To guide this review, the following research questions were formulated:

- RQ1: What cyber risk analysis frameworks have been proposed and are adaptable for wind power plants from a CPS point-of-view?
- RQ2: How do these frameworks differ in approach, technique, or method?
- RQ3: To what extent do current studies integrate safety and security?
- RQ4: What methodological gaps and research opportunities are there for developing comprehensive cyber risk analysis frameworks for WPPs?

By responding to these questions, this systematic review aims to provide a transparent evidence base and actionable guidance for researchers, system designers, and operators seeking to strengthen the cyber resilience and safety of wind energy infrastructure.

The remainder of this paper is organised as follows: Section 2 introduces the basic concepts in CPSs, WPP architectures, and cyber risk analysis. Section 3 describes the PRISMA-based methodology and the synthesis framework. Section 4 presents the results of this methodology, while Section 5 focuses on discussing the results and identifies research gaps. Finally, Section 6 concludes with implications and future research directions.

2. Background

This section provides the conceptual and technical background necessary to interpret the cyber risk analysis frameworks reviewed in this study. It focuses on three elements that directly shape our synthesis: (i) core CPS concepts, (ii) the specific architecture and attack surface of WPPs, and (iii) risk and cyber risk analysis frameworks relevant to safety-critical energy systems. Each subsection concludes by explaining how these concepts connect to the research questions and taxonomy presented in Section 3.

2.1. Cyber–Physical Systems

Today, devices and systems in the physical environment are increasingly interconnected through computing, communication, and control technologies, forming what are known as CPSs [16,17]. According to the National Institute of Standards and Technology (NIST), CPSs are intelligent systems composed of engineered networks of interacting physical and computational components that exchange information and exert control

over one another [18]. These systems underpin many critical infrastructures, including transportation, manufacturing, and energy, where software decisions directly influence physical behaviour. A conceptual model of CPS is shown in Figure 1.

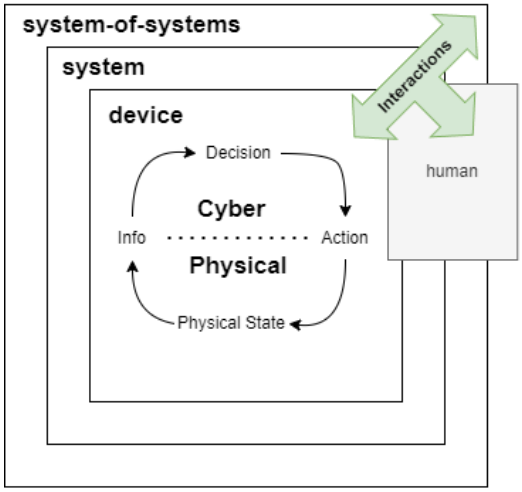

Figure 1. CPS conceptual model.

In the NIST model, CPSs are characterised by tightly coupled cyber and physical domains linked through sensing, computation, communication, and actuation loops. Information from the physical world is captured by sensors, processed by computational components, and then translated into control actions that modify the physical state. This bidirectional interaction enables advanced functionalities such as real-time optimisation and remote supervision but also creates the possibility that cyber incidents propagate into physical faults, safety hazards, or service disruptions.

For safety-critical infrastructures, three CPS properties are particularly important for cyber risk analysis. First of all, the feedback between cyber and physical layers means that compromised measurements or control signals may be used to drive systems into potentially unstable or unsafe operating regions. Secondly, reliance of CPS is mostly on heterogeneous networks and protocols that interconnect components across different organisational and geographic boundaries, which can increase the attack surface and the potential for cascading failures. Third, safety and security are interdependent: a security breach that can alter control logic, timing, or configuration can undermine functional safety guarantees and lead to physical damage or grid instability.

In this review, these CPS characteristics provide the conceptual basis for classifying cyber risk analysis methods according to their ability to capture cyber–physical interactions. They directly motivate the synthesis dimensions used later in Sections 3 and 4, namely qualitative versus quantitative treatment of risk, model-based versus data-driven techniques, and informal versus formal verification of safety and security properties.

2.2. Cyber–Physical Nature of Wind Power Plants

In modern WPPs, the interaction between cyber and physical layers extends beyond individual turbines to farm-wide control and grid integration. The core of this infrastructure is the SCADA system, which enables real-time monitoring, coordination, and remote operation of multiple turbines through PLCs, communication networks, and central control servers [19,20]. SCADA continuously collects measurements (e.g., wind speed, rotor speed, and power output), processes alarms and events, and dispatches control commands to maintain safe and efficient operation.

Figure 2 illustrates a simplified three-layer structure of a WPP, comprising the physical layer (turbines, generators, and transformers), the cyber layer (PLCs, SCADA servers, and

communication links), and the supervisory/business layer (control centre applications and enterprise IT). The tight coupling between these layers means that cyber incidents affecting SCADA logic, network traffic, or configuration can propagate into mechanical stress, abnormal electrical behaviour, or loss of grid services [20,21]. Compared to generic CPS, WPPs thus combine high-value assets, distributed automation, and strong safety–security interdependence.

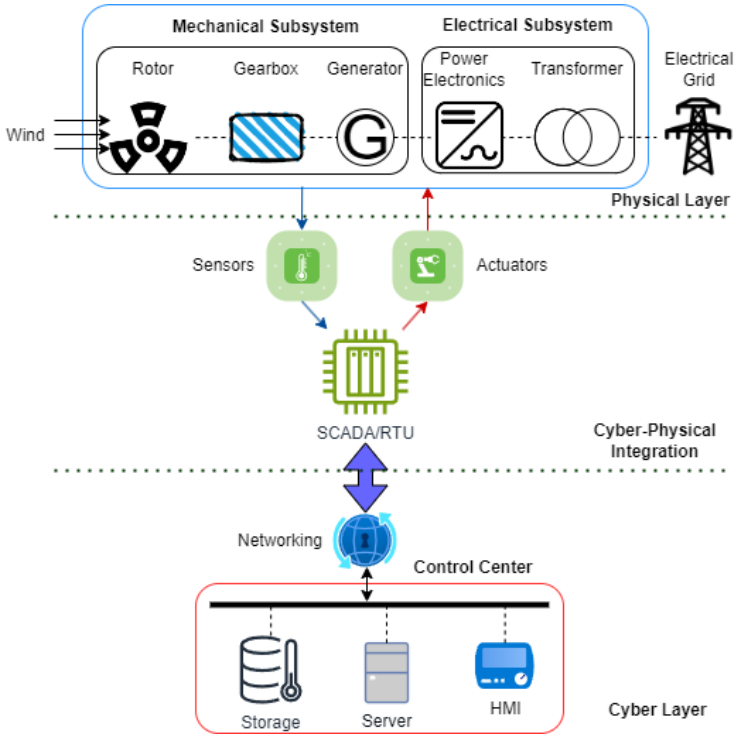

Figure 2. Wind power plant as a CPS [19].

The IEC (International Electroctechnical Commission) has developed two new standards, IEC 61850-7 and IEC 61400-25, to formulate a common communication architecture to monitor and control substations and WPPs, respectively [22]. This lets any SCADA system communicate with any device in the network, enabling much easier control of a large number of wind farms from the control centre. Although it is of major interest to the developers to have such a level of control, it also opens the door for potential security breaches. Figure 3 illustrates such a SCADA network of a wind farm. It shows that most of the risks originate from cyber–physical access points within the SCADA system (which are many). To reach a wind turbine, attackers may target several critical points:

1. **Wind Turbine Control Panel (WTCP):** This is each wind turbines' individual control hub. An attack here is the most direct and costly as the attacker needs some kind of physical access to the wind turbine to perform malicious actions. However, once they gain this access, they can crack the pin by using brute force or dictionary attacks to obtain user access to the control panel. Then, they may obtain control privileges to the control panel by using buffer overflow attacks and malicious commands may then be sent to the intruded WTCP.
2. **Wind Farm Local LAN:** This network acts as a backbone for all the components within the wind farm. The attacker can get into the system by bypassing the firewall and by exploiting a vulnerability in either the communication server or the application server (as they communicate outside the network) of the local control centre. Furthermore, the attacker will exploit a zero day in the database service to reach the workstation

and will obtain host-level privileges through a buffer overflow attack. Root access from here can disrupt or alter communication and control.

3. **Control Centre LAN:** This network is the nerve centre for managing the entire wind farms based on IEC 61850-7. After bypassing the firewall, attacker uses https service to exploit a zero day found in the web server, which may be in the demilitarised zone (DMZ). The attacker has to bypass another firewall which separates the DMZ from the control centre. This entry lets the attacker exploit any known vulnerability in the communication server to gain user-level access there. Once the attacker finds vulnerability in secure-shell or remote-shell services, they get hold of the application servers. From there, they reach the control centre operator console by exploiting any vulnerability present in the network file system or database services. Then, they upgrade their privileges similarly through a buffer overflow attack. Any harmful actions here can result in the loss of control over multiple wind farms and can destabilise broader power distributions.
4. **Remote Control LAN in the Substation:** This network governs integration of a wind farm with the wider power grid. The attacker, after bypassing the firewall, tries to get into the communication server by exploiting a zero day. Then, they find a vulnerability in either the secure shell service or remote shell service to gain access to the application server. Here, they exploit a vulnerability in the network file system to get hold over the operator system, where they obtain root privileges similarly through a buffer overflow attack. Attacks here can result in losing control over multiple wind turbines.

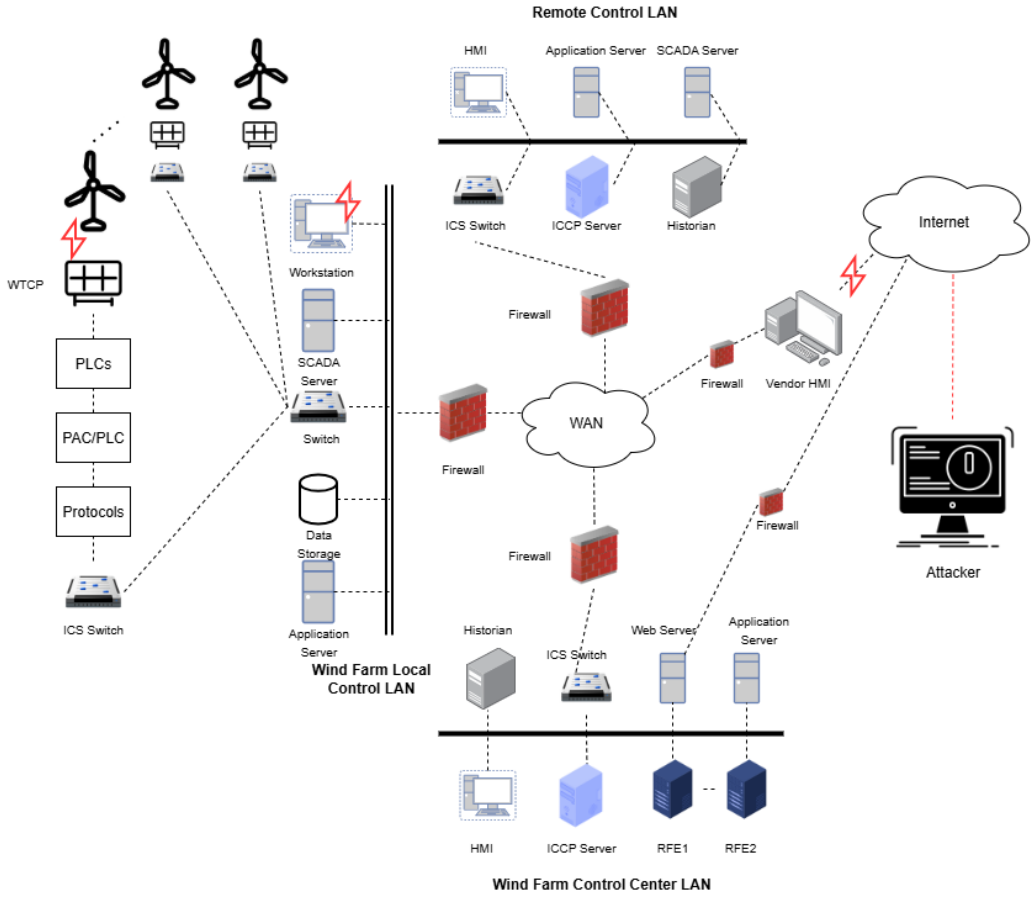

Figure 3. The SCADA network in a wind farm [20].

Compromising any of the aforementioned access points poses severe threats to the safety of wind farm operations [20]. A cyberattack, if successful, can disrupt turbine opera-

tions, reduce power generation, damage equipment through malicious control commands, and destabilise the grid.

While WPPs share commonalities with other renewable plants, several characteristics differentiate their cyber risk profile. The physical consequences of cyber incidents are predominantly mechanical (e.g., overspeed, blade fatigue, and tower loading), not just informational; offshore and remote WPPs depend on long-distance and sometimes bandwidth-constrained communication links; and their hierarchical SCADA architectures are latency-sensitive and often integrate legacy devices [14,19,21]. These features demand cyber risk analysis methods that integrate network behaviour, control dynamics, and structural safety, rather than focusing solely on IT-layer confidentiality or availability.

In this review, the WPP architecture and access points in Figure 3 serve as a reference model for evaluating the literature. They allow us to distinguish studies that treat generic CPS or bulk power systems from those that explicitly model turbine-level, farm-level, or grid-interface risks, and they inform our synthesis of which components and layers remain under-analysed in current WPP cybersecurity research.

2.3. Cyber Risk Analysis

Risk in safety-critical infrastructures is commonly defined as the combination of the likelihood of an unwanted event and the severity of its consequences [23]. For engineered systems such as WPPs, this includes both conventional hazards (e.g., mechanical failure and extreme weather) and cyber-originated events (e.g., intrusions into SCADA or communication networks) that can lead to physical damage or loss of service [15,17].

Risk analysis is the systematic process of identifying, evaluating, and prioritising risks in order to support appropriate mitigation and decision making [23]. Figure 4 illustrates the fundamental components of risk analysis, namely risk assessment, risk management, and risk communication. In the context of energy CPS, it typically considers five interrelated concepts: threats (adversarial or accidental sources of harm), vulnerabilities (weaknesses that can be exploited), controls (preventive or detective safeguards), assets (components or functions of value), and impacts (operational, economic, safety, or environmental consequences). Cyber risk emerges when cyber threats successfully exploit vulnerabilities in digital or communication assets, allowing adverse effects to propagate into the physical system. A simple representation often used in engineering risk studies expresses risk as the product of the probability of loss and the magnitude of that loss,

$$\text{Risk} = P_L \times M_L$$

where P_L denotes the probability (or frequency) of an adverse event and M_L denotes the magnitude of the associated loss. This abstraction is useful for comparing scenarios and prioritising mitigation options, but in CPSs such as WPPs, both terms depend on complex interactions between cyber events, control responses, and physical dynamics.

Building on these general concepts, cyber risk analysis methods for CPSs and WPPs can be grouped into three broad methodological families that structure our review:

- Qualitative and semi-quantitative frameworks, such as STRIDE-based threat modelling, attack trees, security standards mappings, and structured expert scoring. These approaches organise threats and vulnerabilities and are widely used in practice for awareness and high-level prioritisation, but they often rely on subjective assessments and rarely quantify how attacks translate into safety or reliability impacts for specific WPP components.
- Quantitative and model-based techniques, including Bayesian networks, Markov decision processes, Petri nets, and reachability or model-checking-based analyses. These methods use probabilistic or formal models to estimate compromise probabil-

ities, sequences of events, or reachable unsafe states. They offer greater rigour and reproducibility but require detailed system models and data, which remain scarce for operational WPPs and may be costly to obtain.

- Data-driven and hybrid AI/ML approaches, which apply machine learning (e.g., anomaly detection, classification, and reinforcement learning) to operational or simulated data from turbines and SCADA networks. Recent work explores such approaches for wind and other energy assets, promising adaptive detection and online risk assessment, yet validation is often limited by data availability, privacy constraints, and computational limits on turbine-side devices.

In this systematic review, these three families underpin the synthesis dimensions used in Section 4: qualitative versus quantitative treatment of cyber risk, model-based versus data-driven techniques, and informal versus formal verification. They provide a common lens for comparing the 62 included studies and for assessing to what extent existing methods capture the specific cyber–physical risk profile of wind power plants, including safety–security interdependencies and grid-level consequences.

Figure 4. Elements of risk analysis.

3. Methods

This section describes the methodology followed to conduct the systematic review in accordance with the PRISMA guidelines [24]. The process included protocol development, comprehensive database searches, screening and eligibility assessment, data extraction, and synthesis of results.

3.1. Protocol and Registration

The review protocol was developed internally by the authors before starting the searches, following the PRISMA framework and tailored to methodological research on cyber risk analysis rather than clinical trials. The protocol specified the review questions (Section 1), eligibility criteria, databases to be searched, search strings, screening stages, and data extraction fields. It also pre-defined the synthesis dimensions (qualitative vs. quantitative, model-based vs. data-driven, and informal vs. formal) used to classify included studies.

3.2. Eligibility Criteria

Studies were selected according to predefined inclusion and exclusion criteria designed to capture cyber risk analysis methods applicable to wind power plants and closely related energy CPSs.

Inclusion criteria:

- Peer-reviewed journal or conference papers published between January 2010 and January 2025.
- Studies that propose, apply, or systematically evaluate a cyber risk analysis framework, model, or method for CPSs, CPESs, or power/energy infrastructures.
- Methodological or technical content that is directly applicable to wind energy contexts, including at least one of the following: (i) models of wind turbine components (e.g., controllers, sensors, and converters), (ii) analysis of SCADA or control networks used in distributed systems, or (iii) scenarios explicitly involving WPPs or generic wind farms.

Exclusion criteria:

- Non-technical documents (e.g., editorials, opinion pieces, policy briefs, and news articles) and purely organisational or management frameworks.
- Studies focusing exclusively on non-energy CPS domains (e.g., healthcare and autonomous driving) without transferable cyber risk methods for energy systems.
- Papers without accessible full text, duplicate publications, or extended versions of already included work (in which case, only the most complete version was retained).
- Pure incident reports or high-level surveys that do not propose or analyse a specific risk analysis method or model.

During screening, borderline cases were discussed among the authors to ensure consistent application of these criteria, particularly for studies that mentioned renewable energy only tangentially.

3.3. Information Sources

Searches were conducted across four major digital libraries: IEEE Xplore, ScienceDirect, SpringerLink, and MDPI journals. These databases were chosen because they collectively provide broad coverage of electrical and power engineering, control and automation, computer science, and cybersecurity research, including key venues for CPSs and smart grid security. No restrictions were placed on country of origin or publication venue beyond peer-review status.

To complement database searches, backward and forward citation chasing was performed on several seminal CPSs and wind-security papers identified in the initial results, in order to reduce the risk of missing relevant methodological work.

3.4. Search Strategy

Nine database queries were constructed using combinations of key terms and Boolean operators related to “wind power plants”, “cyber risk”, “cyber–physical systems”, and “safety”. A total of 632 records were initially identified. Table 2 summarises the individual queries and their respective result counts.

3.5. Selection Process

All retrieved records were exported to a reference management database (Zotero), where exact-title and DOI matching were used to automatically detect duplicates; any remaining duplicates were removed manually, resulting in an overall duplicate rate of approximately 18 %. The screening proceeded in three stages:

1. Title screening: Records obviously unrelated to cybersecurity, CPSs, or energy systems (e.g., purely mechanical wind-turbine design or solar PV-only studies) were excluded.
2. Title and abstract screening: Papers that mentioned cybersecurity but did not include a risk analysis method (e.g., general awareness articles and high-level policy reports) or focused on non-energy CPSs without transferable methods were removed.

3. Full-text assessment: The remaining 102 articles were read in full and assessed against the eligibility criteria. Typical reasons for exclusion at this stage included (i) frameworks exclusively targeting transmission-level smart grids without any distributed generation or WPP context; (ii) descriptive case studies of solar or hydro plants with no explicit risk analysis method; and (iii) papers that discussed wind energy only in passing within broader renewable portfolios without methodological detail.

Disagreements during full-text assessment were resolved by discussion among at least two authors. In total, 62 studies met all criteria and were retained for detailed analysis.

Table 2. Electronic search strategy and results across databases.

Search Query	IEEE Xplore	ScienceDirect	MDPI	SpringerLink
"wind power plants" AND "cyber risk"	30	6	2	1
"cyber–physical energy systems" AND "risk analysis" AND "safety"	1	98	23	7
"wind power plants" AND "cyber risk" AND "safety"	4	9	0	1
"wind power plants" AND "cyber attack" AND "safety"	3	50	18	0
"CPS" AND "cyber risk analysis" AND "safety"	64	7	8	6
"CPS" AND "cyber risk analysis" AND "security"	132	14	15	8
"CPES" AND "cyber risk analysis"	4	0	1	0
"wind power" AND "cyber risk analysis"	57	2	0	1
"wind power" AND "cyber risk assessment"	52	0	5	3

3.6. Data Collection Process

A structured data extraction form was developed and piloted on a subset of articles to ensure consistency. For each included study, the following variables were extracted:

- System context (generic CPS, power system/CPES, wind-specific).
- Modelling and analysis approach (qualitative, semi-quantitative, or quantitative).
- Technique classification (model-based vs. data-driven vs. hybrid).
- Verification level (informal, semi-formal, or formal).
- Treatment of safety and security
- Main findings and limitations reported by the authors.

Data extraction was carried out by one reviewer and spot-checked by a second to reduce transcription errors and ensure consistent coding of the taxonomy dimensions.

3.7. Synthesis Framework

The synthesis framework provides the analytical lens for structuring and interpreting the results reported in Section 4. Cyber risk analysis approaches were compared along six cross-cutting properties commonly used in the security and risk management literature [25,26]: **ease of implementation**, **subjectivity**, **data requirements**, **reproducibility**, **risk prioritisation capability**, and **scalability**.

Ease of implementation captures how straightforward it is for practitioners to apply a given approach in realistic settings, including the need for specialised skills or tools. Subjectivity reflects the extent to which outputs depend on expert judgement and qualitative scoring rather than on explicit models or measurements. Data requirements assess the quantity and quality of data needed to obtain reliable results, a critical factor in WPPs where operational datasets are scarce and sensitive [27]. Reproducibility considers whether similar conclusions are likely to be obtained when the method is applied by different analysts or to comparable systems. Risk prioritisation denotes the ability to rank or classify risks to support decisions about where to focus mitigation efforts. Finally, scalability examines

whether an approach remains tractable as system size, complexity, or the number of attack paths increases (e.g., from a single turbine to a multi-farm offshore cluster).

In our defined synthesis, these six properties are not used as formal scoring criteria but as structured vocabulary for qualitatively comparing the strengths and limitations of different methods in the WPP context.

3.7.1. Qualitative vs. Quantitative Risk Analysis

A qualitative approach to evaluating security risks focuses on identifying, analysing, and prioritising risks based on subjective judgements rather than quantitative measurements. One of its key advantages is cost-effectiveness, as it does not require extensive data collection or detailed statistical analysis, making it quicker and less resource-intensive. Furthermore, qualitative risk assessment is highly flexible and can be adapted to different systems without relying on rigorous mathematical proofs. By leveraging the expertise and insights of individuals, it allows for a nuanced understanding of risks, which can be effectively communicated to stakeholders who may lack technical expertise. This clear communication helps decision-makers grasp the significance of potential risks and take timely action.

However, qualitative analysis has limitations. Its subjective nature can lead to inconsistencies and biases, potentially resulting in incomplete risk assessments. It may not provide precise estimates of the likelihood or impact of cyberattacks, and it is less suitable for large-scale or complex projects where detailed analysis is necessary. Because evaluation criteria often depend on specific contexts, results may not be easily comparable across different organisations or projects. Finally, the reliance on judgement can reduce transparency and make it harder to build trust among stakeholders who prefer data-driven assessments.

In contrast, quantitative risk analysis employs data and mathematical models to estimate the probability and potential consequences of security threats. By quantifying probabilities and impacts, it provides a more detailed and objective assessment of risks, enabling organisations to prioritise the most significant threats. This precision supports effective decision-making, allowing resources to be allocated efficiently and risk management strategies to be targeted appropriately. Additionally, quantitative analysis facilitates communication with stakeholders by presenting risks in a data-backed format that is easier to validate and understand. Its rigorous nature also enhances credibility with regulators, auditors, and other stakeholders who often require a formalised approach to risk management.

Despite its strengths, quantitative risk analysis also faces several challenges. Its effectiveness relies heavily on the availability of accurate and reliable data, which may not always be accessible. The method is often complex and time-consuming, requiring specialised expertise and computational tools to perform detailed analyses. This complexity can make it more costly than qualitative approaches. Additionally, fully capturing the real-world complexities of an organisation's environment can be difficult, and certain risks may be hard to quantify due to limited or unavailable data.

Figure 5 compares qualitative and quantitative approaches along the six properties of the framework. In general, qualitative methods score highly on ease of implementation and adaptability but lower on reproducibility and rigorous risk prioritisation. Quantitative methods exhibit the opposite pattern: they offer stronger support for reproducible, prioritised decisions, at the cost of higher data requirements and implementation effort. This trade-off is reflected in the distributions reported in Section 4, where most WPP-focused studies remain qualitative or semi-quantitative despite the availability of advanced quantitative methods in the broader CPS literature.

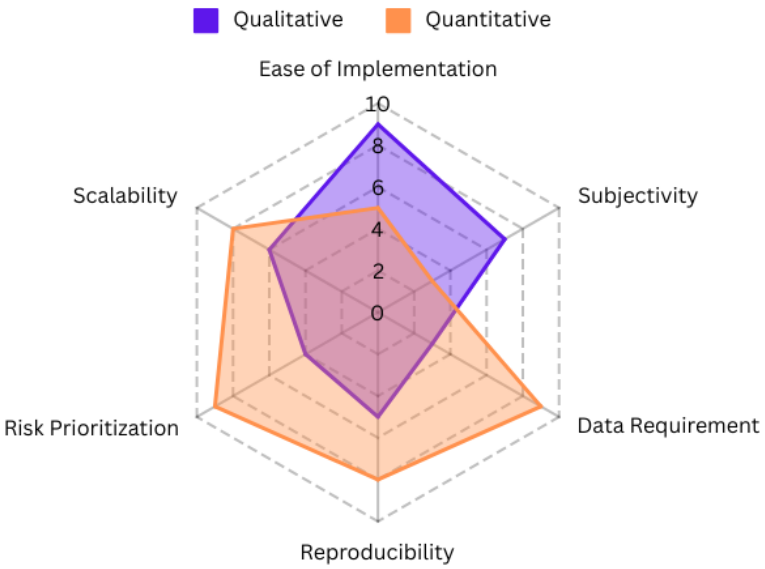

Figure 5. Comparison of qualitative and quantitative risk analysis.

3.7.2. Model-Based vs. Data-Driven Risk Analysis

Model-based risk assessment methods utilise mathematical models and theoretical frameworks of systems to evaluate risks in CPS. These approaches are rigorous and require a comprehensive understanding of the system to derive an exact or abstract model. They are well-structured and highly reproducible and can be validated mathematically, making them particularly suitable for systems that demand high reliability and formal analysis. Another benefit is their ability to provide clear causal explanations of risks, which enhances interpretability and facilitates communication with stakeholders. However, model-based methods are often limited by the difficulty of building accurate models for large-scale, heterogeneous, or dynamic systems. They are also time-consuming and resource-intensive and may not adapt well to rapidly evolving threats or unforeseen scenarios.

In contrast, data-driven approaches rely on the collection and analysis of operational data to identify patterns that reveal vulnerabilities. These methods do not require explicit system modelling, which can save time and costs, and they are especially applicable to highly interconnected and dynamic environments. They are also capable of capturing subtle and complex correlations that may be missed in analytical models, making them well-suited to detecting emerging or unknown threats. Furthermore, data-driven methods can adapt in real time as new data becomes available. On the downside, their effectiveness depends heavily on the availability and quality of data, which may be incomplete, noisy, or biased. While techniques such as synthetic data generation and transfer learning can mitigate some of these limitations, their application remains challenging and often less effective for highly complex and diverse systems. Interpretability is another limitation, as many advanced data-driven methods (e.g., machine learning) function as "black boxes," making it difficult to explain risk outcomes. In addition, these approaches often require significant computational resources and may struggle to generalise beyond the specific datasets on which they were trained.

As summarised in Figure 6, model-based approaches tend to score higher on interpretability, formal analysis potential, and structured reproducibility, whereas data-driven methods excel in adaptability and pattern detection but are more sensitive to data quality and resource constraints. Hybrid approaches that integrate model structure with data-driven components—such as learning parameters of a Bayesian graph from data or

constraining ML models with physical invariants—offer promising compromises and are highlighted in Section 5 as an important future direction.

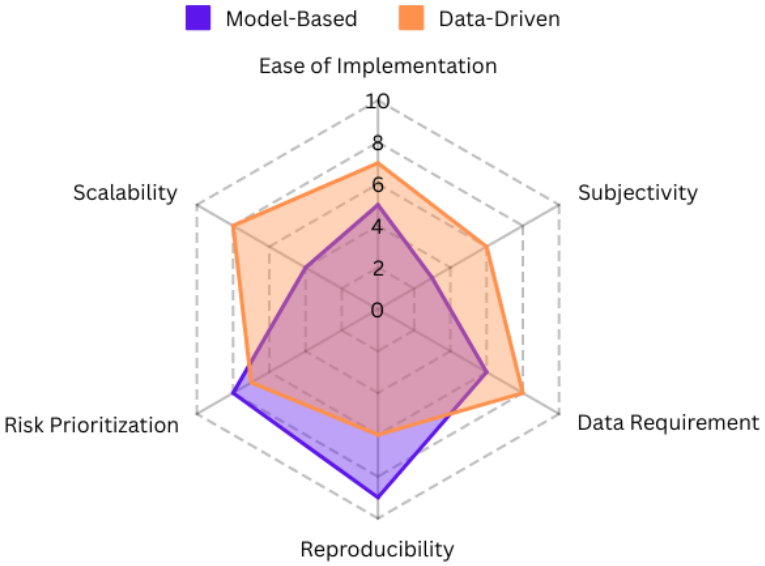

Figure 6. Comparison of model-based and data-driven risk analysis.

3.7.3. Informal vs. Formal Risk Analysis

Informal methods are typically straightforward and accessible for identifying and assessing risks. They rely on the expertise and intuition of teams or established frameworks to recognise potential threats and vulnerabilities, making them easy to understand and apply across various domains. These methods provide a quick and flexible means of risk assessment, enabling organisations to rapidly identify and prioritise potential risks without requiring specialised training or resources. However, due to their reliance on subjective judgements and qualitative analysis, informal methods may lack the precision and rigour necessary for comprehensive risk assessment.

In contrast, formal methods offer a systematic and rigorous approach to the verification and validation of CPS. Formal methods in system design involve using rigorously specified mathematical models to develop software and hardware systems [28]. Techniques such as model checking and theorem proving provide guarantees to ensure system safety [29,30]. Formal methods verify correct behaviour by checking the model against a set of verification properties, traditionally categorised into two main types:

- **Safety properties**, which define configurations that are unauthorised and must be avoided across all possible system states and evolutions.
- **Liveness properties**, which capture the potential or eventual occurrence of desired system behaviours or transitions.

As systems grow in complexity and safety concerns escalate, formal methods provide an additional layer of assurance. However, they are computationally expensive and their scope is limited. Informal methods, by contrast, excel in applicability to various scenarios through simulation environments. Yet, their reliance on subjective judgements and qualitative analysis may compromise precision and rigour, potentially affecting safety. Key distinctions of formal methods include the use of formal verification schemes, where system principles must undergo rigorous proof before acceptance [31,32]. Tools like UPPAAL (for real-time systems), NuSMV (for finite and infinite states), PRISM (for probabilistic analysis), and SPIN (for concurrent systems) verify properties, generating counterexamples for debugging [33–36].

Traditional system design relies primarily on extensive testing to verify behaviour, but testing has limitations in providing conclusive results [32]. In contrast, once a theorem is proven true within formal methods, its validity persists. Formal methods can analyse risks associated with CPS, identify potential vulnerabilities across all state spaces, and guide the development of more resilient approaches to address these vulnerabilities. Typically, model checking and theorem proving are used to evaluate system safety properties in an automated manner. A brief comparison of formal and informal methods is presented in Table 3. The formal modelling of CPS and the application of risk assessment methodologies to these models are increasingly valued due to the advantages of formal methods. The objective is to model the system and its specifications formally, so that the system can be checked against these specifications for all possible inputs and states.

Table 3. A comparison of formal and informal methods.

Aspect	Formal Methods	Informal Methods
Characteristics	Based on rigorous mathematical foundations, providing precise and unambiguous models.	Rely on expert judgement, heuristics, and qualitative analysis; often less structured and systematic.
Benefits	High precision, verifiable and repeatable results, strong theoretical foundation.	Easy to understand and use, require less training, flexible and adaptable.
Limitations	High complexity, requires specialised knowledge, computationally intensive.	Subjective and prone to bias, lack of repeatability, less precise and rigorous.

Figure 7 and Table 3 illustrate that formal methods typically achieve higher scores in precision, reproducibility, and reduction in subjectivity, while informal methods offer advantages in ease of implementation and scalability to loosely specified or rapidly changing contexts. In practice, many WPP studies adopt semi-formal positions—for example, using structured models without exhaustive verification—which we classify accordingly in the results.

To demonstrate how the synthesis framework maps onto a concrete WPP scenario, consider a false-data-injection attack on a wind-speed sensor. A qualitative approach such as STRIDE would identify the threat under the "tampering" category and qualitatively rank its severity. A quantitative model, such as a Bayesian network, could estimate the probability that sensor compromise leads to incorrect pitch control and subsequent mechanical stress. A model-based formal analysis using hybrid automata might then verify whether unsafe rotational speeds are reachable under corrupted inputs, providing guarantees about safety properties. Finally, a data-driven anomaly detector trained on SCADA telemetry could mitigate control by flagging inconsistent wind-speed patterns in real time. This layered example illustrates how the qualitative/quantitative, model-based/data-driven, and informal/formal dimensions intersect when analysing cyber–physical risks in wind power plants.

3.8. Study Risk of Bias Assessment

Given the methodological and conceptual focus of the included literature, standard clinical risk-of-bias tools were not applicable. Instead, potential biases were assessed qualitatively using three criteria: (i) peer-review status and venue, (ii) clarity and completeness of the methodological description (e.g., explicit models, assumptions, and parameter

choices), and (iii) availability of validation or reproducibility evidence (e.g., case studies, tool availability, and datasets).

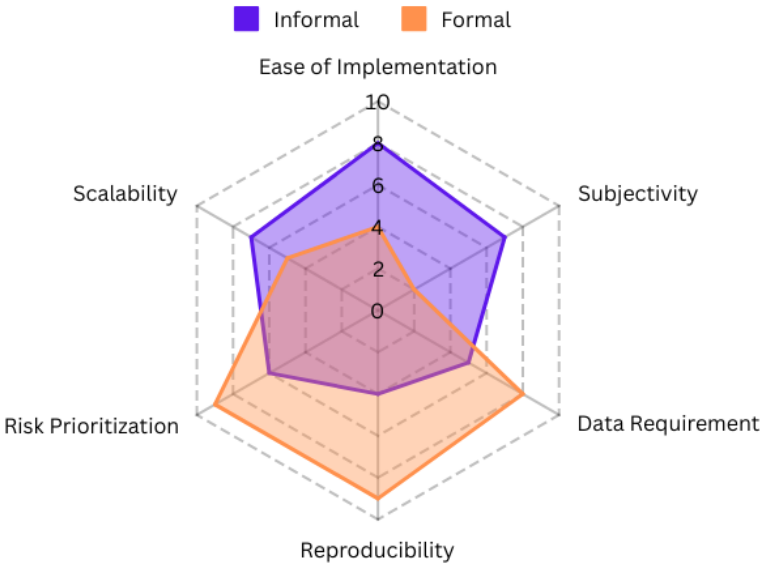

Figure 7. Comparison of informal and formal risk analysis.

Studies with vague descriptions of their models or with no discussion of limitations were treated cautiously when synthesising results. Database bias and language bias are possible, as the search was limited to four major English-language databases; this limitation is revisited in Section 5 when discussing the overall strength of evidence.

3.9. Synthesis Methods

Given the heterogeneity of study designs, system contexts, and outcome measures, a quantitative meta-analysis was not feasible. Instead, we applied a structured narrative synthesis combined with descriptive statistics based on the extracted variables. Results were organised according to the taxonomy defined in Section 3, comparing approaches along three axes: qualitative vs. quantitative, model-based vs. data-driven, and informal vs. formal.

3.10. Reporting Bias and Certainty Assessment

Publication bias was not formally assessed due to the non-statistical nature of the synthesis. However, potential selection bias was mitigated by searching multiple databases and applying explicit inclusion/exclusion criteria.

4. Results

This section reports the findings of the PRISMA-guided systematic review, summarising both quantitative and qualitative evidence extracted from the 62 included studies. A total of 632 records were initially identified through database searches; after duplicate removal and multi-stage screening, 62 studies met the eligibility criteria (Figure 8). The synthesis is presented in two parts: first, generalised CPS studies that inform methodological foundations (Section 4.1); second, state-of-the-art studies focusing specifically on wind power plants (Section 4.2). This separation avoids overlap and clarifies how generic CPS research translates into domain-specific WPP applications.

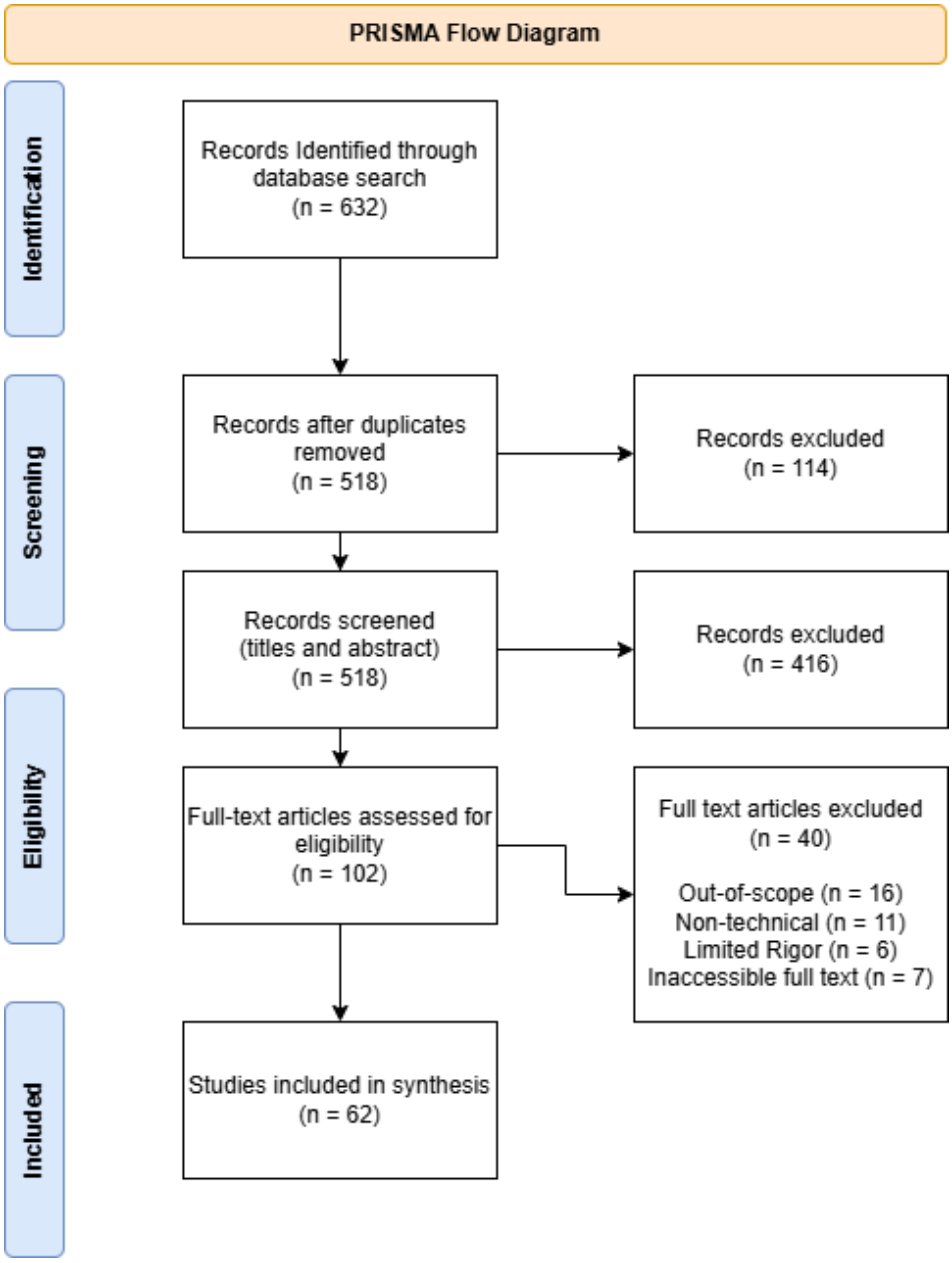

Figure 8. PRISMA flow diagram of study selection.

4.1. Generalised CPS Studies

Of the 62 included works, 36 examined cyber risk analysis across generic CPS domains, such as smart grids, autonomous vehicles, industrial automation, and robotics, without explicit reference to wind power. This split underscores a methodological imbalance: while the majority of studies focus on generic CPS or bulk power systems, fewer than half adapt their methods specifically to wind power plants. As a result, many advanced techniques—such as probabilistic model checking, hybrid automata, or CPS-wide Bayesian risk models—are available in principle but remain under-exploited for the particular mechanical, environmental, and control characteristics of WPPs.

These studies were retained because their modelling or analytical frameworks are transferable to the energy sector and underpin later WPP-specific research (Section 4.2). CPS research emphasises that increasing interconnection of information and control layers through ICT, remote sensing, and IoT devices amplifies vulnerabilities [37–39]. Safe-

guarding availability, integrity, and confidentiality—adapted to physical-process safety—is central to these analyses [40,41].

Threat-modelling frameworks such as STRIDE, DREAD, and PASTA provide expert-driven, qualitative assessments [42–45]. They are lightweight and scalable but subjective. Quantitative approaches employ probabilistic or game theoretic models, Markov chains, Petri nets, and Bayesian networks to assign measurable likelihoods and impacts [46–49]. These offer reproducibility but rely on reliable datasets that are often unavailable in CPS contexts.

Model-based methods, attack trees [50], state machines [46], reachability analysis [51,52], and hybrid automata [53,54] dominate the CPS literature due to their interpretability and formal structure. Data-driven techniques using CNNs, reinforcement learning, and deep RL frameworks [55–57] learn patterns directly from telemetry, providing adaptability but demanding extensive data and facing explainability gaps.

Informal frameworks and attack surface catalogues [58,59] support quick scoping but lack rigour. Formal verification using model checking, SMT solving, or probabilistic model checking delivers mathematical soundness for smart-grid and vehicular CPSs [52,53,60–63]. Such methods are computationally expensive and face state-space explosion in complex networks.

Across CPS studies, qualitative methods dominate early-stage assessments; quantitative and model-based techniques provide depth but require significant computational and data resources. These results are also presented in Table 4. These insights establish a methodological foundation that later WPP-specific studies build upon to address domain-particular cyber–physical couplings.

Table 4. Examination of the cyber risk analysis methods for CPSs.

Framework/Tool	Approach	Technique	Method	Reference Literature
DREAD	✢	★	❍	[42,44]
STRIDE	✢	★	❍	[43,44]
Cyber Kill Chain	✢	★	❍	[64,65]
MITRE ATT&CK	✢	★	❍	[66–68]
OCTAVE Allegro	✢	★	❍	[69]
Simulation	✦	★	❍	[70–72]
Attack Trees	✦	★	◗	[50,73]
PASTA	✤	★	❍	[45]
Model Checking	✤	★	●	[46,60,74]
Theorem Proving	✤	★	●	[75]
Probabilistic Model Checking	✤	★	◗	[62,63]
Reachability Analysis	✤	★	●	[52–54]
Online Risk Assessment using CNN	✤	☆	❍	[55]
DRL-based risk analysis	✤	☆	❍	[56]
ML-based threat identification	✤	☆	❍	[76]
SARSA Framework	✤	☆	❍	[57]

Approach: ✤ = Quantitative, ✢ = Qualitative, ✦ = Semi-Quantitative; **Technique**: ★ = Model-Based, ☆ = Data-Driven; **Method**: ❍ = Informal, ◗ = Semi-formal, ● = Formal.

In relation to **RQ1** and **RQ2**, these 36 CPS-focused studies show that a rich arsenal of cyber risk analysis frameworks exists at the generic CPS and smart-grid levels, spanning qualitative threat catalogues, probabilistic models, formal verification, and emerging data-driven methods. However, most of these frameworks are demonstrated on simplified testbeds or non-WPP domains, and few explicitly consider turbine-specific dynamics or

SCADA architectures. This gap indicates that substantial methodological knowledge is available but has not yet been systematically transferred to wind power plants.

4.2. State of the Art for Wind Power Plants

The remaining 26 studies explicitly target wind energy systems, analysing cyber threats, risk propagation, and safety impacts within turbine and SCADA infrastructures. This section presents those domain-specific results, which adapt or extend general CPS methods to WPP architectures.

Qualitative investigations—including attack surface mappings and STRIDE-based analyses [59,64,65,70,77]—support practitioner awareness but lack numerical precision. Quantitative approaches apply Bayesian networks and Markov decision processes to offshore WPPs [48,49], producing probabilistic risk estimates yet demanding reliable data and substantial modelling effort.

Model-based techniques predominate: automaton-based turbine controllers verified via model checking [74], SMT-based false-data-injection frameworks [78], and stochastic CPS process models [46]. Emerging data-driven work applies CNNs, reinforcement learning, and hybrid ML–formal methods [55,57,76] for adaptive detection. These enhance scalability but remain constrained by limited labelled datasets and hardware limitations on embedded controllers.

Informal vulnerability catalogues for generators and SCADA nodes [71] offer broad coverage but qualitative results. Formal methods—model checking, reachability, and probabilistic reasoning—provide objective verification [47,74,78] yet face scalability challenges across multi-turbine farms.

WPP research demonstrates gradual migration from conceptual CPS frameworks to specialised models that capture turbine-specific cyber–physical dynamics. Formal frameworks such as finite-state machines, timed and hybrid automata, Petri nets, Bayesian graphs, and MDPs ([46–49,52–54,74,79,80]) each contribute distinct advantages. Across the formal modelling frameworks in Table 5, a clear trend emerges. Methods based on finite-state machines, timed automata, and Petri nets are typically applied to isolated subsystems—such as a single turbine controller or communication protocol—where state spaces remain manageable. Hybrid automata and probabilistic models extend this analysis to continuous dynamics and stochastic behaviour, but they are rarely scaled beyond small case studies. Almost none of the reviewed works demonstrate farm-level verification or consider heterogeneous fleets with varying turbine types and communication topologies. This indicates that, for WPPs, the maturity of model-based techniques is still at the subcomponent or single-system level, with system-of-systems analysis largely absent.

AI/ML integration faces further barriers: turbine-side devices have limited computational resources, hindering deployment of deep networks. Lightweight or federated ML architectures (e.g., TinyML and model compression) are therefore needed for real-time edge inference. Future studies should explore hybrid computation that balances latency, accuracy, and energy efficiency for secure, safe turbine control.

As shown in Figure 9, only a minority of studies explicitly link cyber events to physical safety outcomes. Attacks on SCADA loops can cascade into turbine instability, gearbox damage, or grid disconnection, yet such scenarios are seldom quantified. Offshore and floating farms remain under-represented despite distinct cyber–physical risks and communication challenges. Thus, only a small subset of methods simultaneously addresses cyber–physical coupling, safety consequences, and WPP-specific architectures. Many studies remain confined to one or two dimensions. For example, studies either focus on SCADA communication security without modelling turbine mechanics or analyse turbine faults without adversarial behaviour. This pattern suggests that most current work stops at

identifying vulnerabilities or attack paths, without quantifying how these translate into physical damages. Consequently, even when cyber risks are analysed, decision-makers receive limited guidance on safety implications, which directly affects the applicability of these methods to real WPP operations and to **RQ3**.

Table 5. Formal modelling frameworks for cyber risk analysis in CPSs.

Modelling Framework	Description	Benefits	Limitations	Reference
Finite State Machines	Model CPS behaviour as a set of discrete states with transitions, capturing system dynamics and attacker actions.	Suitable and verifiable for discrete systems and control logic.	Limited for continuous dynamics and concurrent systems.	[46]
Timed Automata	Extends FSM with clocks to model time-dependent behaviour, used for real-time CPS risk analysis.	Captures timing constraints, ensures real-time safety.	Complex to model, computationally intensive.	[74]
Hybrid Automata	Combines discrete states and continuous dynamics to model CPSs with physical and cyber components.	Handles continuous and discrete behaviour.	High complexity, scalability challenges.	[52–54]
Petri Net	Graphical and mathematical model using places, transitions, and tokens to represent concurrency, resource flow, and CPS interactions.	Models concurrency well, visually analysable.	State explosion for large systems, limited for continuous dynamics.	[79,80]
Bayesian Graph	Probabilistic directed acyclic graph modelling dependencies to estimate cyber attack frequencies and risks in CPSs.	Handles uncertainty using probabilities, good for CPSs.	Requires valid probability data.	[47,48]
MDP	Models states, actions, and probabilities to assess risks and optimise attack mitigation in CPSs.	Quantifies decisions under uncertainty, optimisation.	Computationally intensive, needs accurate probabilities.	[49]

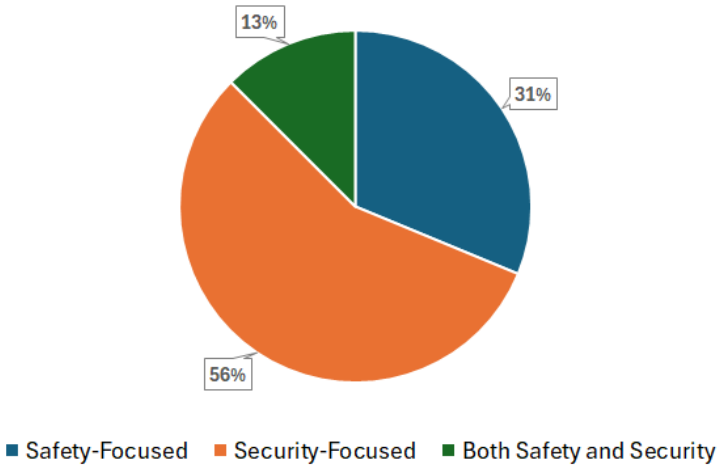

Figure 9. Integration of safety and security dimensions in reviewed WPP studies.

As illustrated in Figure 10, applicability of cyber risk analysis approaches also varies with the size of WPPs. It shows the trend of the studies according to our synthesis framework presented in Section 3. Purely formal methods can assist us with giving the highest level of security and safety affirmations for a few wind turbines but become intractable as the size of the system increases [81]. As the system grows in size, applicability of informal methods rises. This is because they are computationally inexpensive and easier to apply. But, due to the fact that they are subjective, it may not be possible to draw safety guarantees from them. Semi-formal and probabilistic methods establish a balance by modelling the

system in an abstract way and making some inference in terms of probability of safety or security compromises. These methods have the potential to analyse the risk at the wind farm level. But, again due to the abstraction, it may not be possible to link security compromises with hazards [73]. This fragmented coverage explains why some methods meet the operational and safety requirements and some only fulfil security directions, identified in **RQ4** and highlighted later in the Discussion. Hybrid frameworks that blend formal verification with data-driven adaptability appear most promising for achieving comprehensive, scalable cyber risk assessment in future renewable energy systems. For instance, modelling the system using machine learning and then drawing the safety certificates for the system may be an interesting direction. In this way, one can reduce the effort required for modelling these large state-space systems and put more work into establishing safety guarantees.

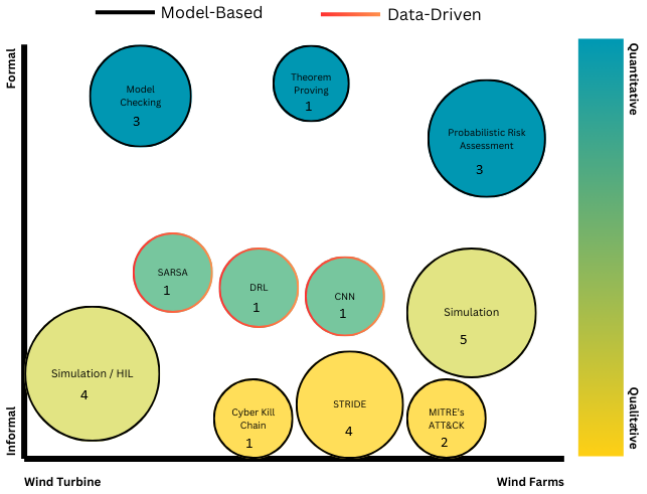

Figure 10. Scope of cyber risk analysis methods applied to WPPs.

These 26 WPP-specific studies reveal that existing cyber risk frameworks for wind energy are dominated by qualitative and model-based approaches, with only a small number of formal and data-driven methods tailored to turbine controllers or farm SCADA networks. It is because dynamical modelling of WPPs is difficult due to their electromechanical nature as compared to other renewables like solar, where the system dynamics are purely electrical. Security compromise in a single turbine may cause rotor overspeed, which can lead to fire or blade fragmentation, which may cause further physical destruction along with grid blackouts. The taxonomy in Table 5 and related text show that finite-state machines, timed and hybrid automata, Petri nets, Bayesian graphs, and MDPs are the main formal modelling paradigms used, each trading off rigour against scalability and data needs.

The results provide the following answers to the research questions. For **RQ1**, a diverse set of cyber risk analysis frameworks exists, but only a subset has been adapted specifically to wind power plants. For **RQ2**, the taxonomy reveals clear trade-offs between qualitative, model-based, and data-driven approaches, with formal methods offering assurance but limited scalability and ML-based techniques offering adaptability but weak validation. For **RQ3**, only a minority of studies integrate safety and security in a unified manner, and even fewer quantify safety outcomes. For **RQ4**, common gaps include data scarcity, limited scalability of formal models, under-representation of offshore and floating WPPs, and the lack of hybrid frameworks that combine formal rigour with data-driven adaptability.

5. Discussion and Research Gaps

This discussion integrates the evidence gathered from the 62 studies included through the PRISMA-guided systematic review. By comparing generalised CPS research

(Section 4.1) with domain-specific analyses for wind power plants (Section 4.2), we identify methodological trends, limitations, and opportunities for advancing cyber risk analysis in renewable energy systems.

5.1. Cross-Domain Comparison

Across all the reviewed literature, qualitative and semi-quantitative approaches, such as STRIDE, DREAD, MITRE ATT&CK, and the Cyber Kill Chain, remain the most widely adopted, representing roughly 45% of included works. These frameworks are valued for accessibility and communication but provide only descriptive threat mappings. Quantitative and model-based techniques (approx. 35%), including Bayesian networks, Markov decision processes, and Petri nets, offer formalism and reproducibility but depend on scarce probability or operational data. Data-driven or hybrid AI/ML approaches (approx. 20%) are emerging but remain under-validated due to dataset limitations and computational constraints on edge devices.

A clear pattern emerges between domains. General CPS studies emphasise methodological innovation, formal verification, probabilistic reasoning, and hybrid automata, whereas WPP-specific studies focus on adaptation and feasibility. The transition from generic CPS to WPP reveals a loss of methodological depth: only a small subset of CPS methods have been successfully contextualised for turbine controllers or SCADA networks. This gap underscores the need for systematic technology transfer between theoretical CPS models and practical wind-energy applications.

5.2. Integration of Safety and Security

A central finding for **RQ3** is that less than one-third of the WPP-focused studies explicitly model the coupling between cyber incidents and physical safety consequences. In most cases, cyber risks are characterised in terms of compromised components, disrupted communication, or loss of availability, with only qualitative statements about potential damage. This gap has concrete implications for WPP operations: without explicit models linking, for example, false-data injection on wind-speed sensors to rotor overspeed, tower loading, or emergency shutdown behaviour, operators and regulators cannot quantify how cyber incidents affect safety margins or compliance with design standards.

As a result, many existing frameworks are difficult to use for safety-informed decisions such as setting conservative operating envelopes, prioritising security investments around safety-critical subsystems, or justifying continued operation under degraded conditions. In practice, this means that even when cyber risks are assessed, there is limited evidence on whether proposed countermeasures truly reduce the probability of physical harm or large-scale grid disturbances. Formal verification studies, such as those using hybrid automata or probabilistic model checking, begin to bridge this divide yet remain computationally constrained. A future research priority is therefore to establish unified risk models that express cause-and-effect chains from cyber compromise to mechanical or electrical damage, supporting quantifiable safety metrics.

This review also reveals an interaction between data scarcity, the limited scalability of formal methods, and computational constraints on turbine-side devices. Data scarcity—stemming from confidentiality, the rarity of documented attacks, and heterogeneous turbine fleets—limits the calibration and validation of both probabilistic models and ML-based detectors. To compensate, many formal and model-based studies rely on assumed or synthetic parameters, which weakens confidence in their quantitative outputs when applied to real WPPs.

At the same time, scalable formal verification of large multi-turbine systems remains challenging: state-space explosion restricts most demonstrations to single controllers or

small testbeds, while extending models to the farm level would require abstractions that risk omitting relevant attack paths. On the other side, deploying sophisticated data-driven methods at the edge is constrained by the processing, memory, and communication capabilities of PLCs and embedded SCADA nodes. Together, these factors create a feedback loop in which limited data hampers validation, formal methods struggle to scale, and edge devices cannot easily host complex analytics—slowing down the maturation of robust, field-ready cyber risk frameworks for WPPs.

5.3. An Illustrative Example

To illustrate how the reviewed methods could be instantiated in practice, we developed a conceptual Markov decision process (MDP) model of an attacker targeting WPP SCADA components. This example, together with illustrative probability curves, is provided in Appendix A as a non-empirical proof of concept. It is deliberately separated from the PRISMA-guided synthesis to avoid conflating new modelling contributions with the systematic review itself.

In brief, the example shows how MDP-based attacker models can encode different attack paths and costs, and how probabilities of compromise evolve over time for components such as the WTCP and farm LAN. Once representative vulnerability and exploitability data become available, similar models could be used to quantify risk under different defensive strategies. This conceptual demonstration directly reflects the hybrid, quantitative directions highlighted in the emerging research priorities below.

5.4. Emerging Directions

Taken together, the differences highlighted in Sections 4.1 and 4.2 and the preceding discussion motivate several concrete research directions that directly address the methodological gaps identified for RQ1–RQ4.

- **Integrated hybrid frameworks.** Our synthesis shows that most WPP-focused studies remain qualitative or semi-quantitative and rarely combine formal models with data-driven components, despite the prevalence of such methods in the broader CPS literature (RQ2). Building on this imbalance, future work should develop approaches that combine explicit CPS models (e.g., automata, Bayesian graphs, and MDPs) with data-driven components for parameter estimation or anomaly detection, so that safety–security interactions can be quantified rather than only described qualitatively (RQ3).
- **Shared and synthetic datasets.** Many quantitative and ML-based approaches identified in Section 4 could not be transferred to WPPs because of scarce and non-representative operational data, a recurring limitation across the WPP-specific studies (RQ1 and RQ4). Future research should therefore create anonymised operational datasets or validated synthetic data generators that reflect realistic WPP architectures, attack scenarios, and environmental conditions, enabling reproducible evaluation and fair comparison of competing methods.
- **Scalable abstractions for formal verification.** Only a minority of studies apply formal verification, and those that do are often restricted to small controllers or highly simplified network models due to state-space explosion (RQ2). Designing abstraction techniques and compositional models that scale formal analysis from single devices to multi-turbine and multi-farm systems would directly address this limitation and make it possible to extend rigorous guarantees to whole WPPs.
- **Safety–security co-modelling.** For RQ3, fewer than one-third of WPP-specific studies explicitly model the coupling between cyber incidents and physical safety consequences, and even fewer link turbine-level effects to grid-level impacts. Future

frameworks should therefore develop unified risk models that encode cause–effect chains from cyber compromise (e.g., sensor tampering and SCADA intrusion) to mechanical stress, protection actions, and loss of grid services, providing quantitative safety metrics alongside conventional security indicators.

These directions provide direct responses to the specific methodological differences and evidence gaps revealed by this review, and they outline a concrete agenda for advancing WPP-focused cyber risk analysis beyond its current qualitative and fragmented state.

5.5. Synthesis

In summary, this systematic review shows that, for **RQ1**, a diverse set of cyber risk analysis frameworks exists across CPS and power systems, but only a subset has been adapted specifically to wind power plants. For **RQ2**, the proposed taxonomy reveals clear trade-offs between qualitative, model-based, and data-driven approaches, with formal methods offering strong assurance but limited scalability and ML-based techniques providing adaptability but weak validation in real WPP settings. For **RQ3**, less than one-third of WPP studies explicitly link cyber incidents to physical safety consequences, and even fewer consider both turbine-level and grid-level impacts. Addressing **RQ4** therefore requires domain-specific adaptation of rigorous CPS methods, improved data resources, and hybrid safety–security co-modelling, moving the field from descriptive threat enumeration toward quantifiable, operationally actionable risk assessment for WPPs.

A key limitation of this review is the potential database and publication bias introduced by our search strategy. We restricted electronic searches to four major digital libraries (IEEE Xplore, ScienceDirect, SpringerLink, and MDPI journals) and to peer-reviewed conference and journal papers published between January 2010 and January 2025. Relevant work indexed only in other databases published in non-English venues or reported as grey literature, such as technical reports and industrial case studies, may therefore be underrepresented in our corpus, which could skew the apparent distribution of methods across application domains and research communities.

6. Conclusions

This PRISMA-guided systematic review analysed 62 studies on cyber risk analysis for cyber–physical systems and wind power plants. For **RQ1**, a broad range of frameworks exists—qualitative threat catalogues, probabilistic models, formal verification, and emerging ML-based methods—but only a minority are explicitly tailored to WPP architectures and operational realities. For **RQ2**, the synthesis reveals clear trade-offs: qualitative approaches are widely used and easy to apply but subjective; model-based and formal methods offer greater rigour but struggle to scale beyond single controllers; and data-driven techniques provide adaptability yet remain under-validated for real farms due to data and hardware constraints.

For **RQ3**, fewer than one-third of WPP-specific studies explicitly discuss the coupling between cyber incidents and physical safety consequences, and even fewer link turbine-level effects to grid-level impacts. As a result, many frameworks identify vulnerable components but do not quantify how attacks could cause rotor overspeed, tower loading, or loss of ancillary services. For **RQ4**, the review identifies recurring gaps: data scarcity and limited dataset representativeness, poor scalability of formal methods to multi-turbine systems, under-representation of offshore and floating farms, and a lack of hybrid frameworks that combine formal assurance with data-driven adaptability.

A key conclusion is that few existing methods are fully adapted to the operational, environmental, and safety requirements of WPPs. Many CPS risk models assume stable communication and normal environmental conditions, whereas offshore wind farms face

intermittent satellite links, harsh weather, and complex maintenance logistics. Similarly, formal verification studies often focus on abstract controllers without modelling mechanical constraints such as blade fatigue or tower resonance, limiting their direct applicability. These mismatches show that direct transfer of generic CPS methods to WPPs is insufficient.

Future work should therefore move beyond general recommendations towards concrete implementation pathways. First, hybrid frameworks are needed that combine simplified formal or model-based representations of turbine and SCADA behaviour with lightweight ML components. For example, a farm-level Bayesian or automata model could define safe operating regions and expected control responses, while a compact anomaly detection model on turbine-side hardware monitors deviations in wind speed and power signals. This would combine explicit safety constraints with adaptive detection, yielding more actionable risk estimates. In practice, this would help when a false data injection attack becomes successful in deceiving the safety filter, but anomaly detection will provide the needed resilience.

Secondly, scalable abstraction techniques are needed to extend formal methods from single devices to multi-turbine and multi-farm settings. Practical options include modular verification of turbine controllers and other subcomponents. An interesting direction is to model WPPs as two aggregated group of wind turbines, where one group can represent the dynamics of healthy turbines and one group can represent the dynamics of a compromised turbine. This would enable us to study cascading effects in case of failure of one group on other and overall network grid while reducing the overall computational complexity.

Finally, safety–security co-modelling should become standard in WPP cyber risk analysis. The key idea is to combine the stochastic effects of cyber attacks with the deterministic evolution of WPPs. This would then make it possible to combine the attack actions with their effect on each control component. We can then interlink safety and security properties together to check whether a safety violation is possible via a certain attack action. Future frameworks could explicitly link the cyber compromise of a SCADA server and check the effect of different attack actions on the wind plant controller to changes in load envelopes, protection actions, and possible grid service violations, providing quantitative safety indicators alongside security metrics. Embedding these chains into risk models would give operators clearer evidence on which mitigations best reduce both cyber risk and physical hazard, supporting better design and operational decisions.

Taken together, these directions outline practical steps to adapt the rich methodological arsenal of CPS cyber risk analysis into tools that meet the specific operational, environmental, and safety demands of wind power plants.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/en19030677/s1.

Funding: This research was funded by the Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/W524554/1. The authors gratefully acknowledge EPSRC for its financial support of this work.

Data Availability Statement: No new data were created or analyzed in this study.

Acknowledgments: The assistance of Grammarly in refining the writing style is acknowledged. Microsoft Copilot (GPT-4) is also recognised as having been employed to summarise the initial notes and to proofread the final version of this document. We affirm that no content generated by artificial intelligence has been presented as the author's own work.

Conflicts of Interest: The authors declare no conflicts of interest. There is no role of any funders in the design of this study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Full Form/Description
WPP	Wind Power Plant
CPS	Cyber–Physical System
CPES	Cyber–Physical Energy Systems
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SCADA	Supervisory Control and Data Acquisition
EMS	Energy Management System
IT	Information Technology
OT	Operational Technology
ICT	Information and Communication Technology
IoT	Internet of Things
IEC	International Electrotechnical Commission
LAN	Local Area Network
WTCP	Wind Turbine Control Panel
DoS	Denial of Service
DDoS	Distributed Denial of Service
AI	Artificial Intelligence
ML	Machine Learning
CNN	Convolutional Neural Network
DRL	Deep Reinforcement Learning
RL	Reinforcement Learning
SARSA	State–Action–Reward–State–Action (RL Algorithm)
MDP	Markov Decision Process
PMC	Probabilistic Model Checking
SMT	Satisfiability Modulo Theories
FSM	Finite State Machine
UAV	Unmanned Aerial Vehicle
NIST	National Institute of Standards and Technology
NRC	National Research Council
PLC	Programmable Logic Controller
GPU	Graphics Processing Unit

Appendix A. MDP-Based Attack Model for a Wind Farm SCADA Network

We can consider the MDP-based attacker model in Figure A1 for the aforementioned SCADA network illustrated in Figure 3, where we can see that the attacker is capable of causing physical damage to our wind turbines through cyber means. It is quantified by the probability of a successful attack, which is dependent on the attacker's capability as well as the stochastic data we obtain from the exploitability and vulnerability of wind plant sub-components. Such incidents also result in significant economic losses from downtime, repair costs, and contractual penalties. More critically, they present safety hazards to both personnel and the public through the malfunctioning of turbines or other compromised systems.

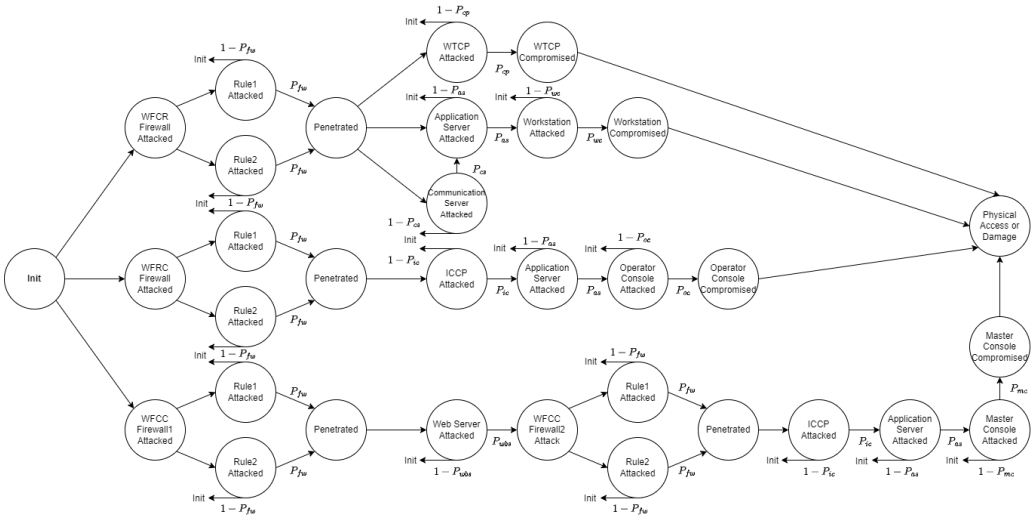

Figure A1. MDP-based attack model for wind power plants.

Although actual empirical data is required to fully implement probabilistic models, the validity of this approach can be demonstrated by using carefully curated values to obtain an overall estimate of potential outcomes. As shown in Figure A2, the probability of a WTCP compromise is the highest, reflecting the multiple attack vectors that target it. Other components exhibit lower probabilities of compromise, particularly under scenarios with limited attacker capabilities, which are inherently linked to the cost of each attack attempt.

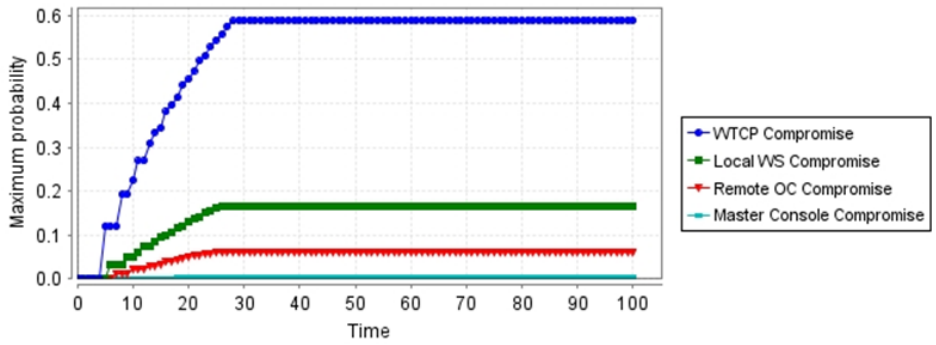

Figure A2. Max. probability of compromise vs. time at constant capability.

Additionally, Figure A3 illustrates that as the attacker's cost increases, the probability of compromise eventually stabilises near a maximum value. These findings highlight the potential utility of the approach, particularly when accurate data on the exploitability and vulnerabilities of wind plant components becomes available.

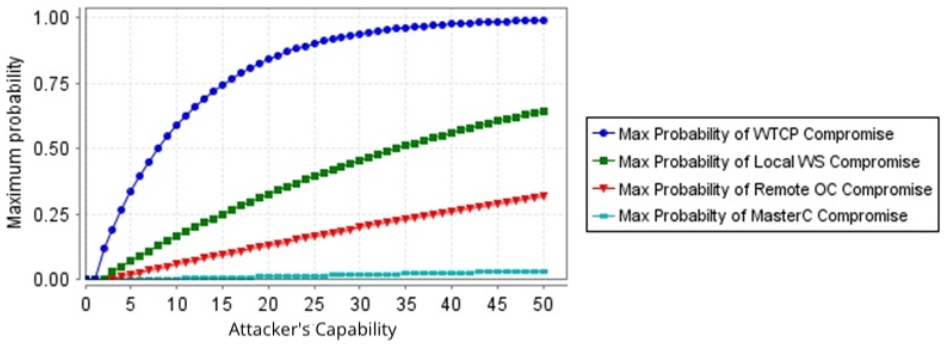

Figure A3. Max. probability of compromise vs. attackers' capability.

Overall, this proof-of-concept demonstration is intended solely as an illustrative extension of the insights gained from this review. Because it uses hypothetical values rather than operational datasets, its findings should not be interpreted as empirical results. Instead, the experiment highlights how quantitative modelling approaches—such as MDP-based attacker models—could be applied once real vulnerability and exploitability data become available.

References

1. History of Wind Energy. Available online: https://www.energy.gov/eere/wind/history-us-wind-energy (accessed on 24 June 2024).
2. Henze, M.; Hiller, J.; Hummen, R.; Matzutt, R.; Wehrle, K.; Ziegeldorf, J.H. Network Security and Privacy for Cyber-Physical Systems. In *Security and Privacy in Cyber-Physical Systems*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2017; Chapter 2, pp. 25–56. [CrossRef]
3. Cybersecurity: The Key to Safeguarding a Renewable Future. Available online: https://www.powerengineeringint.com/cybersecurity-2/cyber-security-the-key-to-safeguarding-a-renewable-future (accessed on 26 June 2024).
4. Freudenberg, W.K. Why Windfarms Need to Step Up Cyber Security. Available online: https://www.dnv.com.au/article/why-windfarms-need-to-step-up-cyber-security-128082 (accessed on 27 June 2024).
5. Cybersecurity of Wind Power a Growing Concern. Available online: https://nationalcenter.org/ncppr/2021/04/02/cybersecurity-of-wind-power-a-growing-concern (accessed on 1 July 2024).
6. Wind Farms Next Target Group for Cyber-Attacks. Available online: https://www.sirris.be/en/inspiration/wind-farms-next-target-group-cyber-attacks (accessed on 1 July 2024).
7. Egan, M. *A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience*; Boise State University: Boise, ID, USA, 2022.
8. First-of-a-Kind U.S. Grid Cyberattack Hit Wind, Solar. Available online: https://www.wind-watch.org/news/2019/11/02/first-of-a-kind-u-s-grid-cyberattack-hit-wind-solar (accessed on 1 July 2024).
9. Wind Turbine Giant Vestas Confirms Data Breach Following 'Cybersecurity Incident'. Available online: https://portswigger.net/daily-swig/wind-turbine-giant-vestas (accessed on 2 July 2024).
10. Enercon Turbines Disrupted by Satellite Cyber Attack. Available online: https://www.modernpowersystems.com/analysis/enercon-turbines-disrupted-by-satellite-cyber-attack-9935239 (accessed on 2 July 2024).
11. Wind Turbine Giant Nordex Hit by Cyber-Attack. Available online: https://www.infosecurity-magazine.com/news/wind-turbine-nordex-cyber-attack (accessed on 2 July 2024).
12. Deutsche Windtechnik Hit by Cyber Attack. Available online: https://renews.biz/77220/deutsche-windtechnik-hit-by-cyber-attack (accessed on 2 July 2024).
13. TA423/Red Ladon: Espionage in South China Sea. Available online: https://www.proofpoint.com/uk/blog/threat-insight/chasing-currents-espionage-south-china-sea (accessed on 2 July 2024).
14. Knack, A.; Hwei Syn, Y.K.; Tam, K. Enhancing the Cyber Resilience of Offshore Wind. Available online: https://cetas.turing.ac.uk/publications/enhancing-cyber-resilience-offshore-wind (accessed on 10 July 2024).
15. Ross, R.S. *Guide for Conducting Risk Assessments*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2012.
16. Krämer, B.J. Evolution of Cyber-Physical Systems: A Brief Review. In *Applied Cyber-Physical Systems*; Suh, S.C., Tanik, U.J., Carbone, J.N., Eroglu, A., Eds.; Springer: New York, NY, USA, 2014; pp. 1–3. [CrossRef]
17. Rajkumar, R.R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the 47th Design Automation Conference (DAC '10), New York, NY, USA, 13–18 June 2010; pp. 731–736. [CrossRef]
18. Cyber-Physical Systems. Available online: https://www.nist.gov/ctl/smart-connected-systems-division/iot-devices-and-infrastructures-group (accessed on 15 July 2024).
19. Moness, M.; Moustafa, A.M. A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy. *IEEE Internet Things J.* **2016**, *3*, 134–145. [CrossRef]
20. Wu, H.; Liu, J.; Liu, J.; Cui, M.; Liu, X.; Gao, H. Power Grid Reliability Evaluation Considering Wind Farm Cyber Security and Ramping Events. *Appl. Sci.* **2019**, *9*, 3003. [CrossRef]
21. Hoppa, M.A. Understanding Cybersecurity Risks in Offshore Wind Farms. In Proceedings of the Association of Computer Science Departments at Minority Institutions Conference (ADMI'23), Virginia Beach, VA, USA, 13–16 April 2023.
22. Gallardo-Calles, J.M.; Colmenar-Santos, A.; Ontañon-Ruiz, J.; Castro-Gil, M. Wind control centres: State of the art. *Renew. Energy* **2013**, *51*, 93–100. [CrossRef]

23. Covello, V.T.; McCallum, D.B.; Pavlova, M.T. *Effective Risk Communication: The Role and Responsibility of Government and Nongovernment Organizations*; Springer: Berlin/Heidelberg, Germany, 1989.
24. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef]
25. Agrawal, V. A Comparative Study on Information Security Risk Analysis Methods. *J. Comput.* **2017**, *12*, 57–67. [CrossRef]
26. Dixit, K.; Singh, U.K.; Pandya, B.K. An Integrated Information Security Risk Assessment (IISRA) Approach. In Proceedings of the XVIII International Conference on Data Science and Intelligent Analysis of Information, Stockholm, Sweden, 24–26 April 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 333–343.
27. Sanghvi, A.; Naughton, B.; Glenn, C.; Gentle, J.; Johnson, J.; Stoddard, J.; White, J.; Hilbert, N.; Freeman, S.; Hansen, S.; et al. *Roadmap for Wind Cybersecurity*; U.S. Department of Energy: Washington, DC, USA, 2020. [CrossRef]
28. What is Formal Methods? Available online: https://shemesh.larc.nasa.gov/fm/fm-what.html (accessed on 28 July 2024).
29. Beyer, D.; Henzinger, T.A.; Jhala, R.; Majumdar, R. The software model checker b last: Applications to software engineering. *Int. J. Softw. Tools Technol. Transf.* **2007**, *9*, 505–525. [CrossRef]
30. Clarke, E.M.; Grumberg, O.; Peled, D.A. *Model Checking*; MIT Press: Cambridge, MA, USA, 2000.
31. Woodcock, J.; Larsen, P.G.; Bicarregui, J.; Fitzgerald, J. Formal methods: Practice and experience. *ACM Comput. Surv.* **2009**, *41*, 1592436. [CrossRef]
32. Batra, M. Formal methods: Benefits, challenges and future direction. *J. Glob. Res. Comput. Sci.* **2013**, *4*, 21–25.
33. UPPAAL—A Model Checker. Available online: https://uppaal.org/ (accessed on 1 August 2024).
34. NuSMV—A Symobolic Model Checker. Available online: https://nusmv.fbk.eu/ (accessed on 15 August 2024).
35. PRISM—A Probabilistic Model Checker. Available online: https://www.prismmodelchecker.org/ (accessed on 15 September 2024).
36. SPIN—A Software Verification Tool. Available online: https://spinroot.com/spin/whatispin.html (accessed on 1 September 2024).
37. Nai Fovino, I.; Carcano, A.; Masera, M.; Trombetta, A. An experimental investigation of malware attacks on SCADA systems. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 139–145. [CrossRef]
38. Ali, S.; Al Balushi, T.; Nadir, Z.; Hussain, O.K. ICS/SCADA System Security for CPS. In *Cyber Security for Cyber Physical Systems*; Springer International Publishing: Cham, Switzerland, 2018; pp. 89–113. [CrossRef]
39. Farwell, J.P.; Rohozinski, R. Stuxnet and the Future of Cyber War. *Survival* **2011**, *53*, 23–40. [CrossRef]
40. CIA Triad. Available online: https://www.fortinet.com/uk/resources/cyberglossary/cia-triad (accessed on 22 July 2024).
41. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
42. The STRIDE Approach to Threat Categorization. Available online: https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers (accessed on 20 September 2024).
43. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Torino, Italy, 26–29 September 2017; IEEE: New York, NY, USA, 2017; pp. 1–6.
44. Sheikh, Z.A.; Singh, Y. A Hybrid Threat Assessment Model for Security of Cyber Physical Systems. In Proceedings of the 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 25–27 November 2022; pp. 582–587. [CrossRef]
45. Wolf, A.; Simopoulos, D.; D'Avino, L.; Schwaiger, P. The PASTA threat model implementation in the IoT development life cycle. In Proceedings of the Workshop on Tools and Concepts for Communication and Networked Systems, Virtual, 28 September–2 October 2020; INFORMATIK 2020. [CrossRef]
46. Netkachov, O.; Popov, P.; Salako, K. Model-Based Evaluation of the Resilience of Critical Infrastructures Under Cyber Attacks. In *Critical Information Infrastructures Security*; Panayiotou, C.G., Ellinas, G., Kyriakides, E., Polycarpou, M.M., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 231–243.
47. Zhang, Y.; Xiang, Y.; Wang, L. Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems. *IEEE Trans. Smart Grid* **2017**, *8*, 2343–2357. [CrossRef]
48. Gabriel, A.; Tecklenburg, B.; Guillouet, Y.; Torres, F.S. Threat analysis of offshore wind farms by Bayesian networks-a new modeling approach. In Proceedings of the ISCRAM 2021 Conference Proceedings—18th International Conference on Information Systems for Crisis Response and Management, Omaha, NE, USA, 23–26 May 2021; pp. 28–31.
49. Bashar, A.; Muhammad, S.; Mohammad, N.; Khan, M. Modeling and Analysis of MDP-based Security Risk Assessment System for Smart Grids. In Proceedings of the 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 8–10 January 2020; pp. 25–30. [CrossRef]

50. Xie, F.; Lu, T.; Guo, X.; Liu, J.; Peng, Y.; Gao, Y. Security Analysis on Cyber-physical System Using Attack Tree. In Proceedings of the 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, 16–18 October 2013; pp. 429–432. [CrossRef]
51. Clarke, E.M.; Kroening, D.; Lerda, F. A Tool for Checking ANSI-C Programs. In Proceedings of the International Conference on Tools and Algorithms for Construction and Analysis of Systems, Barcelona, Spain, 29 March–2 April 2004.
52. Bresolin, D.; Geretti, L.; Muradore, R.; Fiorini, P.; Villa, T. Formal verification of robotic surgery tasks by reachability analysis. *Microprocess. Microsyst.* **2015**, *39*, 836–842. [CrossRef]
53. Tantawy, A.; Abdelwahed, S.; Erradi, A.; Shaban, K. Model-based risk assessment for cyber physical systems security. *Comput. Secur.* **2020**, *96*, 101864. [CrossRef]
54. Jouda, F.; Mehdi, S. Safety Verification in Vehicle Test Applications: Using Reachability Analysis With the Focus on Reachability Tools. Master's Thesis, School of Information Technology, Halmstad University, Halmstad, Sweden, 2018. Available online: http://www.diva-portal.org/smash/get/diva2:1289900/FULLTEXT02.pdf (accessed on 25 August 2024).
55. Gong, Q.; Tan, S.; Wang, Y.; Liu, D.; Qiao, H.; Wu, L. Online Operation Risk Assessment of the Wind Power System of the Convolution Neural Network (CNN) Considering Multiple Random Factors. *Processes* **2019**, *7*, 464. [CrossRef]
56. Nguyen, T.T.; Reddi, V.J. Deep reinforcement learning for cyber security. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *34*, 3779–3795. [CrossRef]
57. Ibrahim, M.; Elhafiz, R. Security Analysis of Cyber-Physical Systems Using Reinforcement Learning. *Sensors* **2023**, *23*, 1634. [CrossRef]
58. Jamil, A.M.; Ben Othmane, L.; Valani, A. Threat modeling of cyber-physical systems in practice. In Proceedings of the International Conference on Risks and Security of Internet and Systems, Ames, IA, USA, 21 August 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 3–19.
59. Staggs, J.; Ferlemann, D.; Shenoi, S. Wind farm security: Attack surface, targets, scenarios and mitigation. *Int. J. Crit. Infrastruct. Prot.* **2017**, *17*, 3–14. [CrossRef]
60. Hnaini, H.; Roux, L.L.; Champeau, J.; Teodorov, C. Security Property Modeling. In Proceedings of the 7th International Conference on Information Systems Security and Privacy—ICISSP, Online, 11–13 February 2021; INSTICC; SciTePress: Setúbal, Portugal, 2021; pp. 694–701. [CrossRef]
61. Mohsin, M.; Anwar, Z.; Husari, G.; Al-Shaer, E.; Rahman, M.A. IoTSAT: A formal framework for security analysis of the internet of things (IoT). In Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA USA, 17–19 October 2016; pp. 180–188. [CrossRef]
62. Mohsin, M.; Sardar, M.U.; Hasan, O.; Anwar, Z. IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. *IEEE Access* **2017**, *5*, 5494–5505. [CrossRef]
63. Krivokuća, S.; Stojanović, B.; Hofer-Schmitz, K.; Nešković, N.; Nešković, A. Smart Water Distribution System Communication Architecture Risk Analysis Using Formal Methods. In Proceedings of the 2020 28th Telecommunications Forum (TELFOR), Belgrade, Serbia, 24–25 November 2020; pp. 1–4. [CrossRef]
64. Cyber Kill Chain. Available online: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed on 24 July 2024).
65. Sabev, E.; Pavlova, G.; Trifonov, R.; Raynova, K.; Tsochev, G. Analysis of practical cyberattack scenarios for wind farm SCADA systems. In Proceedings of the 2021 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 30 September–2 October 2021; pp. 420–424. [CrossRef]
66. MITRE ATT&CK. Available online: https://attack.mitre.org/ (accessed on 26 July 2024).
67. Zografopoulos, I.; Ospina, J.; Liu, X.; Konstantinou, C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access* **2021**, *9*, 29775–29818. [CrossRef]
68. Mccarty, M.; Johnson, J.; Richardson, B.; Rieger, C.; Cooley, R.; Gentle, J.; Rothwell, B.; Phillips, T.; Novak, B.; Culler, M.; et al. Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment. *IEEE Access* **2023**, *11*, 15297–15313. [CrossRef]
69. Caralli, R.A.; Caralli, R.A.; Stevens, J.; Stevens, J.F.; Stevens, J.; Young, L.R.; Young, L.; Wilson, W.R.; Wilson, W.R. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*; Software Engineering Institute: Pittsburgh, PA, USA, 2007. [CrossRef]
70. Yan, J.; Liu, C.C.; Govindarasu, M. Cyber intrusion of wind farm SCADA system and its impact analysis. In Proceedings of the 2011 IEEE/PES Power Systems Conference and Exposition, Phoenix, AZ, USA, 20–23 March 2011; pp. 1–6. [CrossRef]
71. Fursov, I.; Yamkovyi, K.; Shmatko, O. Smart Grid and wind generators: An overview of cyber threats and vulnerabilities of power supply networks. *Radioelectron. Comput. Syst.* **2022**, *4*, 50–63. [CrossRef]
72. Ansari, M.A.; Ghafouri, M.; Ameli, A. Cyber-Security Vulnerabilities of the Active Power Control Scheme in Large-Scale Wind-Integrated Power Systems. In Proceedings of the Electrical Power and Energy Conference, Victoria, BC, Canada, 5–7 December 2022. [CrossRef]

73. Castiglione, L.M.; Lupu, E.C. Which attacks lead to hazards? Combining safety and security analysis for cyber-physical systems. *IEEE Trans. Dependable Secur. Comput.* **2023**, *21*, 2526–2540. [CrossRef]
74. Suryadevara, J.; Sapienza, G.; Seceleanu, C.; Seceleanu, T.; Ellevseth, S.E.; Pettersson, P. Wind Turbine System: An Industrial Case Study in Formal Modeling and Verification. *Commun. Comput. Inf. Sci.* **2014**, *419*, 229–245.
75. Rashid, A.; Hasan, O.; Abed, S. Using an Interactive Theorem Prover for Formally Analyzing the Dynamics of the Unmanned Aerial Vehicles. In *Mobile Robot: Motion Control and Path Planning*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 253–282.
76. Perrone, P.; Flammini, F.; Setola, R. Machine Learning for Threat Recognition in Critical Cyber-Physical Systems. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Virtual, 26–28 July 2021; pp. 298–303. [CrossRef]
77. Yang, B.; Zhang, Y. Cybersecurity Analysis of Wind Farm Industrial Control System Based on Hierarchical Threat Analysis Model Framework. In Proceedings of the 2022 International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT), Xiamen, China, 28–30 October 2022; pp. 6–13. [CrossRef]
78. Datta, A.; Rahman, M.A. Cyber Threat Analysis Framework for the Wind Energy Based Power System. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS' 17), New York, NY, USA, 30 October–3 November 2017; pp. 81–92. [CrossRef]
79. Leveson, N.; Stolzy, J. Safety Analysis Using Petri Nets. *IEEE Trans. Softw. Eng.* **1987**, *SE-13*, 386–397. [CrossRef]
80. Singh, P.; Singh, L. Verification of safety critical and control systems of Nuclear Power Plants using Petri nets. *Ann. Nucl. Energy* **2019**, *132*, 584–592. [CrossRef]
81. Yin, X.; Li, S. Recent advances on formal methods for safety and security of cyber-physical systems. *Control Theory Technol.* **2020**, *18*, 459–461. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.