
Journal of Informatics and Web Engineering

Vol. 3 No. 3 (October 2024)

eISSN: 2821-370X

In Search of Suitable Methods for Cost-Benefit Analysis of Cyber Risk Mitigation in Offshore Wind: A Survey

Yvonne Hwei-Syn Kam^{1,2}, Kevin Jones³, Robert Rawlinson-Smith⁴, Kimberly Tam⁵

^{1,3,4,5}School of Engineering, Computing and Mathematics, University of Plymouth, Drake Circus, Plymouth PL4 8AA, United Kingdom

²Faculty of Engineering, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia

*corresponding author: (yvonne.kamhweisyn@plymouth.ac.uk; ORCID: 0000-0002-9386-0784)

Abstract - In recent years, notable incidents have highlighted the vulnerability of wind energy infrastructure, making cybersecurity crucial for the offshore wind industry. However, justifying the costs of cybersecurity measures is essential. A cost benefit analysis (CBA) is commonly utilised to support decision-making for risk mitigation. With a cost benefit analysis, risk mitigation strategies that strike an optimal balance between the costs of mitigation measures and the resulting risk reduction can be identified. This survey of literature was carried out to identify the existing proposed solutions for cost benefit analysis on cyber risk mitigation measures for offshore wind cyber physical systems. After narrowing the area scope, a systematic search across Scopus and Web of Science, yielded 18 articles, of which six met the selection criteria. It was found that there was a lack of cost benefit analysis of cybersecurity solutions for, or set in, the area of offshore wind directly. From the analysis of the surveyed works, suggestions on future directions were given. The existing literature found lacks detailed cost modelling for offshore wind, beyond general breakdowns encompassing capital, maintenance, and labour/installation expenses, risk and scenario loss. Some of the literature used contextual factors such as compatibility and effectiveness of mitigation measures, effects on OT performance, geographical location, geopolitical context, and installed rated power which could be adapted to suit offshore wind. Since offshore operations contribute significantly to costs, cost modelling and consideration of other relevant factors pertaining to this area would be beneficial if explored. As an emerging area, in the future we expect this research to be a basis and a methodology that can be expanded with a larger data set from other publications in the field. Thus, it represents an opportunity to advance knowledge in offshore wind cyber-physical systems.

Keywords— Offshore, Wind, Cyber, Risk, Mitigation, Cost Benefit Analysis, Survey

Received: 05 July 2024; Accepted: 16 September 2024; Published: 16 October 2024

This is an open access article under the [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) license.



1. INTRODUCTION

Offshore wind refers to the use of wind turbines installed in bodies of water to generate electricity. Offshore wind cyber-physical systems (CPS) refer to the integrated network of physical components and digital technologies used



Journal of Informatics and Web Engineering

<https://doi.org/10.33093/jiwe.2024.3.3.20>

© Universiti Telekom Sdn Bhd.

Published by MMU Press. URL: <https://journals.mmupress.com/jiwe>

in offshore wind farms for the generation, transmission, and distribution of electricity. In recent years, cybersecurity has become a concern for the offshore wind (OW) industry. A 2022 report [1] stated that energy executives expect more cyber attacks on the industry in the proceeding two years. They expect cyber attacks to cause operational shutdowns (85%) and damage to energy assets and critical infrastructure (84%). 74% expect an attack to harm the environment and 57% expect it to cause deaths. Forbes reported that there were 2,365 general cyberattacks in 2023 with 343,338,964 victims [2]. An increasing trend of cyberattacks has also been seen in the wind industry [3].

1.1 Cyber Incidents And Scenarios In The Wind Industry

Thus, cyber risk mitigation is an important area to allocate an organization's budget. It has become more imperative because of the high threats of cyberattack in the past years. In recent years, a series of notable incidents underscore the vulnerability of wind energy infrastructure. This has ranged from denial-of-service attacks to attacks that have disrupted communication to wind turbines. A Denial-of-Service (DoS) attack aims to overwhelm a website or network, causing degradation in performance or rendering it completely inaccessible [4]. DDoS are a form of DoS that originates from more than one source. In 2012, 50Hertz, a German wind and solar entity, fell victim to a Distributed Denial of Service (DDoS) attack on their web pages and email infrastructure [5]. In 2019, sPower, a renewables company, experienced a denial of service (DoS) attack which caused their firewalls to reboot causing communication outages. While not causing any loss of power generation, significantly impaired the company's visibility into approximately a dozen wind and solar farms, spanning California, Utah, and Wyoming [6].

Subsequently, in 2021, Vestas encountered a cyberattack on its Information Technology (IT) system, prompting the shutdown of IT systems across various business units and locations for containment. Some personal data was also made public [7]. In the following year, Viasat's KA-SAT network faced a substantial attack. 30,000 satellite communication (SATCOM) terminals were compromised, rendering them inoperative. This included ENERCON's SATCOM modems which caused them to lose communication to 5800 wind turbines across 1217 wind farms [8]. Additionally, in 2022, both Nordex Group SE [9], a major wind turbine manufacturer, and Deutsche Windtechnik [10], a turbine maintenance company, fell victim to cyber attacks, prompting a self-imposed shutdown of remote communications to wind turbines as a preventive measure. Because of the prevalence of attacks, cybersecurity is a critical aspect of the offshore wind (OW) industry to protect itself from cyber attacks.

Researchers [11] have demonstrated the risks to offshore wind farms by inserting malicious code that could manipulate physical wind turbines, potentially causing emergency shutdowns and mechanical strain. They have made case studies of the impacts of cyber attacks, ranging from wind turbine control and damage to wind farm and substation disruption and damage.

In other attack scenarios, a cyberattack could disrupt the functioning of critical systems at wind farms, leading to power outages. If these attacks were to coincide with breaches of other energy sources, the resulting power failures could be widespread. This is particularly alarming when considering the potential impact on vital services, such as hospitals, where loss of power could be life-threatening [12].

Moreover, the loss of control over wind farm systems could have immediate and dangerous physical consequences. For instance, if turbine blades were to spin uncontrollably in high winds, the excessive stress on the motors could cause fires, endangering first responders and exacerbating the damage [13].

These scenarios, together with the past incidents, illustrate the necessity of implementing and maintaining strong cybersecurity measures to protect against the growing threat of cyberattacks on wind infrastructure.

1.2 Cyber Security Spending

Cybersecurity solutions for cyber risk mitigation can be costly and therefore needs to be justified in an organisation. Gartner forecasted that spend will increase to \$215 billion in 2024, an increase of 14.3% from 2023 [14]. The number of cybersecurity solutions available, and their range of capabilities and costs, makes cost benefit analysis a critical part of an organisations cybersecurity strategy [15]. A cost benefit analysis (CBA) is commonly utilised to

support decision-making in risk mitigation. With a CBA, risk mitigation strategies that strike an optimal balance between the costs of mitigation measures and the resulting risk reduction can be identified [16].

1.3 Cyber Risk Mitigation In IT vs OT

In cyber risk mitigation there are two kinds of systems to consider, Information Technology (IT) and Operational Technology (OT). The differences in IT and OT necessitate different strategies for cyber risk mitigation.

1.3.1 Availability Takes Priority In OT

The approach to cybersecurity in offshore wind or energy OT diverges significantly from general IT practices. This is due to the paramount importance of maintaining availability. In the OT realm, the priority hierarchy places Availability (i.e., A) as the utmost concern, followed by Integrity (i.e., I) and Confidentiality (i.e., C) [17],[18]. This ordering differs with IT systems which order priority according to firstly Confidentiality, Integrity and then Availability, also known as the CIA triad. Figure 1 shows the differences in OT vs IT priorities.

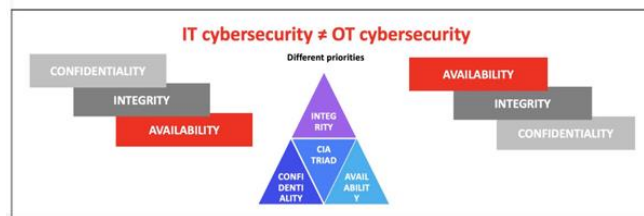


Figure 1. OT vs IT priorities [18]

The importance of availability is especially true with energy sectors which are a critical infrastructure. Thus, addressing vulnerabilities in energy systems such as offshore wind OT is imperative, as failure to remediate vulnerabilities leaves these assets susceptible to exploitation by attackers which may then cause downtime. Considering the continuous and uninterrupted operation required for energy production, such unscheduled downtime is unacceptable.

1.3.2 Purpose And Architectural Differences Between IT And OT

IT systems mainly focus on information, while OT systems are oriented towards controlling and monitoring physical processes, where the goal is to maintain availability. There are differences in architectures, protocols (e.g. MODBUS, OPC XML-DA protocols), and communication standards, thus, it is essential that that targeted and effective security strategies for OT are used.

1.3.3 Implementing Conventional IT Strategies In OT Is Not Straightforward

Employing conventional cybersecurity risk mitigations might not yield the same level of effectiveness or may not be suitable for OT systems as they may be for IT systems. An example of this is in software security updates or patching.

- Patching is problematic and can cause problems

Unlike the IT domain, OT faces unique challenges that hinder not only the development of security patches, but also in installing those patches. Several reasons contribute to this complexity, including non-compatible hardware such as legacy equipment. This includes computers running old, unsupported version of Windows for which there are no available patches, or legacy equipment that prevents the implementation of patches. Applying patches may disrupt operations, leading to periods of downtime.

- Deferred patching and its consequences

Patch management in IT is often automated and regularly deployed, whereas in OT, delay arises due to the need for uninterrupted operation [19]. Anything that may result in downtime, for example the patching process, must be meticulously planned and executed to minimize any potential disruptions. In scenarios where patches cannot be immediately installed, their deployment could be deferred until the next scheduled shutdown. Mitigation measures in OT are usually deployed during maintenance windows, rather than immediately, leaving vulnerabilities exposed until that time. Worse, they could be postponed potentially indefinitely. This deviation from traditional IT priorities underscores the unique challenges posed by the operational demands of OT.

Delays in patching could also come from the review process for patches in OT. For example, in 2019, a cyber attack happened on the firewalls that were in use in the U.S. power grid organization sPower, which caused a ten-hour disruption by repeatedly rebooting the firewalls. The were delays in the reviewing and deploying of updates, thus leaving security holes in the network for attack [20].

- Perimeter defence as an alternative to patching

To mitigate risks, alternative controls could be instituted. These may involve disconnecting the OT asset from the enterprise network or demilitarized zone (DMZ), restricting user permissions, or implementing application whitelisting to allow only essential services, thereby blocking all non-essential services. However, these methods could also result in disruption to operations. As discussed, availability can be affected not only by cyber attacks, but also conversely, mitigation measures meant to address the risk of attacks.

1.3.4 Convergence of IT/OT Increases Attack Surface

The convergence of IT and OT refers to these traditionally separate domains merging into a unified ecosystem. Convergence of IT/OT networks increases the attack surface because of the increased connectivity. Attacks in the past have shown that compromises in corporate IT can lead to OT impact. It is a trend that will continue as these once separated environments are increasingly connected [21].

1.3.5 Attack On OT Could Have Physical Effects

The impact of a cyber incident in an OT system can be different from IT because of the different kinds of losses that can arise. Offshore wind, which is the focus of this research, is composed of OT systems that coordinate physical processes. It is a cyber-physical system rather than a purely cyber system because it integrates physical processes (wind turbine energy generation) with computational elements and networks, while pure cyber systems (i.e. IT) operate solely in the digital realm without direct interaction with the physical world. OT is cyber physical and therefore effects of a cyber incident can have physical effects such as damage to equipment, and production loss besides the loss of data and information that is the norm in IT cyber incidents. For example, in 2017, hackers used the Triton virus malware to remotely take over the safety systems of a Saudi petrochemical plant and shut it down (Buli et al., 2023). Researchers [11] have also inserted malicious code to demonstrate ability to manipulate physical wind turbines, which could induce emergency shutdowns and mechanical strain.

1.4 Cost Benefit Analysis Of Cyber Risk Mitigation Considering The Needs Of IT/OT Systems, With Application In Offshore Wind

Noting the convergence of IT/OT, we abbreviate the term used, to OT, because for most part, IT systems cyber risk mitigation strategies are comparatively mature compared to OT, thus primarily the focus of the following discussion will be towards mitigation strategies that affect OT systems. Similar to IT systems, the process of cyber risk mitigation in the OT environment is not only intricate but costly [22].

Because an organization's cybersecurity investment has financial considerations, there should be justification for investment in mitigation measures. When determining the most effective strategy, a cost-benefit analysis (CBA) becomes crucial. There CBA can be used to analyse and evaluate between mitigation measures.

A cost-benefit analysis is the process used to measure the benefits of a decision or taking action minus the costs associated with taking that action [23].

In CBA of OT systems, the expense and effort associated with potential disruption-causing mitigation methods must be weighed against alternative measures. If alternative controls can sufficiently reduce the risk to an acceptable level by preventing attackers from reaching the vulnerable assets, these measures can be considered to determine the most pragmatic approach. In essence, the decision of control measures hinges on a careful consideration of the potential impact, costs, and effectiveness of the control measures in the unique context of the OT environment.

There could be a need to consider the differences in CBA for OT systems, because of, for example, the physical losses that can arise with cyber physical systems in contrast to purely cyber systems. Other essential considerations in a CBA include the suitability of the mitigation measures used in IT systems to be implemented in OT systems, and the timing of deployment, to name a few. Mitigation measures that could be routine to implement in IT may need additional consideration and change management in an OT environment. These could mean different kinds of costs and benefits need to be considered. Thus, cyber risk mitigation cost benefit analysis methods for energy OT applications often have additional considerations that are contextual to the application [24].

Nonetheless, even within the energy sector, OW has substantial differences to other sectors that need to be taken into account, for example the offshore components which necessitate remote access, and with that the associated increase of attack surface. It is not as straightforward to apply a mitigation measure if it involves going offshore as opposed to carrying out cybersecurity modifications onshore. These affect the costs of a cyber incident, and the applicability and costs of mitigation measures.

Thus, there is a need to provide a means to evaluate risk mitigation for offshore wind with visibility and clarity in terms of cost benefits before proceeding with security investment. Cost benefit analysis of offshore wind cyber risk mitigation measures can aid in decision making for selecting the most appropriate cyber risk mitigation measures.

Hence, there is a need for comprehensive cost modelling and cost benefit analysis for cyber risk mitigation measures in offshore wind. This paper presents a literature survey of the methods for decision support using cost benefit analysis for cyber risk mitigation measures in offshore wind.

The remainder of this work is arranged as follows. Section 2 explains the procedures that were used for doing the literature survey. Section 3 presents the results, which are then discussed in Section 4. Finally, Section 5 marks the end of the study.

2. METHODS

This section describes the literature review on mitigation analysis and evaluation via cost benefit analysis for decision support on cyber risk mitigation measures for offshore wind. The review covers the current state of the art (up to September 2024). The section is structured as follows: The first part is the background of the study. It shows the position of the topic within the wider area of CBA for risk mitigation. After narrowing the focus area of the review, a systematic literature review (SLR) was carried out.

2.1 Focus Area Scoping: Cyber Risk Mitigation Cost Benefit Analysis

The methodology for this literature review follows the inverted triangle paradigm (Figure 2), where it starts out with the broad issues, followed by the studies that overlap with this research topic and thereafter narrowed down to studies that are directly related to this research topic [25].

Cost benefit analysis (CBA) of risk mitigation measures has been carried out in different sectors. In this research, we are concerned with cyber risk mitigation. NIST defines cyber risk as risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system [26].

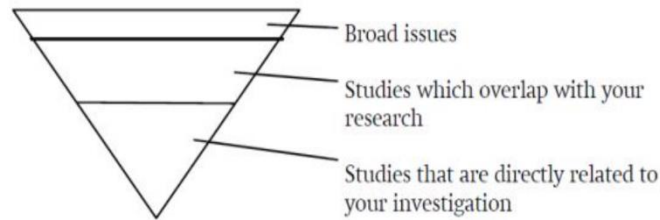


Figure 2. Literature Review Using Inverted Triangle Methodology [25]

Figure 3 shows the literature background on CBA for risk mitigation measures in terms of the works in sectors relevant to this research. It shows the positioning of my research area which is cyber risk mitigation in offshore wind OW (coloured), within the wider area of CBA for risk mitigation.

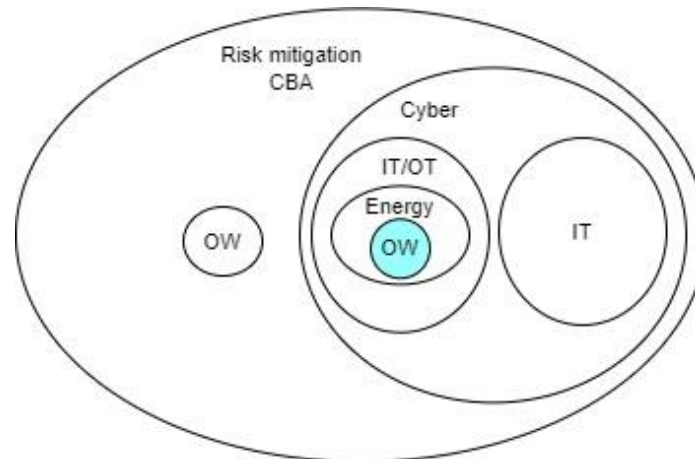


Figure 3. Background Literature And The Positioning Of The Research Topic (Coloured)

Figure 4 shows information similar to Figure 3 but in the form of a structure chart to view the breakdown of the wider topics that led to this project's research area which is CBA of cyber risk mitigation in OW. The breakdown of research on CBA for risk mitigation in different areas is shown.

Risk mitigation is broken down into cyber risk mitigation, which is what the study is concerned about, and non-cyber risk mitigation which encompasses everything else. CBA of risk mitigation is an important analysis tool which is used in all kinds of fields, not only cyber risk. Examples of risk mitigation that is not cyber specific include mitigation of construction risks [27], property risk [28] and petroleum filling risk [29]. Mitigation of risks related to offshore or OW that are not cyber specific are also in this wider category: examples include maritime operations, an offshore resource center, motherships, and remote inspection [30], [31], [32], [33].

Under cyber risk mitigation there are CBAs dealing with IT systems and IT/OT converged systems. There are a number of existing works on CBA for IT systems, such as [31], [33], [35], [37]. They incorporate general costs and benefits such as implementation costs and loss from attacks, that can serve as a general template for OT systems. However, they could lack considerations for contextual factors that are of concern for OT systems. As another example, papers [32], [34], and [36], which are dealing with CBA for IT systems, considered broadly applicable costs such as implementation costs, usability costs, and residual risks. Nevertheless, their framework assumes certain input prerequisites and set up before being able to be used. For example, specific network configuration information, which require software configuration in the context of computer networks, which may not be applicable to OT systems. Thus, for the reasons discussed, it may not be suitable to simply port over previous works on CBA of IT mitigation measures directly to converged IT/OT systems.

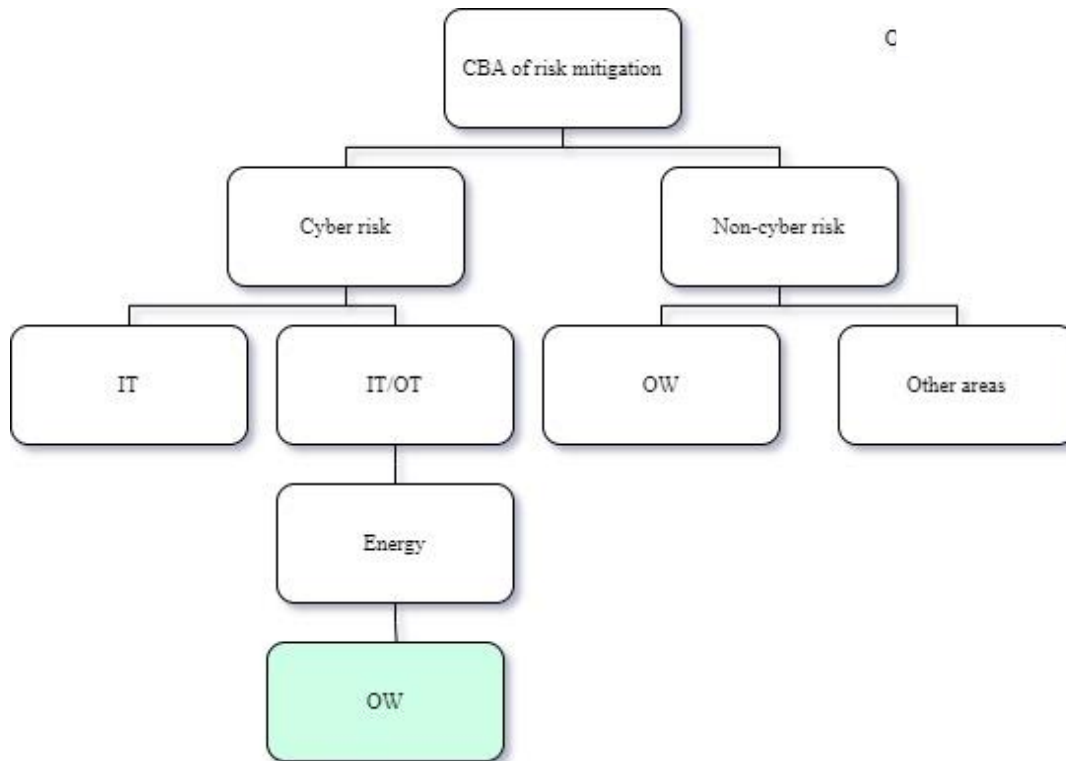


Figure 4. Structure Chart Of The Literature In Cost Benefit Analysis Of Risk Mitigation

Converged IT/OT systems are in the realm of cyber-physical systems. Cyber-physical systems (CPS) are the outcome of the IT/OT convergence. They are systems that coordinate sensing, computation, control, networking, and analytics to interact with the physical world [41]. This term which emphasises the interaction with the physical world is apt to be used for offshore wind which has cyber control and communication with wind turbines. Under the category of IT/OT or CPS systems lies different sectors. The sector of interest is energy systems, which offshore wind falls under.

Thus, the narrowed area of focus is cost benefit analysis on cyber risk mitigation measures for offshore wind cyber physical systems. The following section details a literature search based on the focus area.

2.2. Systematic Literature Review (SLR)

An SLR was carried out for the topic: cost benefit analysis on cyber risk mitigation measures for offshore wind cyber physical systems, in four phases generally following the PRISMA method [42].

- 1) *Identification*: A literature search was conducted firstly by referencing the following research question (RQ), which has the following key words (underlined):
 RQ: What are the proposed solutions for cost benefit analysis on cyber risk mitigation measures for offshore wind cyber physical systems?
 Synonyms and related words were then added for the important keywords. This review draws on articles found in two digital libraries: Scopus and Web of Science.
- 2) *Screening*: At this stage, article duplicates are checked and merged. This is followed by screening the articles that appear in the search results. The screening process involved reading the title, abstract, and keywords, and ensuring that they are written in English. The articles must mention:
 - a. dealing with cyber risk
 - b. cost benefit analysis of alternative mitigation measures
 - c. the setting is CPS or OT or ICS

- 3) *Eligibility*: Following the screening procedure, a selection is made by reading the articles to see if they can answer the research question.
- 4) *Included*: At this point, papers that are chosen will be used in the qualitative synthesis.

3. RESULTS

The following search query was used to search within the title, abstract and keywords:

(cyber*) AND (risk* OR attack*) AND (mitigation* OR reduction* OR mitigate* OR reduce* OR protect*) AND ("cost* benefit* analysis" OR "benefit* cost* analysis") AND (ot OR "Operational Technology" OR ics OR "industrial control system" OR "cyber physical" OR cps) AND (wind OR offshore)
 It returned one result (after removing duplicates), which is [22].

In order to have more results, the search terms were widened to include the adjacent sectors related to offshore wind namely energy, and electrical power sectors to find more applicable works. The widened search query used was:

((cyber*) AND (risk* OR attack*) AND (mitigation* OR reduction* OR mitigate* OR reduce* OR protect*) AND ("cost* benefit* analysis" OR "benefit* cost* analysis") AND (ot OR "Operational Technology" OR ics OR "industrial control system" OR "cyber physical" OR cps) AND (wind OR offshore OR energy OR electric* OR power))

which produced 18 results. After the screening process it was found that six of the papers did not fulfil the criteria, thus they were excluded. The process is shown in Figure 5.

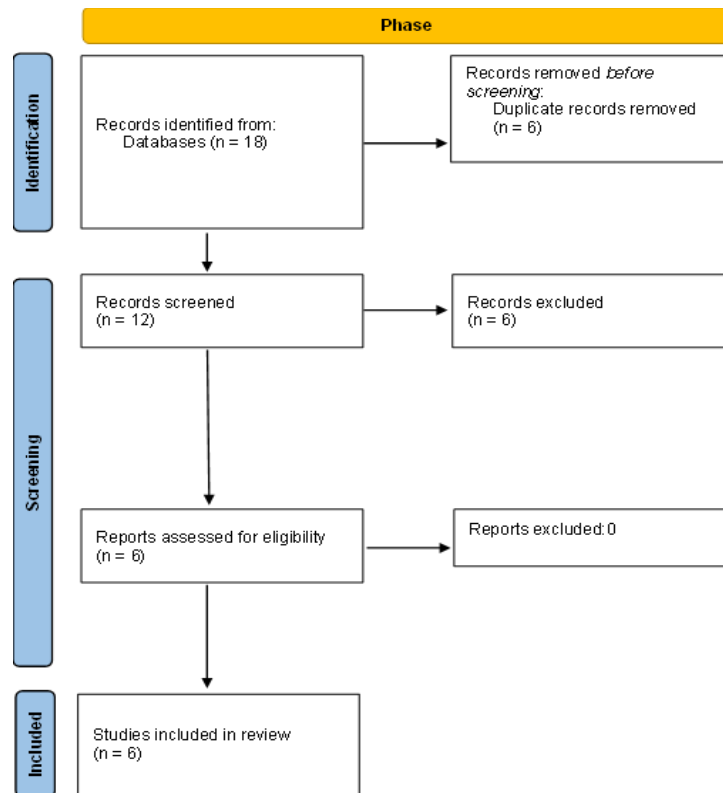


Figure 5. SLR Process

The included results are presented in Table 1.

Table 1. Relevant Work

	Works	Focus/Area	Form of CBA	Cost Model
1.	[43]	Electricity transmission and distribution	Based on risk reduction. Calculated in proportion to a risk score. Does not include cost of control measure.	Scenario loss. Scale of impact of incident {minor, major, catastrophic}, function of control, control availability by site and over time, control effectiveness, threat routes, profile, likelihood, and types
2.	[22]	Wind	CBA using Payback period compared with breach cost	Capital, maintenance, labour, cyber and physical resilience
3.	[44]	Electric power grid	Multi-objective optimization for portfolios of security measures	Mass disconnects, probability of catastrophic impacts, compatibility & effectiveness of mitigation measures. Cost for mitigation measures taken from NESCOR's[45] illustrative costs
4.	[46]	Solar nanogrids	Cost difference: Compares total costs of security implementation and projected intrusion losses	Security grade, Cost of protection, installation, maintenance, geographical location, geopolitical context, installed rated power, with breakdown for several scenarios.
5.	[47]	SCADA systems	Optimisation of Return on Investment (ROI)	Risk exposure, Risk mitigation percentage, overall protection costs, discount percentage
6.	[48]	Wastewater	Expected annual loss (ALE)	Costs associated with sewer overflows. Defense costs: recurring (Trust Anchor (TA) HW, SW, training and key updates) and Non-recurring Costs (TA HW, SW, BIDS and training)

/ - paper contains that topic, x - paper does not contain that topic

TA - Trust anchor, HW – Hardware, SW – Software, BIDS - behavioural intrusion detection system

4. DISCUSSION

The following section discusses the results in terms of their number, provides an analysis of the methods regarding their suitability of implementation in offshore wind and proposes some future directions.

4.1 Number Of Results

The relatively low number of literature search results in this paper concurs with a previous statement by [22] that limited research has been conducted on quantifying the cost-benefit trade-offs of security tools within operational technology applications. In general, there is little work in the area of CBA for cyber risk mitigations in the energy sector, which includes offshore energy and renewables like OW.

The paucity of research in this area is not unexpected, as the energy industry, not least the offshore sector is recently becoming increasingly aware of the sector's vulnerability to emerging cyber threats [49]. In the past, the air gap was applied in SCADA systems which perpetuated the myth of the air gap being still active but that is no longer true [50]. In recent years, attacks on energy infrastructure have been increasing alongside IT and OT convergence dissolving the air gap [51]. Cybersecurity management is matured and constantly upgraded for the IT sector but the process is slower and more nuanced for the OT sector. Cybersecurity for OT has just in the last several years begun to be taken

seriously across the industry [52]. Since energy is a niche area of OT, it makes sense that there are less papers in the area and even less for offshore wind which is an emerging area.

As such, it is vital that the study highlights this research gap. The result, showing only a few eligible studies, underscores gaps in knowledge to be filled, akin to how empty systematic reviews can be used to identify information deficits [53].

4.2 Analysis Of Results

The surveyed CBA methods were examined for suitability for use in offshore wind cyber physical systems. The criteria followed for the paper selection were namely, pertaining to wind, cost benefit analysis of cyber risk mitigation measures, and set within CPS/OT/ Industrial Control System (ICS), to find if there are existing proposed solutions for cost benefit analysis on cyber risk mitigation measures for offshore wind cyber physical systems. The results indicate that all the papers dealt with most of the criteria, except wind, where only one of the papers was set in the area of wind. These papers included case studies to illustrate their methods.

It was found that the methodology of cost benefit analysis used in the papers was not uniform as they did not all use the same method of calculation so there was variety in the cost benefit methods that could be employed. Moreover, for papers [43] and [22] the calculation of cost benefit was not the main focus of the paper. They focused more on the risk reduction using control measures [22] and risk scoring [43]. For [43], the CBA did not include the cost of implementing the controls and thus was not a complete CBA, but presented a projection of the savings from cyber attacks with control measures in place. The cost was in large ranges (£1 million, £10 million, £100 million) rather than actual detailed estimates. Furthermore, the cost modelling was not described in the paper and thus the breakdown of what costs were included was not clear. In reference [44], the authors refrained from conducting cost modeling, instead opting to derive the indicative costs of control measures from a 2015 compilation by the National Electric Sector Cybersecurity Organization Resource (NESCOR) [45].

Generally, there are broad costs from cyber risk mitigation measures such as capital, maintenance, labour/installation, projected losses from a scenario and benefits such as risk reduction. However, since the methods surveyed were aimed at specific application areas, they added their own factors of consideration when it was insufficient to use the general cost benefit factors. In some works, additional factors that come from the mitigation context were used to customise the cost benefit analysis. For example, the paper [22] formulated and calculated physical resilience as a measure of risk. The authors of [46] had a baseline case, but also a specialised case where they considered geographical location, geopolitical context, and installed rated power which made their analysis more apt to their area of solar nanogrids. This is because geographical location affects levels of irradiance, which affects solar power generation and geopolitical context affects energy prices respectively. These customizations for the context made the cost benefit analysis more apt for the situation. However, these customizations were not intended for other areas such as offshore wind. In the context of wind in general, there was one work [22] which focused on a case study to demonstrate cybersecurity resilience in wind energy sites. For cost benefit analysis, the authors included a simple costs of mitigation measures vs cost of attack estimation.

The mitigation measures considered in the works were largely IT/OT network related but no consideration was given to mitigation measures which involves going offshore. The mitigation measures that Mccarty et al. [22] considered were mitigation measures conventionally used and implemented in onshore IT/OT networks, such as encryption, access control, network-based and host-based intrusion detection system (NIDS, HIDS), Security information and event management (SIEM) and security orchestration, automation, and response (SOAR). Similarly, references [46] and [48] also made several scenarios of control measures which were IT/OT network related but these were not for offshore wind.

Overall, the surveyed existing literature lacks detailed cost modelling for cyber risk mitigation in offshore wind. Consequently, the cost benefit analysis and modeling utilized in these studies do not adequately suit the specific context of offshore wind, which constitutes a research gap.

As mentioned, OT systems prioritise risks to availability. It is a concern that mitigation controls could have some adverse effect on the OT system such as latency and disruption, especially on legacy components. This was

considered in some references [44] which considered compatibility of countermeasures, and reference [47] which included a discount percentage due to the performance flaws of the field devices after applying security controls.

The concerns of IT/OT convergence and interconnectedness increasing the attack surface is partially accounted for in factors such as risk exposure [47] but this could be separated into a factor of secondary risk that is caused by the mitigation measure increasing the attack surface. Physical effects, if any, caused by the mitigation measures could also be explored. In summary, the surveyed works did not delve into concerns for offshore wind nor did the case studies conducted explore any mitigation measures to be implemented offshore, thus the existing works lacked considerations for cyber risk mitigation in offshore wind.

4.3 Future Directions

From the literature, there are gaps in literature for modelling the costs and benefits of mitigation measures in offshore wind, and for mitigation analysis and evaluation using cost benefit analysis of cyber risk mitigation measures in offshore wind. Cost benefit analysis for decision support on cyber risk mitigation measures for offshore wind is an area that has not been sufficiently explored compared to other areas inside the wider area of CBA for risk mitigation. From this, we seek to establish that this area deserves further study.

It is important to utilise a CBA that is tailored for the needs of offshore wind. Offshore costs are significant, in terms of installation, operations and maintenance [54]. Similarly, offshore cyber mitigation costs are expected to be high and deserve investigation. Planning and carrying out mitigations that need offshore access or could affect physical processes offshore involves more factors in the cost modelling than what was considered in the existing works. Secondly, because offshore operations contribute significantly to costs, cost modelling pertaining to this area should be expanded to reflect this consideration. The costs could be broken down into the not just the general costs of capital, maintenance, and labor/installation expenses but relevant costs to offshore wind such as costs of crew transfer vessels, and training certification for repair crew.

Works on the CBA for offshore wind could be tailored to address the unique concerns offshore wind, for instance, taking into account the factors involved to apply a mitigation measure offshore. Factors include distance, time, weather and safety because it involves travel to the offshore location. The need for and availability of crew transfer vessel charter, trained crew and maintenance windows are other relevant factors. The framework given in the paper [44] which gave an example of relevant factors for solar power could be referenced and developed for offshore wind with reference to cost modelling such as [54]. Thus, work that is more customised to the needs of offshore wind could be developed.

5. CONCLUSION

A survey of literature was carried out to answer the research question: what are the existing proposed solutions for cost benefit analysis on cyber risk mitigation measures for offshore wind cyber physical systems? The SLR was carried out using the digital libraries Scopus and Web of Science.

The search returned 18 articles, in which 6 were selected. It was found that there were no proposed solutions for or set in the area of offshore wind directly. These papers illustrated their methods using case studies in the setting of energy sectors and general wind.

The existing literature found lacks detailed cost modelling for offshore wind, beyond general breakdowns encompassing capital, maintenance, and labour/installation expenses, risk and scenario loss. Some of the literature used contextual factors such as compatibility and effectiveness of mitigation measures, effects on OT performance, geographical location, geopolitical context, and installed rated power which could be adapted to suit offshore wind. Since offshore operations contribute significantly to costs, cost modelling and consideration of other relevant factors pertaining to this area would be beneficial if explored.

As the studies did not explore any mitigation measures to be implemented offshore or concerns for offshore wind, thus they did not include considerations directly for offshore cyber risk mitigations. From this research, we surmise that the cost benefit analysis and modeling utilized in these studies are inadequately suited to the specific context of

offshore wind. Suggestions of future directions were given based on the analysis of the gaps observed in the surveyed works.

As an emerging area, in the future we expect this research to be a basis and a methodology that can be expanded with a larger data set from other publications in the field. The low number of literature search results concurs with the assessment by other authors [22] that limited research has been conducted on quantifying the cost-benefit trade-offs of security tools within operational technology applications. Nevertheless, this represents an opportunity for knowledge to be added to the area of offshore wind cyber physical systems.

ACKNOWLEDGEMENT

This research was funded by a Supergen ORE PhD Studentship at the University of Plymouth. Special thanks to FRGS Grant (FRGS/1/2022/ICT07/MMU/03/1).

AUTHOR CONTRIBUTIONS

Yvonne Hwei-Syn Kam: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation;

Kevin Jones, Robert Rawlinson-Smith, Kimberly Tam: Project Administration, Supervision, Writing – Review & Editing;

CONFLICT OF INTERESTS

No conflicts of interests were disclosed.





REFERENCES

- [1] R. A. Coveney, "Energy executives expect more extreme cyber-attacks but defensive action is lagging, new DNV research reveals," *DNV*, 2023. [Online]. Available: <https://www.dnv.com/news/energy-executives-expect-more-extreme-cyber-attacks-but-defensive-action-is-lagging-new-dnv-research-reveals-224890>
- [2] St. John, "Cybersecurity stats: Facts and figures you should know," *Forbes Advisor*. 2024. [Online]. Available: <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/>
- [3] S. G. Freeman, M. A. Kress-Weitenhagen, J. P. Gentle, M. J. Culler, M. M. Egan, and R. V. Stolworthy, "Attack surface of wind energy technologies in the United States," *Idaho National Laboratory (INL)*, Idaho Falls, ID, INL/RPT-24-76133-Rev000, 2024, doi: 10.2172/2297403.
- [4] "Denial of Service (DoS) guidance," *NCSC*, 2024. [Online]. Available: <https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection>
- [5] L. Falk, "Power grid operators attacked via DDoS - The H Security: News and Features," *heise*. 2023. [Online]. Available: <http://www.h-online.com/security/news/item/Power-grid-operators-attacked-via-DDoS-1767170.html>
- [6] P. Paganini, "sPower it the first renewable energy provider hit by a cyber attack that caused communications outages," *Security Affairs*, 2023. [Online]. Available: <https://securityaffairs.com/93271/hacking/spower-cyber-attack.html>
- [7] S. Jacobsen, "Hackers make some Vestas' data public after ransomware attack," *Reuters*, 2021. [Online]. Available: <https://www.reuters.com/business/energy/hackers-make-some-vestas-data-public-after-ransomware-attack-2021-12-09>
- [8] M. Sheahan, C. Steitz, and A. Rinke, "Satellite outage knocks out thousands of Enercon's wind turbines," *Reuters*, 2022. [Online]. Available: <https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28>
- [9] B. Radowitz, "Nordex becomes second German OEM wind turbine maker to suffer cyberattack since Russian invasion began," *Recharge / Latest renewable energy news*. 2023. [Online]. Available: <https://www.rechargenews.com/wind/nordex-becomes-second-german-oem-wind-turbine-maker-to-suffer-cyberattack-since-russian-invasion-began/2-1-1195698>
- [10] Petkauskas, "Deutsche Windtechnik hit with a cyberattack, a third on Germany's wind energy sector," *Cybernews*. [Online]. Available: <https://cybernews.com/news/deutsche-windtechnik-hit-with-a-cyberattack-a-third-on-germanys-wind-energy-sector/>

- [11] J. Staggs, D. Ferlemann, and S. Sheno, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 3–14, 2017, doi: 10.1016/j.ijcip.2017.03.001.
- [12] A. Knack, Y. K. H. Syn, and K. Tam, "Enhancing the cyber resilience of offshore wind," 2024, doi: 10.13140/RG.2.2.33041.24162.
- [13] K. Tam, "How cyberattacks on offshore wind farms could create huge problems," *east anglia bylines*, 2024. [Online]. Available: <https://eastangliabylines.co.uk/technology/how-cyberattacks-on-offshore-wind-farms-could-create-huge-problems/>
- [14] Gartner, "Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024," 2024. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024>
- [15] S. Freeman, J. Gentle, and T. Conway, "Cyber Resiliency Within Offshore Wind Applications," *Marine Technology Society Journal*, vol. 54, no. 6, pp. 108–113, 2020, doi: 10.4031/MTSJ.54.6.10.
- [16] O. Špačková and D. Straub, "Cost-Benefit Analysis for Optimization of Risk Protection Under Budget Constraints," *Risk Analysis*, vol. 35, no. 5, pp. 941–959, 2015, doi: 10.1111/risa.12310.
- [17] M. Mesbah, M. S. Elsayed, A. D. Jurcut, and M. Azer, "Analysis of ICS and SCADA Systems Attacks Using Honeypots," *Future Internet*, vol. 15, no. 7, 2023, doi: 10.3390/fi15070241.
- [18] G. Murino, M. Ribaud, S. P. Romano, and A. Tacchella, "OT Cyber Security Frameworks Comparison Tool (CSFCTool)," *The Italian Conference on Cybersecurity (ITASEC 2021)*, A. Armando and M. Colajanni, Eds., in *CEUR Workshop Proceedings*, vol. 2940, 2021, pp. 9–22. [Online]. Available: <https://ceur-ws.org/Vol-2940/#paper2>
- [19] F. Sechi, "Critical Convergence for enhanced safety: A Literature Review on Integrated Cybersecurity Strategies for Information Technology and Operational Technology Systems within Critical Infrastructure," *European Safety and Reliability Conference*, 2023, pp. 3414–3421, doi: 10.3850/978-981-18-8071-1_P539-cd.
- [20] Cimpanu, "Cyber-security incident at US power grid entity linked to unpatched firewalls," *ZDNET*. 2023. [Online]. Available: <https://www.zdnet.com/article/cyber-security-incident-at-us-power-grid-entity-linked-to-unpatched-firewalls/>
- [21] R. Grubbs, J. Stoddard, S. Freeman, and R. Fisher, "Evolution and Trends of Industrial Control System Cyber Incidents since 2017," *Journal of Critical Infrastructure Policy*, vol. 2, no. 2, pp. 45–79, 2021, doi: 10.18278/jcip.2.2.4.
- [22] M. Mccarty *et al.*, "Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment," *IEEE Access*, vol. 11, pp. 15297–15313, 2023, doi: 10.1109/ACCESS.2023.3244778.
- [23] Hayes, "What Is Cost-Benefit Analysis, How Is it Used, What Are its Pros and Cons?," *Investopedia*. 2024. [Online]. Available: <https://www.investopedia.com/terms/c/cost-benefitanalysis.asp>
- [24] Y. Kam, K. Jones, R. Rawlinson-Smith, and K. Tam, "Taxonomy of Cyber Risk Mitigation Cost Benefit Analysis Methods for Energy Infrastructure," *IEEE International Conference on Cyber Security and Resilience (CSR)*, 2024, pp. 771–776, doi: 10.1109/CSR61664.2024.10679375.
- [25] S. Britland, "LibGuides: Literature reviews: Starting your literature review," *University of Reading*. 2024. [Online]. Available: <https://libguides.reading.ac.uk/literaturereview/starting>
- [26] C. C. CSRC NIST, "cyber risk - Glossary | CSRC," 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_risk
- [27] J. Merisalu, J. Sundell, and L. Rosén, "A Framework for Risk-Based Cost–Benefit Analysis for Decision Support on Hydrogeological Risks in Underground Construction," *Geosciences*, vol. 11, no. 2, 2021, doi: 10.3390/geosciences11020082.
- [28] K. Makka and K. Kampova, "Use of the cost-benefit analysis method in the risk management process of SMEs," *SHS Web of Conferences*, vol. 129, 2021, doi: 10.1051/shsconf/202112903019.
- [29] K. Kampova, K. Makka, and K. Zvarikova, "Cost benefit analysis within organization security management," *SHS Web of Conferences*, vol. 74, 2020, doi: 10.1051/shsconf/20207401010.
- [30] S. Basnet, A. BahooToroody, J. Montewka, M. Chaal, and O. A. Valdez Banda, "Selecting cost-effective risk control option for advanced maritime operations; Integration of STPA-BN-Influence diagram," *Ocean Engineering*, vol. 280, no. 114631, 2023, doi: 10.1016/j.oceaneng.2023.114631.
- [31] M. S. Rahman, B. Colbourne, and F. Khan, "Risk-Based Cost Benefit Analysis of Offshore Resource Centre to Support Remote Offshore Operations in Harsh Environment," *Reliability Engineering & System Safety*, vol. 207, 2021, doi: 10.1016/j.ress.2020.107340.
- [32] Y. Dalgic, I. Lazakis, I. Dinwoodie, D. McMillan, M. Revie, and J. Majumder, "Cost Benefit Analysis of Mothership Concept and Investigation of Optimum Chartering Strategy for Offshore Wind Farms," *Energy Procedia*, vol. 80, pp. 63–71, 2015, doi: 10.1016/j.egypro.2015.11.407.
- [33] O. Netland, I. B. Sperstad, M. Hofmann, and A. Skavhaug, "Cost-benefit Evaluation of Remote Inspection of Offshore Wind Farms by Simulating the Operation and Maintenance Phase," *Energy Procedia*, vol. 53, pp. 239–247, 2014, doi: 10.1016/j.egypro.2014.07.233.
- [34] G. Uganbayar, A. Yautsiukhin, F. Martinelli, and F. Massacci, "Optimisation of cyber insurance coverage with selection of cost effective security controls," *Computers & Security*, vol. 101, 2021, doi: 10.1016/j.cose.2020.102121.
- [35] M. N. Alsaleh and E. Al-Shaer, "Automated Cyber Risk Mitigation: Making Informed Cost-Effective Decisions," in *Adaptive Autonomous Secure Cyber Systems*, S. Jajodia, G. Cybenko, V. S. Subrahmanian, V. Swarup, C. Wang, and M. Wellman, Springer International Publishing, 2020, pp. 131–157, doi: 10.1007/978-3-030-33432-1_7.

- [36] A. Dutta and E. Al-Shaer, "'What', 'Where', and 'Why' cybersecurity controls to enforce for optimal risk mitigation," in *IEEE Conference on Communications and Network Security (CNS)*, 2019, pp. 160–168, doi: 10.1109/CNS.2019.8802745.
- [37] M. N. Alsaleh, "ROI-Driven Cyber Risk Mitigation Using Host Compliance and Network Configuration," *Journal of Network and Systems Management*. 2024. [Online]. Available: <https://link.springer.com/article/10.1007/s10922-017-9428-x>
- [38] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, pp. 13–23, 2016, doi: 10.1016/j.dss.2016.02.012.
- [39] M. N. Alsaleh, G. Husari, and E. Al-Shaer, "Optimizing the RoI of cyber risk mitigation," in *2016 12th International Conference on Network and Service Management (CNSM)*, 2016, pp. 223–227, doi: 10.1109/CNSM.2016.7818421.
- [40] A. B. Kayode and A. O. Ajoke, "Cost-Benefit Analysis of Cyber-Security Systems," 2016.
- [41] S. Moore, "Gartner Predicts 75% of CEOs Will be Personally Liable for Cyber-Physical Security Incidents by 2024," *Gartner*. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl>
- [42] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *BMJ*, vol. 339, 2009, doi: 10.1136/bmj.b2535.
- [43] J. D. Bewley, R. Zhang, T. Charton, and R. Wilson, "Prioritisation and cost / benefit analysis of cyber security controls within existing operational technology environments," *International Conference on Developments in Power System Protection (DPSP 2020)*, 2020, pp. 1–6, doi: 10.1049/cp.2020.0033.
- [44] P. Zebrowski, A. Couce-Vieira, and A. Mancuso, "A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems," *Risk Analysis*, vol. 42, no. 10, pp. 2275–2290, 2022, doi: 10.1111/risa.13900.
- [45] "SUPPLEMENTARY TABLES Table A1: NESCOR impact criteria with scoring system (EPRI, 2015b)," 2024. [Online]. Available: <https://onlinelibrary.wiley.com/action/downloadSupplement?doi=10.1111%2Frisa.13900&file=risa13900-sup-0001-TableS1.pdf>
- [46] P. J. Hueros-Barrios, F. J. Rodríguez Sanchez, P. Martín, C. Jimenez, and I. Fernandez, "Addressing the cybersecurity vulnerabilities of advanced nanogrids: A practical framework," *Internet of Things (Netherlands)*, vol. 20, 2022, doi: 10.1016/j.iot.2022.100620.
- [47] J. Wang, D. Shi, Y. Li, J. Chen, and X. Duan, "Realistic measurement protection schemes against false data injection attacks on state estimators," *IEEE Power and Energy Society General Meeting*, 2017, pp. 1–5. doi: 10.1109/PESGM.2017.8274291.
- [48] S. Papa, W. Casper, and T. Moore, "Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 96–106, 2013, doi: 10.1016/j.ijcip.2013.05.002.
- [49] S. Reardon, "The digital evolution: how cybersecurity is key to a successful energy transition," *Offshore*. [Online]. Available: <https://www.offshore-mag.com/energy-transition/article/14301999/dnv-the-digital-evolution-how-cybersecurity-is-key-to-a-successful-energy-transition>
- [50] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, "Forget the Myth of the Air Gap: Machine Learning for Reliable Intrusion Detection in SCADA Systems," *EAI Endorsed Transactions on Security and Safety*, vol. 6, no. 19, 2019, doi: 10.4108/eai.25-1-2019.159348.
- [51] I. Charles and Jr. Christopher, "Protecting the Industrial Control System Environment: Implementing Active Cyber Defense to Aid Mitigation of Threat Intrusions," *Proquest*. 2024. [Online]. Available: <https://www.proquest.com/docview/2445948723?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses>
- [52] V. Jesus and M. Josephs, "Challenges in Cybersecurity for Industry 4.0," *Innovation in manufacturing through digital technologies and applications: Thoughts and Reflections on Industry 4.0.*, 2018. [Online]. Available: <https://core.ac.uk/download/pdf/334461848.pdf#page=74>
- [53] R. Gray, "Empty systematic reviews: Identifying gaps in knowledge or a waste of time and effort?," *Nurse Author & Editor*, vol. 31, no. 2, pp. 42–44, 2021, doi: 10.1111/nae.2.23.
- [54] M. I. H. Tusar and B. R. Sarker, "Maintenance cost minimization models for offshore wind farms: A systematic and critical review," *International Journal of Energy Research*, vol. 46, no. 4, pp. 3739–3765, 2022, doi: 10.1002/er.7425.

BIOGRAPHIES OF AUTHORS

	<p>Yvonne Kam Hwei Syn is currently a Doctoral Researcher in the University of Plymouth, UK. Her research topic is in Cybersecurity of Offshore Wind. She is also a Certified Information Systems Security Professional (CISSP). In 2023-2024 she was as a research assistant at The Alan Turing Institute. Additionally, she is a lecturer and researcher at the Faculty of Engineering at Multimedia University, Malaysia. She has served as Principal Investigator (PI) for a few Malaysian national grants.</p>
	<p>Prof Kevin Jones is a Professor of Computing Science and the Deputy Vice-Chancellor Research and Innovation at the University of Plymouth. As DVC R&I, Kevin provides institution-wide strategic leadership, driving and supporting research excellence, innovation and impact whilst promoting interdisciplinary research, as well as driving and overseeing business ventures and collaboration, and international research partnerships. His research and teaching interests cover the Trustworthiness of Complex Systems, including Cyber Security, and is the founder member of the Maritime Cyber Threats Research Group.</p>
	<p>Dr Robert Rawlinson-Smith is a professional engineer with 30+ years of experience in the renewable energy sector. Throughout his career he balanced his involvement in commercial work with significant involvement in collaborative European and UK funded R&D activities. He is currently an associate professor in ORE Engineering School of Engineering, Computing and Mathematics (Faculty of Science and Engineering).</p>
	<p>Dr Kimberly Tam is the theme lead for Marine and Maritime at The Alan Turing Institute and Associate Professor at the University of Plymouth. Her work on maritime-cyber risk assessment, including quantifying risk, won the 2019 Lloyd's Science of Risk Prize. She was the Co-I on an H2020 Project Cyber-MAR and is the academic lead of the Cyber-SHIP lab. She is also PI on projects on cyber-resilience of AI being used for autonomous vessels and cyber resilience of offshore wind.</p>