TKI WIND OP ZEE
Topsector Energie

Research recommendations Cyber Security for Offshore Wind Energy

by Technolution
November 3, 2019

This report was commissioned by RVO (Netherlands Enterprise Agency) on request of the TKI Wind op Zee (TKI Offshore Wind).The opinions expressed in this report are entirely those of the authors (Technolution) and do not reflect the views of the TKI Wind op Zee. TKI Wind op Zee is not liable for the accuracy of the information provided or responsible for any use of the content.

Summary

The energy supply of the Netherlands will become increasingly dependent on offshore wind energy. In 2030, 11.5 GW of installed offshore wind-powered capacity should account for a generation of 49 TWh per year which equals to 32% of the electricity consumption in 2030 [ONTW-KLIM]. This energy supply is becoming of national interest and any risks, including cybersecurity risks, will have to be treated as such.

The Netherlands Enterprise Agency (RVO.nl) and Top consortium for Knowledge and Innovation Offshore Wind (TKI Wind op Zee) have a need for establishing the possible cyber risks involving offshore wind energy with the purpose of developing and refinement the research programming regarding this topic of the Top consortium for Knowledge and Innovation Offshore Wind and Topsector Energy. The Netherlands Enterprise Agency has assigned Technolution with the execution of a short independent exploratory survey.

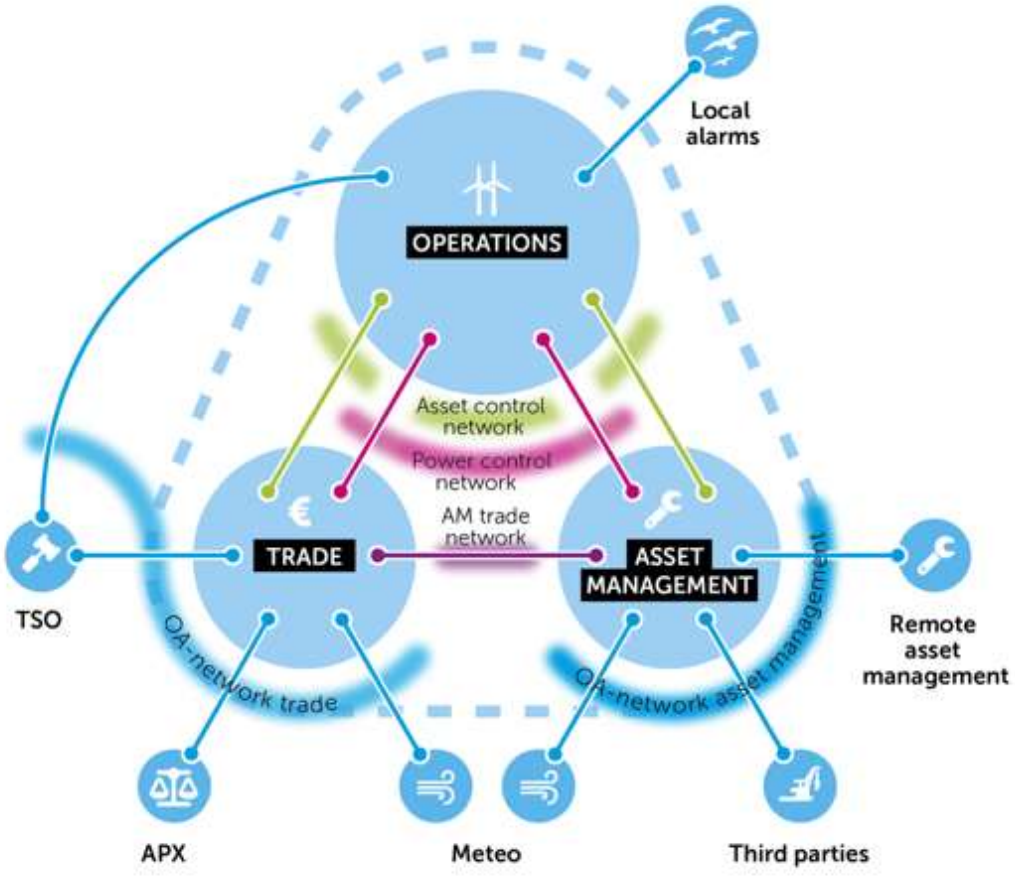
The conclusions and recommendations resulting from this survey are summarized as follows:

- Individual wind farm operators show significant awareness of cybersecurity and its importance. However, of sharing knowledge and best practices within the industry hardly any proof was found. It is therefore recommended to start a trusted community to share best practices and insights and use it to form a shared body of knowledge.
  See section 2.1.

- It is hard to uniformly ascertain cybersecurity of windfarms, due to the current diversity in setups, makes and operating models. Network technology and protocols may vary. Furthermore, an objectively certifiable framework to control cybersecurity threats and their mitigations is not maturely available. It is therefore recommended to devise and implement a fair and powerful framework, probably founded on ISO/IEC62443 and ISO/IEC61400-25.
  See section 2.2.

- A wind farm is part of an ecosystem of several parties, interfaces and subchains from regular office environments to high voltage operations. Cybersecurity threats may and will occur in one place of this ecosystem and exert negative consequences in another part, possibly under the responsibility of different parties. This research found very limited awareness and public knowledge of the shape of this ecosystem and the nature of its risks. A high-level functional architecture of such ecosystems is introduced. It is recommended to initiate a community dialogue in the sector regarding ecosystem cybersecurity and to develop an information model of the sector, possibly maturing the model in this research (see diagram on the next page).
  See chapter 3.

- In a future wind park ecosystem, many risks may occur. At this moment, classification of these risks is quite subjective. It is therefore recommended to pursue more objectified classification, for instance by rigorous resilience simulations in a ‘digital twin’. Nonetheless, based on qualitative assessment it is recommended to commence research regarding maximum cluster size (minimizing fallout from problems), advanced digital access (e.g. one-way or one-time) and resilience to integrity faults of meteo data. *See chapter 4.*



Functional architecture offshore wind energy, including networks

Inhoudsopgave

1 Introduction

Offshore wind energy is crucial when it comes to realizing the current climate objectives for 2030. From 2023 until 2030, the planned increase of energy from offshore wind farms is minimal 1000 megawatts per year for just the Netherlands. This results in an established capacity of 10,6 gigawatts of offshore wind energy in 2030. Offshore wind energy also offers great potential for long-term climate objectives. In order to be able to realize a transition to a completely CO2-free electricity system, an additional increase of offshore wind energy to an established capacity of 60 gigawatt towards 2050 is possible [ONTW-KLIM].

The future energy supply will become increasingly more dependent on offshore wind energy. The reliability and availability of the electricity supply is crucial during the integration of offshore wind energy into the energy system. In order to achieve this, the security of the energy supply needs to be in order, both the physical security as well as the cyber security.

1.1 Research goal

The Netherlands Enterprise Agency (RVO.nl) and Top consortium for Knowledge and Innovation Offshore Wind (TKI Wind op Zee) have a need for establishing the possible cyber risks involving offshore wind energy with the purpose of planning and focusing the research programming regarding this topic of the Top consortium for Knowledge and Innovation Offshore Wind and Topsector Energy. The Netherlands Enterprise Agency has assigned Technolution with the execution of a short independent exploratory survey regarding the cyber risks concerning offshore wind farms [TOR].

The primary goal of this study is to provide TKI Wind op Zee with recommendations towards programming the research and innovation agenda with regards to Cyber Security in the Dutch Offshore Wind sector.

1.2 Research focus

To ensure that this research meets up to this goal, two priorities were set to guide its focus:

1. Any innovation agenda has a long-term horizon; hence this research will focus on long-term expected security concerns. Possible current issues will be addressed were appropriate.

2. The impact of security vulnerabilities increases with scope as does the technical and organizational complexity to mitigate these risks. For a sector wide innovation agenda, it is therefore most relevant to focus on concerns from the perspective of the larger energy ecosystem around offshore wind.

The focus for this research is summarized in the following diagram.

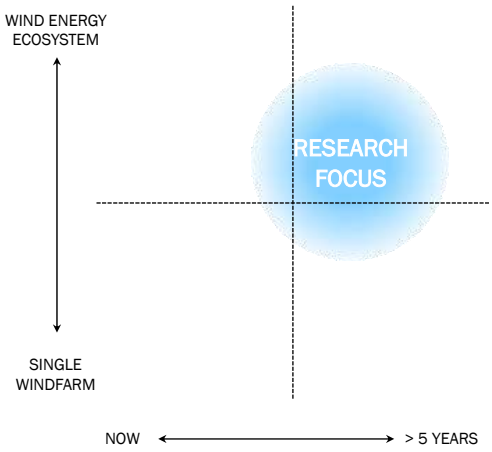


Figure 1 - research focus

1.3 Research approach

The Dutch market participants who play a role in the production of offshore wind energy in the Netherlands were invited to take part in this survey. The interviews were done based on group sessions. During the execution of the survey, Technolution used the method described in the Cyber Security for Smart Energy Guideline [HANDR-UE] in order to determine the cyber risks.

The survey was divided into three steps:

- Literature study to explore the IT/OT architecture of offshore wind farms and their ecosystems.
- Illustrating the possible security issues (scenarios) based on generic and industrial-specific security aspects.
- Discussing these scenarios with market participants in two group sessions. In order to achieve an image that is as realistic as possible, market participants from the offshore wind energy chain are invited for the group sessions.

To ensure practical usability of the study by TKI a final step was taken:

- Reviewing the findings with academic professionals on security of electricity grids and representatives of TKI.

1.4 Guide to this report

This report is not structured as a chronological account of the research process. Instead the research findings are grouped with regard to timeline (current vs. future risks) and scope (single farm vs. ecosystem risks) as depicted in

Figure 2.

All findings relevant to a single wind farm scope are found in chapter 2, with current issues in paragraph 2.1 and future issues in paragraph 2.2.

A current view on complete ecosystem security is found in chapter 3, also introducing a functional architecture model as a means to discuss ecosystem-wide information flows and risks.

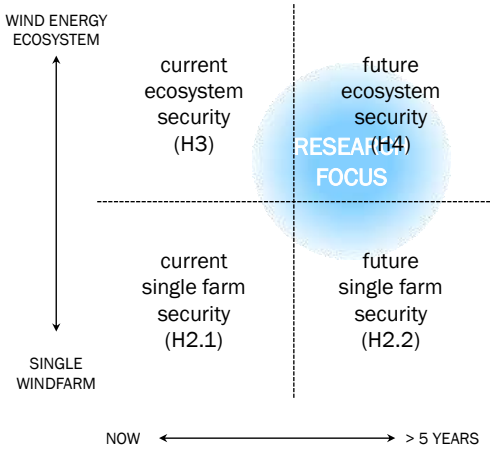


Figure 2 – structure of this report

This model is used in chapter 4 to identify and classify probable future ecosystem risks and proposed mitigations to research.

In chapter 5 all recommendations from this research are summarized.

2 Cyber Security of a single wind farm

Although the research focuses on longer term ecosystem risks, looking at the current levels of security of a single windfarm asset is a natural starting point. This chapter first summarizes the current status (2.1) as found in the investigation and then shares expectations regarding longer term security at local operations level 2.2.

2.1 Current single farm security awareness

2.1.1 Findings

- Existing offshore wind farms have been built at different times, by different contractors, using different products and they are run by different operators.
- Furthermore, we have not found cybersecurity standards or guidelines that have been uniformly applied for purposes of tendering, licensing, insurance or other means of ensuring compliance[1].
- Exploring other recent publications pertaining to the security of wind farms[2], corroborate the view that there is a strongly rising awareness in the sector of cybersecurity concerns, yet no convergence to consensus, normalization or standardization of vulnerabilities and mitigations.
- Consequently, it is very probable that currently operational windfarms have a strong diversity of existing cybersecurity risks, of possible mitigations and of the extent to which these mitigations are effectively implemented.
- It is positive to note that all wind farm operators that have been contacted for this survey were aware of cybersecurity threats and reported conducting active investigations and mitigations.
- However, several market parties declined participating in this survey, primarily in order to allocate scarce resources to their internal concerns and possibly due to concerns of sharing sensitive information.
- The market participants that participated in the group sessions have indicated they do not wish to reveal any details regarding the operational security of their networks.
- Although the current cybersecurity threat status of single windfarms is not the focus of this survey, it is definitely significant that the parties involved seem to have a strongly individual attitude towards cyber security.

2.1.2 Recommendations

- It is not opportune for any party in the Dutch offshore wind sector to compete on security. Moreover, it is probably advantageous to most current operators to share knowledge regarding cybersecurity threats.
- In comparable sectors it has been found advantageous by industry companions and even competitors to join forces to improve sector wide security awareness, quality and best practices, such as for example the *Vereniging Erkende Beveiligingsbedrijven (VEB)* and the *European Network for Cyber Security (ENCS)* specific to DSOs.

[CS1] It is recommended to set up a trusted community of operators to jointly optimize efforts of each single player. Such a community can start small, by just opening communication channels on active threats and sharing information on solutions.

[1] As an illustration the wind farm project and site descriptions [HKN-PSD], [IJM-VAL], [BWFIII-PSD], [BWFI-PSD], [NOZ-KC-2017-III], [NOZ-KC-2016] do not contain any security-related topics. [NOZ-HKZ] mentions a requirement for physical locks on all doors. See Chapter 6 for the references.

[2] See for instance the publications [DNV-WFCS], [UL-WFCS], [BH-AWF] as referenced in Chapter 6.

- With regard to the currently diversified landscape, it is not reasonable in the short term to expect conclusive uniform cybersecurity guidelines and standards. However, also in a diversified world a shared body of knowledge can be built up. The aforementioned ENCS for instance actively shares best practices[3].
- As a trusted community evolves over time, it may actively pursue and develop these best practices into industry standards. An example of this is the Payment Card Industry Data Security Standard (PCI DSS), which is under governance of the payment industry (the PCI Security Standards Council).

[CS2] It is recommended to bundle shared knowledge into a set of best practices and solutions, to use for each individual operator's cybersecurity efforts. The trusted community could play a major role in this, possibly supported by a research institute or by adjacent platforms such as ENCS.

2.2 Future single farm security measures

2.2.1 Findings

- The diversified current state that was indicated above, is not an optimal security strategy. A diversified landscape costs more efforts to survey and control and as a result more non-mitigated vulnerabilities will arise (more possible weakest links).
- For tendering, licensing and possibly insuring future wind farms it is therefore desirable to have an explicitly assessable set of norms and standards with regards to the quality and resilience of an implementation to cybersecurity threats.
- Complicating this notion is that cybersecurity threats and mitigations are generally to dynamic to be captured by a very specific standard with detailed implementation and technology prescriptions. International standards understandably take years to establish and new vulnerabilities may develop in days.
- In such situations it is generally opportune to resort to a generic standard that enforces properly sustained processes to counter cybersecurity threats, augmented with a sector specific standard that details information flows, cybersecurity risks and classifications.
- For offshore wind the most relevant generic cybersecurity standard is probably *ISO/IEC62443 – Cybersecurity for industrial automation and control systems*. This is an established standard for management control of cybersecurity in Operational Technology (OT)[4] and certification programs are widely available.
    - Adherence to a generic standard prescribing management controls must be the basis for ensuring cyber security.
    - While an industry specific standard may effectively and efficiently lower major risks across a sector, it will by nature lag significantly behind any newly occurring threats.
    - As a result, generic managerial processes to stay up to date on actual industry threats are essential for good security. Sharing industry best practices as recommended earlier in this report strongly facilitates these processes.
- As a standard specific to offshore wind it may be best to start with *ISO/IEC61400-25 - Communications for monitoring and control of wind power plants*, which provides mechanisms for authorization and logging and describes how to use it. However, it is not currently well applicable for purposes of cybersecurity control. For instance:
    - It is not a complete enumeration of data flows through a wind farm. This precludes a complete assessment of possible cyber security risks.
    - It does not provide or prescribe a mechanism for determining the impact of a breach of availability, integrity or confidentiality for the specific types of data that are described. This makes risk classification more subjective.
    - It does not provide or prescribe a method to choose the correct mechanisms for securing or separating data flows based on risk classifications.

[3] See [ENCS-PSG] as an example.

4 Comparable to the more widely known ISO/IEC27001 for Information Technology (IT) security.

    - The standard does not provide interface implementation recommendations, while actual security levels heavily depend on the exact implementation.
- The ISO/IEC61400-25 may grow to include (mechanisms to determine) cybersecurity threats and proposed mitigations, but this will take significant time. To make any such endeavour effective, to start sharing industry best practices is a major step forward.

2.2.2 Recommendations

- To ensure that any new commissions of wind farms are built and operated securely in a level playing field market (no false competition by bad security hygiene) it is of importance to swiftly converge to a national (and preferably broader!) framework for cybersecurity.
- Such a framework will probably consist of a combination of generic and specific standards, a suitable (re)certification structure and regulatory governance.
- Organizing the sector's participation, starting with planning an ambitious, yet attainable implementation roadmap and following up with a sustained industrial commitment to its governance, will be a critical success factor.

[FS1] Research the optimal cybersecurity framework to maintain throughout the offshore wind sector, including underlying standards and their certification, regulatory structure and governance, implementation roadmap and industry commitment.

- The offshore wind power specific communication implementations and the associated cybersecurity risks are distinct and significant enough (in comparison to other sectors) to require specific guidance.
- The industry size and importance probably warrant an endeavour to capture and ensure such guidance in a standardized form.
- ISO/IEC61400-25 is a good starting point for such an endeavour, albeit quite some work is needed to achieve this (as outlined before).

[FS2] Research how a specific offshore wind power cybersecurity standard can be formed and sustained, possibly starting on the basis of ISO61400-25.

3 Cyber security from Ecosystem perspective

As the share of Offshore Wind power generation increases to a projected 30%+ of Dutch electricity demand in 2030, the implications of cyber security risk will grow beyond single wind farms operators and possibly become of national concern. Therefore, it is crucial to this research to look at cybersecurity from an ecosystem perspective.

3.1 Current ecosystem cyber security awareness

3.1.1 Findings

- In 2.1 it was found that individual wind farm operators appear very security aware. However, this awareness is internally focused and seems delimited to the individual organization boundaries.
- During the workshops for this research, all participating parties (of different roles in the ecosystem) found an overarching view on the ecosystem and its cybersecurity risks insightful and relevant. It was found that sharing such views would be opportune for a larger audience in the offshore wind sector.
- The participants assessed that as off shore wind shares of energy supply grow, the impact of cybersecurity mishaps on the national electricity system will become high.
- An owner of the complete ecosystem and its risks could not be identified. The awareness of ecosystem risks, i.e. beyond individual organizations, seems limited. A community of all stakeholders in the ecosystem dedicated to cybersecurity risks was not found to exist.

- To identify and assess possible cyber security risks, it is imperative to have at least a functional model of the ecosystem and its information flows.
- However, the offshore wind communication standard ISO/IEC61400-25 does not take an ecosystem wide perspective. Neither did literature survey or verification with TU Delft provide an existing relevant model.
- Therefore, during this research and its workshops an initial ecosystem model was made. It is introduced in section 3.2 below.

3.1.2 Recommendations

- In 2.2 it was recommended to start a trusted community of wind farm operators. To maximize trust in such a community it should remain intimate and include only wind farm operators. However, an ecosystem wide view on cybersecurity also warrants a community dialogue, therefore the following recommendation:

[CE1] Set up a community dialogue on ecosystem cyber security, preferably under the umbrella of an existing sector wide community such as NWEA, TKI Offshore Wind or WindEurope. This dialogue should initially increase risk awareness and should evolve to knowledge sharing and innovation.

- An accurate functional information model of the ecosystem is crucial to ensure cyber security and yet no adequate model was found. The initial ecosystem model as introduced below was devised with limited time and has not been rigorously validated.

[CE2] Devise and validate a complete functional information model for the offshore wind ecosystem, possibly, but not necessarily building on the initial model in this research.

3.2 An initial model of the offshore wind ecosystem

The functional architecture shows the different functions in the offshore wind energy chain. The following architecture is determined using information that was acquired in the group sessions with market participants from the offshore wind energy chain. First, paragraph 3.2.1 describes the global functional architecture. In paragraph 3.2.2, the interactions between the parties are indicated using the available networks between the subchains. Paragraph 3.2.3 discusses the functions per subchain in detail and paragraph 3.2.4 shows a summary.

3.2.1 Overall functional architecture

Figure 3 shows the functional architecture of the offshore wind energy chain:

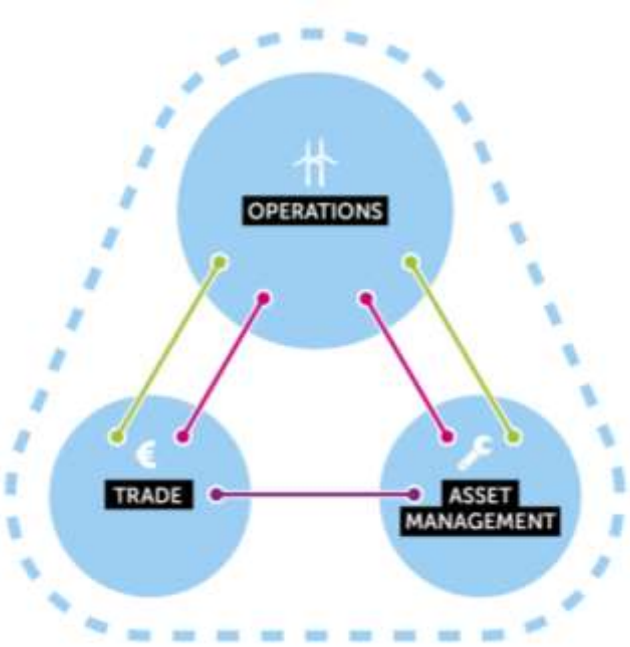


Figure 3 - functional architecture offshore wind energy ecosystem (colors signify different networks)

The offshore wind energy chain in Figure 3 consists of three function subchains, namely:

- ***Trade***
  Trade means trading energy. Based on supply and demand, the trading party (the trader) determines the day-ahead planning and processes the intra-day adjustments regarding the exact amount of energy that is to be/can be supplied. This is also called the power setpoint. This process is executed by human actions supported by technical analysis. Speed of control ranges between 15 minutes to days.

- ***Operations***
  Operations controls the autonomous arrangement in the wind farm. This concerns, for instance, the pitch and yaw control. The setpoints for these autonomous arrangements come from the trade (short term) and asset management (longer term) chains. For operations, it refers to the autonomous processes that require no human intervention. The speed of control ranges between sub seconds to minutes.

- ***Asset management***
  Asset management ensures the continuity and maintenance of all systems within the offshore wind farm. Control is mostly done by human actions. The speed of control ranges between minutes to weeks/months.

3.2.2 Networks

These subchains Trade, Operation and Asset Management interact with each other through various networks. Figure 4 shows the different networks drawn into the offshore wind energy chain.

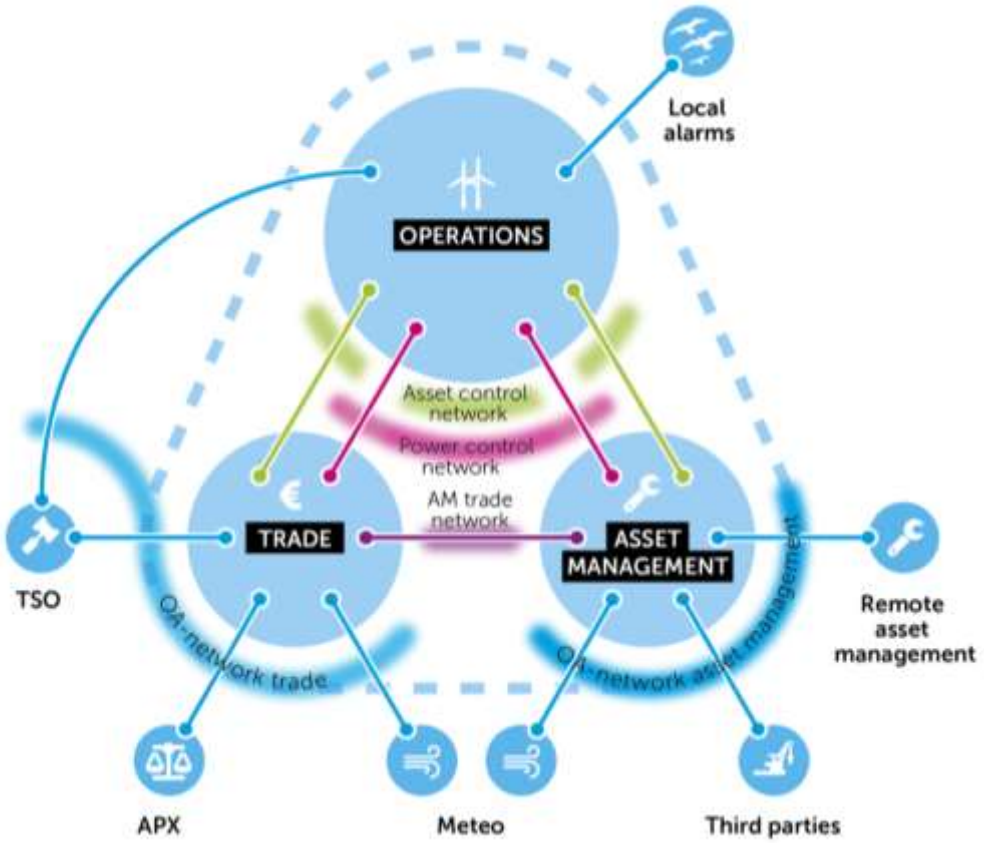


Figure 4 - connections and networks in the ecosystem

The offshore wind energy chain differentiates between four types of networks, namely:

- The office automation networks (OA-networks) of Trade and Asset Management retrieve the data from the supplier via a (standard) internet connection.
- The Asset Management-Trade network. This network is used for exchanging management data that is important to the trader, such as the availability of the turbines.
- The power control network. This network allows for the operation of the power switches and reading out the real-time production.
- The asset control network. This network is directed at operating the wind turbines and infrastructure.

Each of these networks has its own sensitivity to threats, depending on the information it communicates and the function of this information. This is elaborated in the following.

3.2.3 Subchains

This paragraph reveals the details of the data transfer and control that occurs for each subchain (Trade, Operation and Management).

3.2.3.1 Trade

Fout! Verwijzingsbron niet gevonden. shows in detail how information transfer and control is taking place in the subchain Trade.

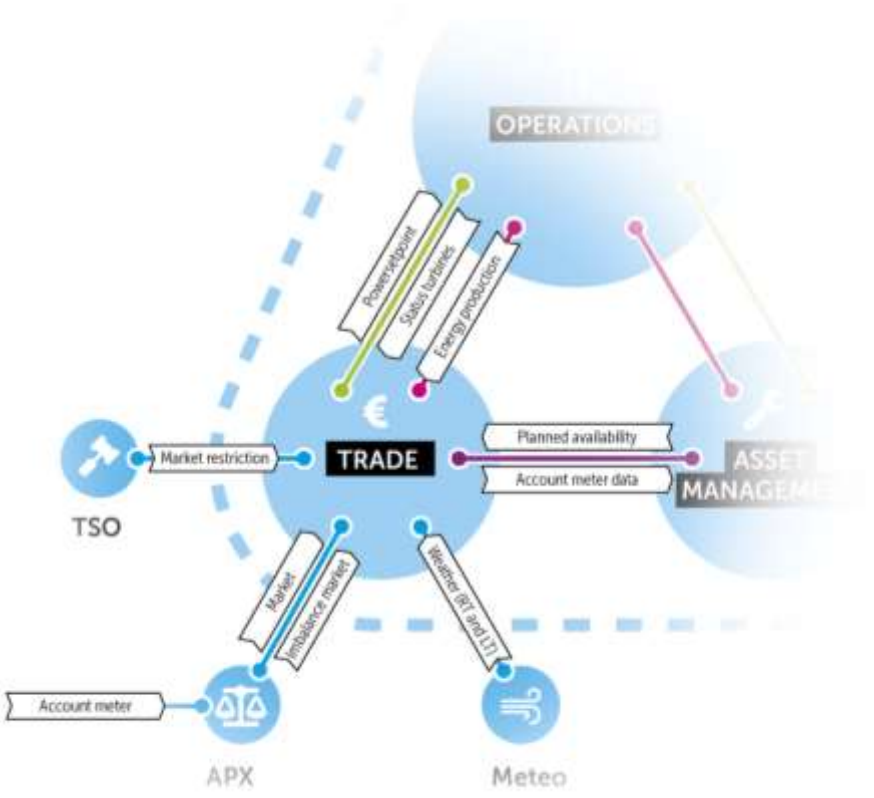


Figure 5 - zooming in on the Trade subchain

The energy that is supplied by the wind farm, will be traded on the energy market. In order to trade the energy, the trader must make a day-ahead planning. The day-ahead planning is a prognosis regarding the amount of supplied energy, based on the weather, available capacity of the offshore wind farm and possible market restrictions (imposed by the transmission system operator; TSO).

On the day, the trader will ensure that the differences between the predicted production (prognosis) and the actual energy production will be settled. The trader can do this by restricting the wind farm's production or by additional purchase or sale of energy. These are referred to as intra-day adjustments. In order to determine the intra-day adjustments, input regarding the real-time meteorological data, the current return of the wind farm and the status of the wind turbines are required.

The trader provides a setpoint to the wind farm for the (maximal) supplied capacity.

3.2.3.2 Operations

Figure 6 shows in detail how information transfer and control is taking place in the subchain Operation.

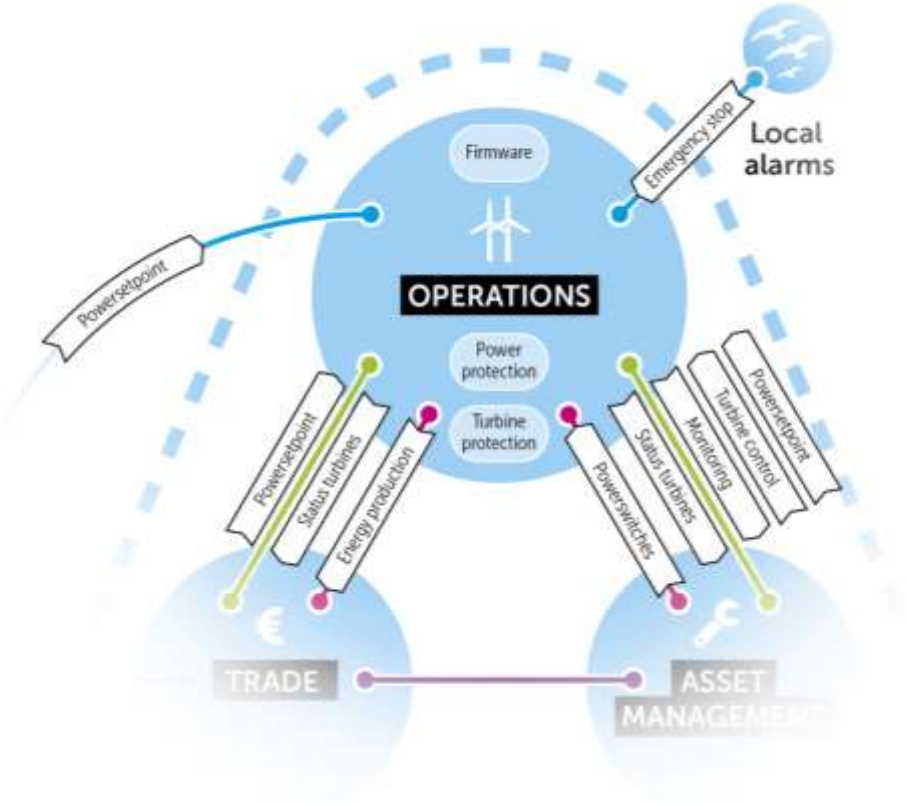


Figure 6 - zooming in on the Operations subchain

The wind turbines are constantly adjusted. The blades are, for example, turned into the wind (yawing). The pitch of the blades is adjusted to the wind speed and the position of the rotor, etc. This is done locally in the turbine in a completely autonomous process. Trade and Asset management can set the setpoints for the power control. Trade has the possibility to operate or shut down the turbines to react to market demands.

Local alarms are increasingly added to wind farms. An example is the detection of wildlife. The sensors detect whether any animals (birds, bats, etc.) are near the wind farm and whether the risk for the animals is too great. If so, the wind farm can autonomously decide to shut down the wind turbine at that particular moment.

3.2.3.3 Asset Management

Figure 7 shows in detail how information transfer and control is taking place in the subchain Asset Management.

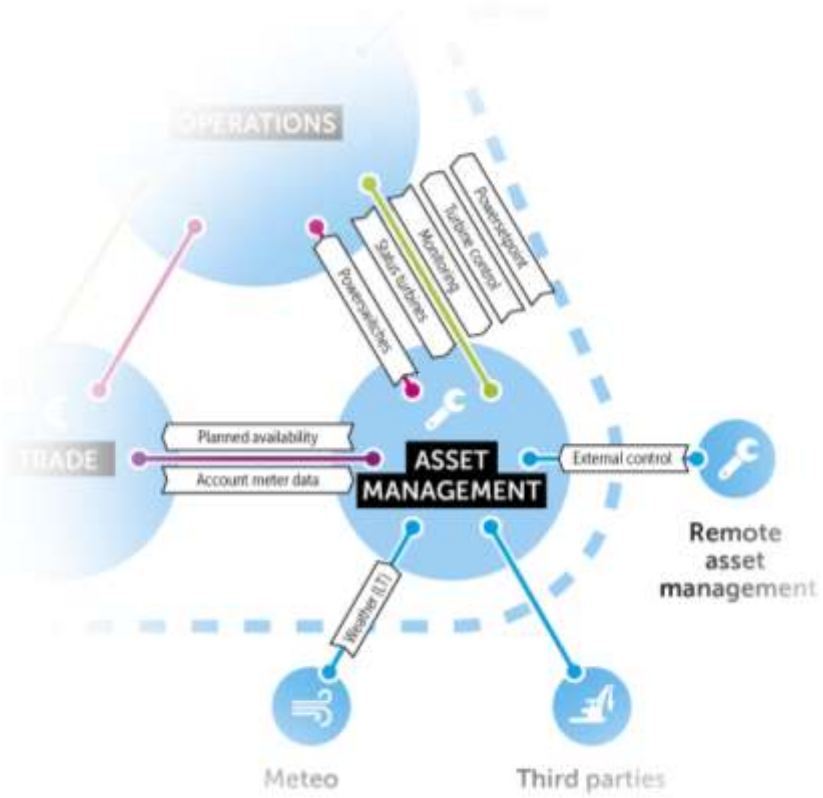


Figure 7 - zooming into the Asset management subchain

Management of the offshore wind farms can be divided into:

- management of the balance of plant; and
- management of the turbines.

Management of the balance of plant is focused on managing and maintaining the infrastructure: the energy transport network with the primary parts such as transformers, power switches and networks.

Management and maintenance of the wind turbines is often performed by specialized parties, such as the supplier of the wind turbine. There is a limited number of suppliers for offshore wind turbines. Management of offshore wind turbines is thus often clustered. The companies manage turbines in various (offshore) wind farms. Management is mostly done remotely from the manager's main location.

There generally is an onsite internet connection on an offshore wind farm for the engineers that maintain it. This connection is used for maintenance activities, but also for private purposes when engineers need to spend the night.

3.2.4 Summary

The following figure (Figure 8) shows the complete overview of the three functional chains. Together, they are the functional architecture of the offshore wind energy chain.

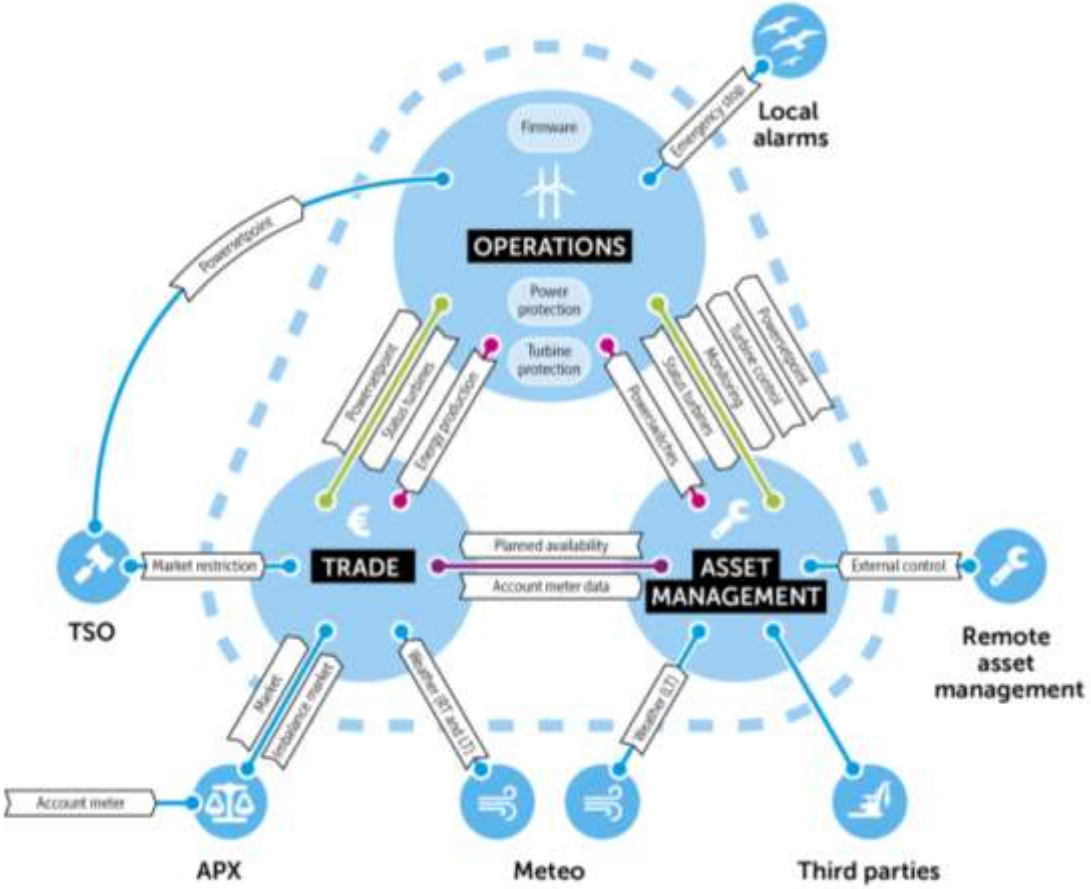


Figure 8 - overview of the functional architecture and interactions

4 Future Ecosystem Cybersecurity

4.1 Findings and recommendations

The following findings and recommendations have been found in an analysis that is summarized in sections 4.2 and 4.3.

4.1.1 Findings

- Chapter Cyber security from Ecosystem perspective 3 described the research finding that there is limited ownership and awareness of risks encompassing the entire ecosystem. Further it introduced an initial functional model of the ecosystem as this was not found in literature.
- After determining and validating this model in the research with the market participants, the group sessions identified possible security issues (risks) from the perspective of the complete ecosystem. The foremost risks are described in paragraph 4.2, starting with the risks prioritized as 'top 3'.
- The risks were prioritized by multiplying expected chance of occurrence times the expected impact of the risk for the ecosystem. Especially with the current level of ecosystem insight, this was found important, yet quite subjective. It is recommended (below) to develop more quantifiable and objective measures.
- To deliver more focused recommendations for research, several proposed mitigations were determined at least for the top 3 risks. These are described in paragraph 4.3.

4.1.2 Recommendations

- The research group with market participants found it inspiring and constructive to identify and assess ecosystem risks in a joint setting. This should not be just a one-time activity, but should be included in a recurring, shared process.

[FE1] It is recommended to use the initial ecosystem model and the initially identified risks as a (recurring) basis for risk assessment discussions in the sector, preferably in a community dialogue as meant in recommendation [CE1].

- Objectively determining the expected chance and impact of risks was found hard. Understandably so, as it requires extrapolating future scenarios in a broad ecosystem.
- To guide research and consequently regulation, it is necessary that the risk classification becomes more quantifiable and objective. Dynamic simulation of 'digital twins' is growing to be suitable for such challenges.

[FE2] It is recommended to quantify the resilience of the large-scale ecosystem to identified risks using rigorous and integral simulation of the ecosystem's resilience e.g. at testbeds such as those present at TU Delft.

- A major risk for the larger energy ecosystem may be the integrity of meteo data. If this data is compromised across the entire ecosystem, the Dutch energy system may not be able to prepare for unexpected highs and especially lows in wind production.
- Assessing the gravity of this risk is a good example of the subjective nature of risk assessment. As it could have a very large impact it is recommended to quantify this risk first and then to find possible mitigations.

[FE3] It is recommended to research the independency of meteo data, the sensitivity and resilience of the ecosystem to incorrect meteo data and to research processes to continuously assess plausibility of the data from multiple independent sources.

- From a wind farm operator perspective, it may be attractive to maximize the size of operational clusters, for maximal cost efficiency and operational synergies. From an ecosystem perspective a large cluster size is not desirable, as it maximizes fallout risks in case of cybersecurity mishaps.

[FE4] It is recommended to research the trade-offs of large cluster sizes (with higher operational management efficiencies) to a significantly lower system risks of smaller cluster sizes, with the goal of proposing a sector wide regulation for cluster size.

- Wind farm operation is a complex business requiring many disciplines for optimal effectiveness and continuity. It is therefore expected for the foreseen future that operation of any wind farm will require the services of multiple specialized parties.
- Cybersecurity risks increase fast with the amount of parties having physical and digital access to operational assets.
- As it is unlikely (see previous bullet) that the number of parties will decrease, it is required to increase the scrutiny on the actual access rights and processes. This starts with a clear responsibility structure, e.g. with the turbine owner in control of the network distributing access and authorizations as needed only. Technological solutions are becoming available also in OT to dynamically set access rights and even data flow directions per information stream.

[FE5] It is recommended to research processes and solutions to ensure that asset management parties by default have ‘read-only’ access to asset data and any interventions with possible physical consequences requiring explicit authorization from the wind farm manager.

4.2 Main future ecosystem risks

The research brainstorms were organized with market participants to identify ecosystem risks and subsequently to substantiate and prioritize these risks, by multiplying impact (possible consequences from an energy ecosystem point of view) with probability (the chances of this risk occurring specifically for offshore wind). Although prioritizing was of subjective nature, for purposes of focus three foremost risks were selected.

They are displayed in Figure 9 and described in paragraphs 4.2.1 through 4.2.3. Other risks that were identified are enumerated in paragraph 4.2.4. Section 4.3 describes proposed mitigations to the risks identified.

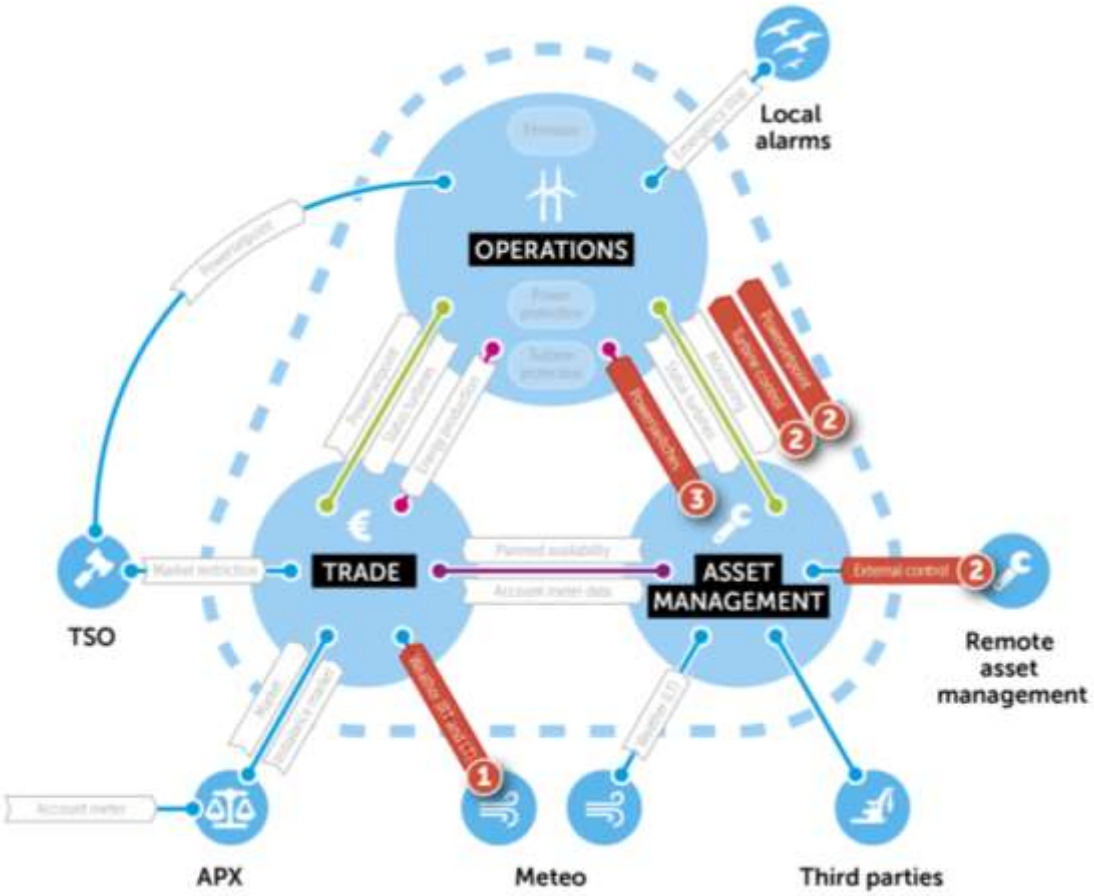


Figure 9 - top 3 ecosystem risks

4.2.1 Risk 1: integrity of wind prediction data

The subchains Asset Management and Trade depend on the weather and thus use meteorological data. Meteorological data is collected by only a few external sources. Due to incorrect, manipulated or missing wind predictions, there is a chance that the expected production of wind farms is estimated incorrectly. This can cause an imbalance on the energy grid.

Figure 10 - dependency on Meteo Data

A relatively small imbalance can be counteracted by the imbalance market, but large differences can lead to problems on the energy distribution network resulting possibly in a blackout.

When multiple large wind farms consult the same source of wind prediction, an intentional manipulation of this source through a cyberattack can cause a blackout of the energy distribution network.

4.2.2 Risk 2: concentration of asset management of wind turbines

The management of wind turbines and wind farms is done remotely. Different market developments possibly result in the fact that within the offshore wind energy chain the management of the wind turbines will be clustered amongst only a few management parties.

The reasons for clustering are:

- the scale size of management increases the efficiency in management and lowers the maintenance costs;
- there is a limited number of suppliers for offshore wind turbines;
- long-term maintenance contracts provided by suppliers;
- limited joining possible of independent management/maintenance parties due to high risks and necessary investment.

Figure 11 - concentration of asset management roles

Because the management interfaces of a large number of wind turbines and wind farms will be accessible to one management party, and probably thus from one location, this is a very convenient point to create a disturbance (e.g. a large-scale shutdown of wind turbines).

4.2.3 Risk 3: concentration of control of power switches

Each wind turbine has a power switch which can be used to shut down the turbine. In addition, a wind farm also has power switches that can be used to shut down multiple turbines at once. In order to operate these power switches effectively, it is done remotely as much as possible. The operation of the power switches is generally under the control of the manager of the farm.

Operating the power switches largely falls into the same category when it comes to risks concerning management and monitoring of the turbines. The remote operation of the power switches is expected to be clustered under a small number of management parties.

Because the interfaces for remote operation of many power switches will be accessible for one management party, and probably thus from one location, this is a very convenient spot to create a disturbance (e.g. a large-scale shutdown of wind turbines).

As manager of the energy grid, TSO has been given the possibility to influence the operation of the power setpoint via a (series of) connection(s). This, however, will only occur in extreme cases when a severe imbalance of the energy network seems inevitable.

The TSO has this possibility for all energy-producing installations that are connected to the energy grid, which includes, for example, coal-fired and gas-fired power stations. Considering the fact that this risk is applicable to the entire electricity system, this report does not go into this aspect as a possible risk for the offshore wind energy chain.

4.2.4 Other potential ecosystem risks

All risks that were identified in the workshops were subsequently classified, by multiplying impact (possible consequences from an energy ecosystem point of view) with probability (the chances of this risk occurring specifically for offshore wind). The highest three classifications were described before, but the following risks were also identified as realistic and definitely warrant further attention. The mitigations in 4.3 are also broadly appropriate to these risks.

- The TSO has very direct operational impact on individual wind farm operation and on offshore wind as a whole (every wind farm being connected to the TSO's HV-grid). Any **cybersecurity breach at the TSO** will therefore have major possible consequences (very high impact).
- Operational wind farms are increasingly equipped with local alarms (e.g. bird radars) that may impose a direct impact on operations (emergency stop). **Local alarms being negatively controlled** may thus pose significant operational risks, which are quite probable to occur at a local scale. However, due to their local nature, it is harder to see such risks spreading to ecosystems scale.
- As anywhere, the human factor is always significant in cybersecurity. Throughout the ecosystem the **compromise of privileged accounts**, e.g. using social engineering or by disgruntled employees, is a major risk. Each party in the ecosystem must remain vigilant to such risks and also remain prepared for this risk occurring at partners.
- Besides the obvious omnipresence of state-of-art mechanical and electrotechnical technology in offshore wind, it is hard to find any asset that is not digitized to a significant amount. The assurance of **quality and integrity of the firmware** in all assets at all partners should thus be of primary concern. Suppliers of mechanical and electrotechnical technology and services often need to catch up on a historic lag.

4.3 Main future ecosystem mitigations

This chapter describes the possible measures that can be taken in order to protect the offshore wind energy chain from the risks mentioned in chapter 4.2. It is possible that some of these measures have already been taken in certain wind farms.

4.3.1 Use of multiple independent sources of wind prediction

The subchain Management and Trade use an external source for meteorological data. Intentional manipulation of this external source can have serious consequences for any (im)balance of the energy distribution network.

By using multiple sources of wind prediction, incorrect predictions of one source can be detected. The independence of these sources needs to be guaranteed.

4.3.2 Authorization of management of wind turbine by farm manager

The management of wind turbines is done remotely. Because the management interfaces of a large number of wind turbines will be accessible to one management party and from one location, this increases the risk of a possible disturbance on a larger scale (e.g. a large-scale shutdown of wind turbines).

The possibilities of such a management party can be restricted when it can only manage a wind turbine with a temporary authorization granted by the farm manager. This temporary authorization does not only require procedural enforcements, but also technical.

Due to this measure, the risk of a remote large-scale shutdown of wind turbines is considerably reduced.

4.3.3 Preventing clustered farm management

Clustering of farm management due to a limited number of organizations increases the risk of a disturbance occurring in a large part of the installed capacity from offshore wind energy that comes from one location.

The risk can be prevented by establishing guidelines regarding the maximal size of clustering. These guidelines can be included in the tenders and licensing procedures of offshore wind farms to be developed in the future.

4.3.4 Network segmentation

Offshore wind energy uses several networks. These serve different purposes and the data and control through these networks thus carries different risks. It is therefore recommended that these networks are separated. This ensures that authorizations are mandatory and that problems or attacks in one network are limited to only that one network. Where a connection between the networks is inevitable, a firewall needs to be put in place to check traffic.

5 Summary of recommendations

The energy network is a dynamic system which allows network managers to adjust on a short-term basis at the moment of imbalance. However, the possibilities to adjust are limited. The larger the installed capacity of an energy source, the larger the possible impact on the energy network during an intentional manipulation.

With the rapidly increasing dependency of the Dutch energy sector on offshore wind power, it is of growing concern to look at cyber security not only from the view of a single wind farm operator, but also from a total ecosystem perspective.

In this report recommendations were given both for shorter (current) and longer (5 year+) time horizons and both for single farm and entire ecosystem perspectives, although the focus of this research is on longer time scale for the entire ecosystem (in line with the goal to provide the sector with research programming guidance).

The recommendations from this report are repeated below, with a short reference, as shown in **Fout! Verwijzingsbron niet gevonden.**.

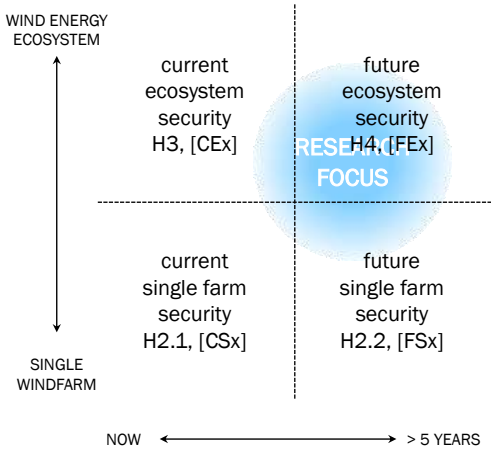


Figure 12 - grouping of recommendations

5.1 Recommendations for Current Single farm cybersecurity [CSx]

[CS1] It is recommended to set up a trusted community of operators to jointly optimize efforts of each single player. Such a community can start small, by just opening communication channels on active threats and sharing information on solutions.

[CS2] It is recommended to bundle shared knowledge into a set of best practices and solutions, to use for each individual operator's cybersecurity efforts. The trusted community could play a major role in this, possibly supported by a research institute or by adjacent platforms such as ENCS.

5.2 Recommendations for Future Single farm cybersecurity [FSx]

[FS1] Research the optimal cybersecurity framework to maintain throughout the offshore wind sector, including underlying standards and their certification, regulatory structure and governance, implementation roadmap and industry commitment.

[FS2] Research how a specific offshore wind power cybersecurity standard can be formed and sustained, possibly starting on the basis of ISO61400-25.

5.3 Recommendations for Current Ecosystem cybersecurity [CEx]

[CE1] Set up a community dialogue on ecosystem cyber security, preferably under the umbrella of an existing sector wide community such as NWEA, TKI Offshore Windor WindEurope. This dialogue should initially increase risk awareness and should evolve to knowledge sharing and innovation.

[CE2] Devise and validate a complete functional information model for the offshore wind ecosystem, possibly, but not necessarily building on the initial model in this research.

5.4 Recommendations for Future Ecosystem cybersecurity [FEx]

[FE1] It is recommended to use the initial ecosystem model and the initially identified risks as a (recurring) basis for risk assessment discussions in the sector, preferably in a community dialogue as meant in recommendation [CE1].

[FE2] It is recommended to quantify the resilience of the large-scale ecosystem to identified risks using rigourous and integral simulation of the ecosystem's resilience e.g. at testbeds such as those present at TU Delft.

[FE3] It is recommended to research the independency of meteo data, the sensitivity and resilience of the ecosystem to incorrect meteo data and to research processes to continuously assess plausibility of the data from multiple independent sources.

[FE4] It is recommended to research the trade-offs of large cluster sizes (with higher operational management efficiencies) to a significantly lower system risks of smaller cluster sizes, with the goal of proposing a sector wide regulation for cluster size.

[FE5] It is recommended to research processes and solutions to ensure that asset management parties by default have 'read-only' access to asset data and any interventions with possible physical consequences requiring explicit authorization from the wind farm manager.

6 References

[BIO] Baseline Informatiebeveiliging Overheid versie 1.0.3, maart 2019.

[ISO27001] ISO/IEC27001, de ISO standaard voor informatiebeveiliging

[NEN61400-25-1] NEN-EN-IEC 61400-25-1, Wind energy generation systems – part 25-1. NEN.

[TOR] Terms of Reference Cybersecurity Offshore Windenergie, dossiernummer TSE3180004, 1 oktober 2018.

[HANDR-UE] Handreiking cyber security voor smart energy, TKI Urban Energy, juli 2017.

[ONTW-KLIM] Ontwerp van het Klimaatakkoord, Klimaatberaad, 21 december 2018.

[NOZ-HKZ] Net op Zee Hollandse Kust (Zuid), Toelichting aanvraag omgevingsvergunning bouwen voor platform Beta, TenneT TSO B.V., 28 februari 2017.

[REG-HKZ] Regeling vergunningverlening windenergie op zee kavels III en IV Hollandse Kust (zuid), Regeling van de Minister van Economische Zaken en Klimaat van 23 november 2018, nr. WJZ/18199760

[NOZ-KC-2016] Kwaliteits- en Capaciteitsdocument Net op Zee 2016, TenneT TSO B.V.

[NOZ-KC-2017-III] Kwaliteits- en Capaciteitsdocument 2017 Deel III: investeringen, TenneT TSO B.V.

[BWFI-PSD] Borssele Wind Farm Zone Sites I and II, Project and Site Description. Netherlands Enterprise Agency, April 2016.

[BWFIII-PSD] Borssele Wind Farm Zone Sites III and IV, Project and Site Description, Netherlands Enterprise Agency, August 2016.

[HKN-PSD] Hollandse Kust (Noord) Wind Farm Zone, Project and Site Description. April 2019.

[IJM-VAL] Final Report: Validation of Studies regarding the Grid Connection of Windfarm Zone Ijmuiden Ver, BLIX Consultancy BV. November 2018.

[DNV-WFCS] Our holistic view on Cyber Security for wind farm critical infrastructures, DNV-GL. October 2016.

[UL-WFCS] Cybersecurity for wind farms, UL, 2018.

[BH-AWF] Adventures in Attacking Wind Farm Control Networks, Black Hat USA 2017.

[ENCS-PSG] Security requirements for procuring substation gateways, ENCS, 2019

7 Glossary

APX	**A**msterdam **P**ower E**x**change, exchange for electricity
DS	**D**istribution **S**ystem **O**perator
IT/OT	**I**nformation **T**echnology/**O**perational **T**echnology
LT	**L**ong **t**erm
OA-network	**O**ffice **A**utomation network
RT	**R**eal **t**ime
TSO	**T**ransmission **S**ystem **O**perator

TKI WIND OP ZEE
Topsector Energie

Postadres
Postbus 24100
3502 MC Utrecht

Bezoekadres
Arthur van Schendelstraat 550
Utrecht

T +31 30 73 70 541
E secretariaat@tki-windopzee.nl
T www.tki-windopzee.nl