Organisational Contexts of Energy Cybersecurity

Tania Wallis(✉), Greig Paul, and James Irvine

University of Strathclyde, Glasgow, UK
Tania.wallis@strath.ac.uk

Abstract. The energy system is going through huge transformation to integrate distributed renewable generation and to achieve the goals of net-zero carbon emissions. This involves a significant adjustment to how the system is controlled and managed, with increasing digitalisation of technology and growing complexities across interconnected systems. Traditionally electricity networks adjusted their supply of energy in response to changes in demand. The future energy system will require more flexible demand to be able to use or store energy when renewables are generating. This change is exacerbated by additional demand for electricity for heat and transport uses.

Utility organisations hold responsibility for securing their networks and assuring the supply of electricity. This paper describes a full investigation of cybersecurity issues and concerns for utilities. This industry review was carried out to create a clear organisational context for the ongoing design of cybersecurity improvements. The assessment of potential impact and consequences of cyber-attack is recommended to direct necessary preparations towards protecting essential functions and processes. Improving resilience across interdependent actors is discussed and resilience measures suggested to guide the contributions of different actors towards whole system resilience.

Keyword: Cybersecurity · Critical infrastructure · Organisational resilience

1 Introduction

Energy distribution networks are undergoing significant change. Traditionally based on a relatively smaller number of central generation sites with simple control and stability through overprovisioning, generation is becoming increasingly distributed with the introduction of renewables such as solar and wind. The network is becoming a 'smart grid' with enhanced control and demand management to improve efficiencies and reduce overprovisioning, and the net zero agenda is increasing demand on the electricity network through the electrification of heat and transport. This has significant cyber security implications. Electrical distribution networks will have to interact more with sources of supply and demand, and more sophisticated control is more vulnerable to attack.

The University of Strathclyde's Power Network Demonstration Centre (PNDC) brings together academics, industry organisations and technologists for pre-commercial

S. Katsikas et al. (Eds.): ESORICS 2021 Workshops, LNCS 13106, pp. 384–402, 2022.
https://doi.org/10.1007/978-3-030-95484-0_22

research and development projects to shape future smart energy networks. The PNDC investigated the organisational aspects of cybersecurity to provide an improved understanding of the future energy system among PNDC members and beyond. This enabled an organisational and sectoral context to be brought to the technical solutions. Furthermore, this research facilitated the coming together of different experiences and understandings across the PNDC membership, such as IT skills adapting to an Operational Technology (OT) context and a synthesis of power systems and telecoms experience. Section 3 describes an assessment of current cyber security concerns within utility networks. Section 4 then proposes how the impact of different issues can be assessed, and Sect. 5 emphasises key aspects to improving the resilience of power networks.

1.1 Approach

This research involved bringing together different experiences to make clear the context of a changing energy sector. The changing role of Distribution Network Operators (DNO) was also considered as they would be evolving to include system operator responsibilities to balance power flows for their grid zones.

The research builds upon Hurst's work that recommended a holistic defence in depth approach after surveying different infrastructure security strategies. Proactive protection needs a broad view of the infrastructure, coordinated responses to disruptions and requires diverse information about systems, networks, devices and processes to model correct behaviour [1].

Key concerns and issues on achieving cybersecurity for future energy scenarios were evaluated through a workshop and interviews with PNDC industry partners. This included 20 people with cybersecurity responsibilities, in UK based operations, from the spread of organisations listed below.

- 5 energy companies
- 3 telecom service providers
- 2 suppliers of automation and smart grid equipment
- 2 consultants in security and risk.

A grounded theory approach was followed, combining insights from literature, relevant project experience and analysis of the discussions [2]. The workshop brought together IT security skills, OT engineers and telecoms experts to form the organisational context of a future Distribution System Operator (DSO). This enabled a backdrop of shared understanding for the ongoing development of cybersecurity implementations in the sector to be formed. Several round-table discussions, with different skillsets in each invited an open exploration of the issues. Bringing together stakeholders in this way to address sector specific issues with mutual cooperation and by going beyond organisational boundaries aligns with Burns' partnership approach [3]. The arising issues were then discussed as a whole workshop group and categorised into emerging themes that are outlined in Sect. 3. Interactions during the workshop and the experience of participants enabled the building of the analysis and the discovery of the categories [4].

The workshop output formed the basis of some follow-up interviews with each of the participating organisations. Interviews allowed time to further explore with in-depth

discussion, using open questioning based on the themes and categories that arose during the workshop [4]. These interviews were conducted in a semi-structured manner to allow further sharing beyond what could be communicated in the group workshop setting. The use of anonymity during the interview stage, where stakeholders were less willing to share sensitive information in a group, provided a platform for gathering and analysing information anonymously and then acting on it collectively [3]. A multi-actor approach by listening and understanding different perspectives across industry was paramount to this research [5]. The compilation of workshop and interview findings later allowed PNDC members to select priority issues to set the focus for future cybersecurity projects at PNDC.

The emphasis of this exercise on the needs of DNO organisations was important due to their holding responsibility for the cybersecurity of their operations and services. While the focus needed to be on PNDC members due to this work leading into future work based at PNDC, it holds relevance to the energy sector in general and beyond the UK and to the necessity of ensuring an understanding of organisational context for more effective cybersecurity implementations.

2 Preparing for Future Energy Scenarios

With uncertainties about the impact of cyber security on organisations within the energy sector, exploring potential scenarios can help direct more effective preparations. Each scenario gives us a future vantage point from which to observe the present situation. The capacity to manage future uncertainties requires both learning from past attacks as well as consideration of different futures [6].

Table 1 shows different areas of activity that can be distinguished, from solving one-off problems to looking at longer term capability, using an exploratory mindset or achieving closure with decisions and actions. All four activities play a role in effective preparations.

"Systems cannot be constructed to eliminate security risk" [7] so it is essential that systems are designed to recognise, resist and recover from attacks. Longer term considerations and the ability to adapt to new threats are important for systems to sustain assurance over time. A continued adaptation is necessary to respond both to changes in threats and changes in functions or usage of the system that could enable an attack.

Table 1. Dimensions of purposeful activity [8]

	Single activity problem solving	Ongoing activity surviving/thriving
Opening up exploration	What's going on? Making sense of the latest threat landscape	What's coming? Anticipation preparedness
Closure decisions	Developing a strategy to deal with cybersecurity	Organisational learning adapting to changes and new threats dynamic response

This research focussed more on the opening up and exploratory dimension of Table 1 to provide an improved awareness and understanding of the situation and context of future energy networks and enable decisions to be made on the priorities and focus areas for future projects at PNDC.

2.1 Setting the Context

National Grid operates the transmission network in much of the UK. Its future energy scenarios (FES), shown in Fig. 1, offer a context to explore potential cyber security scenarios and impacts. Four different pathways are described towards net-zero carbon emissions, including consumer or system transformation as different ways to reach 2050 goals [9]. The FES will require an integrated whole system approach to manage a more complex picture of power flows and to coordinate demand with supply.

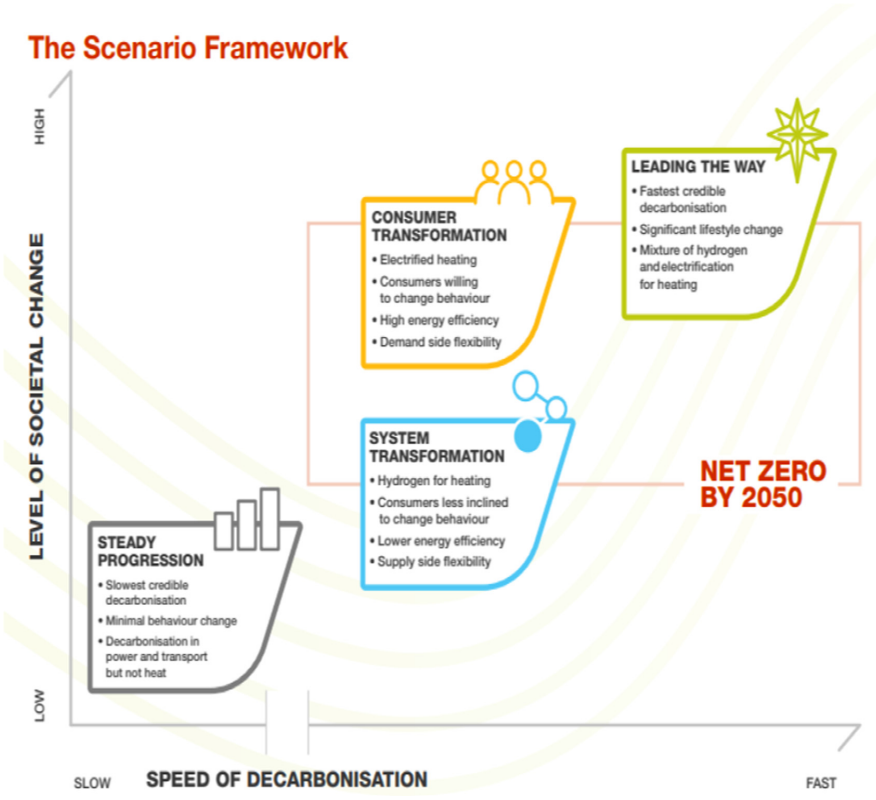

Fig. 1. National grid future energy scenarios [9]

During our Industry Review detailed in Sect. 3, the importance of organisational context was apparent, and it was clear that cybersecurity approaches and mitigations essentially must consider the operational and cultural context they need to function

within. The real potential of a vulnerability is also highly contextual. “The real impact of a vulnerability is heavily dependent on the context surrounding the targeted device” [10]. Considering risks from an operational perspective as well as a security perspective ensures that cybersecurity risks are managed from an organisational understanding [11]. The wider engineering solution around it could be more important than the security solutions especially where there are security gaps. A vulnerable asset can be assessed based on its importance to the organisation using ‘Environmental Metrics’ to customise a vulnerability score by assigning a high medium or low value in terms of Availability Integrity Confidentiality [12].

A significant power outage in the UK in August 2019 emphasised the importance of adaptability and cooperation in operating a changing and complex power system [13]. Stronger and faster interactions are expected between different aspects of the energy sector, to obtain value from coordinating and optimising the whole system. The wide adoption of data-driven insights to manage a distributed energy system must be balanced with the necessary attention to cybersecurity and privacy. From a policy perspective, attention is being paid to securing consumer smart devices in the FES, both in terms of the devices themselves, and their interactions and data flows required. In addition to privacy concerns, where different actors and devices have control and can trigger changes to the system, a coordinated and secured approach within safe parameters must prevent unwanted consequences.

Electricity markets driving consumer demand with price incentives will necessitate digital solutions to prevent sudden swings in demand. For example, Electric Vehicle (EV) charging patterns will need to be managed to spread the load away from peak demand and towards periods of higher renewable generation.

The Energy Networks Association (ENA) provides guidelines for Distributed Energy Resources (DER) to facilitate meeting cybersecurity requirements with small generators. They require consultation and collaboration between the DER operator, the DNO and any third-party providers involved [14]. Similar agreements attending to cybersecurity will need to be developed for the coordination and connection of increasing amounts of offshore wind generation.

While these future scenarios point to an increasing need for digital solutions, a consequence driven approach to cybersecurity is emerging through cyber informed engineering that recommends keeping reliance on digital technology to a minimum for critical functions and processes [15]. It will be important to prioritise essential functions by protecting the hardware, software, processes and procedures that enable them, in order to prevent unwanted consequences [16]. Analysis of these new scenarios with new dependencies will identify potential impacts to avoid, where it is most necessary to reduce pathways for malicious control of essential assets and functions. Particular attention will need to be given to reliance on offshore wind, aggregation of flexibility services, energy storage and the capability to spread new load patterns towards renewable generation patterns. Network reinforcements will be required for distribution networks to cope with increasing power flows, especially to meet electrification of heat and transport, and to avoid the constraint of renewable generation. The cost of this “can be minimised by deploying smart and innovative non-build solutions” and through better integrated planning [9]. Traditionally the energy system had supply responding to changes in demand,

the new scenarios put supply in charge and expect smart flexible demand to either use or store electricity when it is available. To prevent opening additional pathways to attack, cybersecurity must be embedded into these smart solutions.

All these FES will need the support of a highly interconnected control structure, and will also increasingly interact with natural gas, hydrogen and biofuels. Aggregated technologies on the demand side, responding to half hourly price signals, will require managing at street, local and regional level so that distribution networks protect system stability. A whole street of EVs responding to price signals, all drawing or all feeding back power to the system, could otherwise cause instability. Achieving Net Zero expects a "deep digitalisation of all energy assets" [17]. This will require secure solutions at all levels. "As new sources of flexibility come online, we will need their operational data" [17]. Information becoming available in more places could also be assisting adversaries to build a clearer view of the system. The transformed energy system will require "interaction between digital platforms, technologies and markets signals" and "interoperability across data, services and technologies" [17]. An increasingly interactive and interoperable energy system must be developed with cybersecurity in mind.

With this opening up of access to data and lots of pathways into networks, it is likely to become too much to monitor for anomalies without some simplification to effectively oversee the cybersecurity of such solutions. The integrity of data is essential where it is being used to control devices and system responses. An honest look at our reliance on complex digital solutions, and the recognition that we will have "combined technologies, delivering multiple services", "smart technologies, all digitally enabled" and "deployed at scale and throughout the energy system" [17] makes it clear that cybersecurity must be fully embedded into the journey to net zero. Where dependencies are greatest and to protect essential functionality, priority decisions will need to be made. An engineering perspective must find ways of defending an extensive attack surface such as keeping system capabilities within safe limits, while retaining the system orchestration that digitalisation brings.

3 Industry Review

A review was undertaken by PNDC of the main points of concern in cyber security in utility networks. The approach used is detailed in Sect. 1.1. The review started with a cybersecurity workshop attended by various energy sector actors, including DNOs, vendors and consultants. Follow-up meetings and discussions were then held with participants to build a full picture of the situation. This provided a thorough organisational context for ongoing design of cybersecurity improvements and to prioritise innovation projects at PNDC. The following sub-sections describe the emerging cyber security issues and requirements for these energy sector organisations.

3.1 Accessing Multiple Sites

There is a requirement for security of both local access to equipment within a substation's own network and remote access to substations over wide area networks. The need for remote access support for substations is required from third parties, vendors and external

contractors. Corporate network access into substations was also essential, requiring an economical solution which meets the needs of different branches of the business, yet preserves security of the operational network.

There was a strong requirement for Identity and Access Management (IAM) capability, with a need for logging of actions, as well as control of who is able to access systems, and a facility for revocation of access, while considering the unique nature of an operational network and ensuring availability of systems. To avoid the introduction of complex security systems which slow down operations, operational networks often do not feature the same security features as corporate networks, such as 2-factor authentication. Introducing stronger verification of the identity of a party connecting to equipment, as well as the actions they are permitted to carry out, must consider the operational context of an always-on environment.

In a control room setting, it is difficult to switch the identity of the operator without shutting down and restarting the interface which is not appropriate for a real time environment. There are layers needed to the solution, and there is a different class of problem for unattended equipment.

For remote access there were issues with creating VPN tunnels into substations such that alternatives to VPN may need to be considered. A specific concern was how to manage cryptographic keys and VPN configurations, and in making coordination and management scale to the high number of substations sites.

There were different views on the extent of encryption and whether it is necessary for all communications to be encrypted or would authentication alone offer sufficient security for certain services. Grid protection applications, in particular, could require very fast, potentially sub-millisecond encryption to meet latency requirements.

There was a desire to look into "encrypted by default" communications within operational networks, provided suitable provisions are made for availability, reliability and performance. However, there was a concern with regard to the security and management of certificates and cryptographic keys, and ensuring the correct handling of issuance and revocation, to avoid any downtime or loss of functionality.

Specific technologies for linking sites were discussed, such as whether there were any security benefits to using MPLS over more traditional technologies. There was considerable concern about the widening cybersecurity issues caused by moving towards IP-based networks and IEC 61850 substations.

There are some unique challenges within operational networks which can make deployment of standard solutions more complex, such as most single-sign-on systems failing if the centralised authentication server fails or goes offline. It would be possible to build a more resilient solution using Public Key Infrastructure (PKI) technology, to securely authenticate parties through certificates issued on a regular basis, with no direct requirement for the authentication servers to remain online to permit remote access to systems during outages or other emergency scenarios. For log aggregation, the main priority would be ensuring provenance of the logs against tampering, while keeping bandwidth usage to a minimum for remote sites which have limited network link capacity available for log aggregation. PKI was seen as a potential approach to securing networks, although the risks of quantum computing advances were highlighted as DNOs – and regulators – traditionally expect relatively long-term deployments of equipment.

3.2 Securing Legacy Equipment and Future Networks

There is a significant challenge in managing legacy equipment as the network moves to a more integrated environment with inter-connected systems, especially as legacy equipment was often not designed with security in mind. Legacy devices frequently lack access control and other security measures, and assume the network is only available to fully trusted devices. It is not possible to change, modify or update legacy equipment to be compliant with newer security systems, and many older security protocols feature weaknesses which cannot be resolved other than by updating to a newer version of the protocol such as Transport Layer Security (TLS) protocol.

If legacy equipment has no access control, any party with access to the network to which that device is connected may interact with the equipment, and potentially carry out operations. To maintain the security of such devices, it is necessary to firstly identify these devices, and secondly ensure that they are isolated from other network traffic with network segmentation, and from remote users with VPN access, limiting access to nodes that specifically require it. Legacy equipment almost invariably has no logging or auditing capabilities, meaning that attempts to gain access to the equipment may not be detected. Building adequate secure capability around legacy systems is essential. Security monitoring is vital to stop attacks more quickly, identify suspicious access or traffic, and monitor configuration and authentication events.

Lifetime management of equipment is an issue, including ensuring suitable vendor support, particularly for embedded systems where security updates are not necessarily forthcoming a small number of years after release.

The practical security considerations of firmware updates on equipment in the field were also raised. There is a perceived risk of updating working equipment, due to the loss of availability while updating or other failure due to the update. However, software vulnerabilities present a serious risk to the security of the network, and insecure devices could be used as "pivot" points to explore other parts of the network, potentially exposing more critical systems to attackers. The risks of allowing non-updated devices to remain on the network needs to be evaluated, perhaps using penetration testing outcomes, versus the risks of carrying out an update (ideally remotely), and the impact on security and availability this may have. Another risk introduced through remote updates is the potential for an attacker to use this method to deploy a malicious update, indicating a requirement for remotely updateable devices to have suitable security in place to authenticate any updates issued.

With a large number of embedded systems deployed in the network, an interest was expressed in whitelisting technology, which could be used to constrain embedded devices to mitigate against malicious software or other attacks, by ensuring that only the specific software originally installed on the device would be able to execute.

To improve the integrity of the OT environment, there could be potential for the use of VPN tagging to monitor data flows and record log in access and operations on legacy equipment which may not currently have support for this.

3.3 Network Monitoring

The introduction of malicious equipment to a secure network is a security concern. Having the capability to monitor networks for the introduction of new devices, or changes

to existing devices, would reduce cost and provide a more rapid response. Additionally, identification of specific unusual traffic is a potentially beneficial proactive measure, in order to attempt to gain early warning of unusual behaviour on a network, or of a device being compromised. The benefit of monitoring also extends to monitoring devices for important security updates, to ensure that each device is patched against any known vulnerabilities, and running the latest approved software revision. This process could be combined with targeted penetration testing to identify widely deployed devices which should be tested to ensure no obvious vulnerabilities are present. However, controlling and verifying devices present on networks is challenging given the numbers of devices involved.

There was a need to improve visibility of all devices connected to networks. Most large systems such as servers had agents installed, but no monitoring or control of the devices present, or how they are managed and patched.

The need to better understand the traffic experienced within SCADA networks was recognised. Concern was raised over how to correctly identify both "good" and "bad" traffic within a network, for intrusion detection and prevention systems. There were questions over when to stop traffic, and risk interrupting availability, versus permitting and then investigating after-the-fact, since detections systems are generally preferred for SCADA environments,

There was an interest in log aggregation for auditing and accountability of actions, which was felt to be a growing concern in the future with increasing remote access. There are challenges with limited bandwidth to some remote sites, and the need to ensure logs are transmitted securely.

The transition to IP-based networks brings about opportunities to improve resilience and availability by removing reliance upon centralised points of failure. This comes with significant alterations to network design and organisation, specifically around security. A distributed trust management approach would permit equipment to communicate only with other authorised devices, ensuring that any unauthorised devices introduced to networks would be unable to interfere with or communicate with authorised devices. Such an approach, without requiring a single centralised point of failure for authentication, was identified as a potential area for future work, particularly applying the concept of distributed trust in a non-product specific context**.**

3.4 Building Incident Response Capability

Capabilities to identify, respond and recover from a cyber-attack are limited at present. The current power system was not designed to handle the effects of a cyber-attack. It has been designed with n-1 redundancy as a goal, to handle the loss of generation or transmission assets. In the context of cyber security, there are many other scenarios to be prepared for. There is a need to develop faster detection of malicious or unpredicted activity and to design appropriate responses to potential cyber incidents.

Appreciating the differing context of an OT environment is crucial to handle cybersecurity in an appropriate way for an operational setting. The focus leans towards protecting systems and restoring operations. Incident responses must consider real-time and availability requirements. For example, control systems cannot be disconnected from

the network if under attack like an office computer could be. Cyber-security responses appropriate for an OT environment are needed.

Defining Responsibility. Part of incident response will be to define the level of incident handling within an operator's capability and agree responsibilities within and across organisations. Operators need to decide what needs to be passed up to, for example, the National Cyber Security Centre (NCSC), or how to engage a response across supply chain organisations, so that an incident response structure can be agreed. Also, identifying where practical help may be needed to withstand an attack, especially over a long time period: e.g. a sustained Denial of Service attack for several days. An effective coordination of the response needs to also be established so that crisis management procedures are in place for cyber security. Previous cyber-attacks have highlighted the use of cascaded attacks to reduce the efficacy of responses. Crisis management must also consider how procedures would be implemented under degraded communications, or following the failure of communications infrastructure as a result of the attack.

To resolve attack situations, organisations will need to build a reliable and strong network of partners for incident response and recovery, as well as agreeing on escalation processes and responsibility levels within and between organisations.

3.5 Knowledge of Threats

With an uncertain picture of evolving threats, utilities are expected to prepare for unknown threats to their essential services. Concerns were raised over being without a formal threat landscape for operational networks. While the latest threat landscape is constantly evolving, intelligence gathering could indicate attack trends and future security risks and help to prepare for new scenarios. The potential for an interactive platform to share an evolving picture of threats was discussed. While there are clearly some challenges to producing an all-encompassing threat landscape model, it was felt that most work is being carried out "in the dark", with limited awareness of the types of attack techniques that could be faced.

Identifying various scenarios will aid the preparation of responses to cyber incidents. It is important to consider how vulnerabilities in digital components could cause failures across the grid and to consider different threat agents and types of attack. This will help to identify high impact scenarios and build up a picture of the potential scenarios that need to be prepared for to reduce the impact of attacks.

3.6 Electricity Sector Specifics

There is the risk of single site compromises cascading into a wider system threat and affecting other organisations as well. It was noted that the involvement of cross-DNO working groups, would be needed in these circumstances. Being unprepared for cyber incidents exposes the system to the risk of cascading effects which could result in a brownout or even blackout situation. There is also the risk of manipulation of or loss of control and monitoring systems. The ability for an attacker to exert control over large loads, or indeed a significant number of smaller loads, could adversely affect system balancing and lead to blackouts. Likewise, malicious control of generation could affect supply and cause instability.

Real Time Performance. There are technical challenges with securing protection communications, due to the need for ~ 4 ms response times, and the perception that this is difficult to achieve alongside secure communications. A cost/benefit and performance analysis was felt to be necessary for securing extensive distribution networks. The security risks to assets from secondary substation and below needs further investigation. The impact of encryption on performance and availability to discover where high speed encryption applications may be needed. Encryption, for example, could add cost, without providing sufficient benefit.

Active Network Management New technology such as Active Network Management (ANM) is presenting DNOs with new security challenges. ANM requires connections to both the primary control network and secondary telemetry networks, limiting the traditional approach of segregating these networks. With the potential introduction of servers and other equipment within substations, and wider deployment of connected monitoring equipment, itself vulnerable to attack and manipulation, a more ANM-oriented network is introducing new security and management requirements. This was considered important, due to the ability for ANM to interact with and control generation equipment on third party sites and networks.

3.7 Organisational Culture

Unwillingness to risk introduction of complexity which may otherwise impact on availability means that operational networks frequently lack the same security measures found on corporate networks, such as 2-factor authentication and other measures to ensure security during sign-in processes.

The challenge of management not being familiar with the currently deployed systems was also highlighted as a concern, given the significant changes in approach to security required with newer, more interconnected equipment. Another challenge identified was in keeping up with advances in IT, and security in general. The pace of change and developments, and the speed with which information about vulnerabilities may be disseminated makes it difficult for small cyber security teams to keep up to date with information. A need for training in cyber security was also highlighted, to ensure everyone who needs it has a strong basic knowledge of the essentials for securing systems. The ability for a 'small' mistake to completely compromise the security of an installation was a concern. An example given was of an engineer bridging the 'secure' operational side of the network to a WAN link using a patch cable while working on equipment. Knowing the organisational context that security solutions are to be implemented and maintained within gives a broader view of what is needed to build a security culture and more secure ways of working.

Overall governance of cybersecurity within the organisation as a whole needed some attention. Progress had been made in different business units but had resulted in different approaches and security policies, which would be better unified and coordinated. There was interest in establishing a broad governance and security architecture, to create a secure state to aim towards when deploying and designing systems.

IT/OT Integration The organisational boundaries between operational and corporate sides of IT provisions were also highlighted as being a concern – equipment not installed

by IT and not connected to the corporate IT network was considered to be outside the responsibility of IT. Advances in corporate security (single sign-on, enforced 2-factor authentication etc.) had not been replicated on the operational network due to IT not having visibility of activity on the OT side.

It was recognised a new model for working was required to manage the increasing numbers of computer systems (such as servers) in operational networks. There was a desire for the IT teams to manage such systems, as this was more within their area of expertise, but this presented challenges such as providing access for corporate IT staff into substations.

Supply Chain Security Based upon the significance with which it was emphasised by all DNO members consulted, some of the largest risks to DNO operations appear to be posed by their supply chains, and by connections which are permitted from external third parties, operating outside the control of the DNO's business and security policies. Taking some measures to begin to increase the level of trust in suppliers and components is an important step.

Equipment vendors increasingly wish to have remote access abilities to provide support. This introduces risk if a supplier's internal procedures are insufficient to prevent abuse of this access, or if there are technical weaknesses in the implementation of the remote access system. Currently, such connections are established through VPN links, but with very little logging and auditing of the specific equipment connected to, and actions carried out. The number of external connections to controlled networks will increase, both due to practical and business reasons. Connections to third party generation sites are one such example, where it is necessary for relatively simple communications to take place over an external IP network. While best efforts are made to assume the worst-case when considering third party networks, there is clearly potential for compromise here. There would be security benefits in having the capability to segment access to only a particular type of equipment, or localised site, to reduce exposure of assets to those with remote access. Care should be taken around legacy devices and protocols being introduced to IP-based networks, to ensure they cannot be reached from untrusted areas of the network, such as incoming VPN connections and similar.

The reliance of DNOs upon their supply chain of suppliers, vendors and subcontractors was recognised as being a major limitation of current cybersecurity measures. Questions were raised on how to audit, assess and review the cybersecurity competencies of third parties, especially while considering implementation-specific requirements or validation of vendor claims. There is also the issue of the validation of the supply chains of the vendors themselves. A code of practice for suppliers and other third parties, covering their expected capability in cyber security, was highlighted as an important requirement going forward.

Within substations, a significant concern identified was in managing suppliers' understanding of substation implementations and preventing inappropriate hardware from being installed in substation environments, where it is left unmanaged with security issues. For example, features that may be disabled on a product may still leave functioning remnants, capable of communication and remote exploitation.

The trade-offs and challenges of embedded systems were also discussed, specifically around short support periods from Original Equipment Manufacturer (OEM), which are

often only a few years. The need for significantly longer equipment lifespans, causing vulnerabilities and weaknesses to get "locked in" with no clear way to mitigate or resolve them without OEM involvement.

Inter-Organisational Issues. There is a need to define collective responsibility across interdependent organisations, in order to secure energy systems and to ensure all market players and applications have achieved an adequate level of cyber-security. Aiming for a consistent approach across organisations will require collaborative agreements on cyber security responsibilities and increasing cyber-awareness both within and between organisations. Considering suppliers and components that affect the criticality of an operator and understanding security requirements in different operational contexts will help to adapt countermeasures to different use cases. With a better understanding of appropriate countermeasures, DNOs can agree obligations with suppliers to implement technical or organisational security measures and make plans to ensure compliance with those obligations. This could include a classification of threats, risks and vulnerabilities that indicates how essential certain measures are and the level of implementation required depending on criticality for the operator.

3.8 Recognising the Shared Context

It was important to bring together a shared understanding of the future energy situation through this research activity with different players. Operational teams were getting to know new capability and new systems, learning an unfamiliar context. For example, keeping the power network stable involves controlling generation equipment on third party sites, managing Electric Vehicle (EV) charging patterns, so that power flows can be optimised within the constraints of the network. The resulting increase in complexity and data traffic, mean the availability and integrity of measurement data is essential to minimise unnecessary curtailment of generation. Agreement on cybersecurity requirements and code of conduct is also necessary between generators, DNOs, aggregators and other third-party providers.

The academic and industry experts participating in this research activity gained a closer understanding of the issues the DNOs face. This has provided a shared understanding from which to design more applicable cybersecurity solutions and deployments going forward. Our multi-actor approach was able to consider the wider engineering solution, beyond security, for wider protection from undesirable consequences, especially where security is lacking. Knowing the operational perspective allows cybersecurity to be managed from an understanding of the organisational context.

Achieving security across organisational boundaries arose as a significant issue across several topic areas, including cooperation during incident response. The collective responsibility across interdependent organisations requires an adequate cybersecurity level across all market players.

Painting the picture of both organisational and sectoral contexts provided a backdrop of understanding among different players for ongoing cybersecurity research projects at PNDC. A quarterly theme meeting continues to bring together members from different companies in the energy sector to further guide the research programme of PNDC.

4 Exploring Impact and Uncertainty

The FES all present an increased use of smart technology and therefore an increased exposure to cybersecurity risks. There are multiple dependencies on assurance decisions in the supply chain and across diverse actors. It is important to recognise and respond to risks across all interconnected stakeholders and elements so that threats are not missed at different points across those interactions. It is necessary to secure beyond just the critical components with everything interconnected and a wide set of roles and technologies supporting the system. An integrated system inherits the security limitations of each interacting component. Transparency of assurance actions will be necessary where there is dependency on the cybersecurity maturity level of other actors.

Attacks are inevitable and are constantly evolving. By establishing clear responsibility for assurance and effective coordination across stakeholders, a broader protection across people, processes and technology can be attained. This would be aided by effective measures to evaluate the assurance of all components and their interactions and make sure appropriate areas are addressed across all aspects of the socio-technical system.

An exploration of impacts and consequences in a power system context was carried out. Sharing an appreciation for potential consequences can give different stakeholders a reason to take the necessary action. Table 2 outlines a selection of potential impacts showing consequences of cyber events including data loss, data modification or unwanted control actions.

There may also be indirect or unintended consequences involved in the system's response to a threat. Considering the system functions and how particular workflows and stakeholders are affected by the sequence of the threat through the technology, people and processes can help to uncover potential consequences of a threat.

4.1 Impact Analysis

Consider the roles, processes and underlying IT and OT technologies involved in delivering energy system functions, the assets and actors involved at each step in a business process. The flow of activities can be mapped onto components and interactions to identify the assets and actors [18]. This will build a picture of the systems, devices, communications channels, internal and external actors etc. that are supporting the functions [15]. The expected 'deep digitalisation' of assets [9] correspondingly requires a deep enough knowledge of system operation to know all the sources of control and automation and potential access pathways for attackers. Detailing the assets that contribute to essential functions and their impact if unavailable or compromised and from where changes can be made to configurations and settings [15]. The scale involved also changes the threat exposure i.e. how many instances of the data or device there are and if an asset is centralised or distributed [18].

A functional example such as operating within network constraints requires the secure retrieval of data from the network for real-time information on thermal ratings and voltage stability. This may also require access to smart meter voltage data or power flow and voltage information at DER connections. The cybersecurity of a 3rd party data centre or cloud service could also be a part of this flow of information. Threats to

Table 2. Potential impacts of cyber attack [19, 20, 21]

Event	Consequences
Temporary outages	Activation of load shedding tripping of protection communications outage causing delay in data transmission/control actions
Affecting synchronisation	Coordinating connection and re-connection of generators, without proper synchronisation could destroy generators
Resource unavailable	Denial of service attacks making a resource unreachable or unresponsive, and affecting data streams from devices e.g. phasor measurement data
Stealing data	Extracting confidential information social engineering to gain credentials Eavesdropping, sniffing IP packets, intercepting wireless transmission side-channel attack to infer cryptographic keys from unintended information leakage. Impacting customer privacy, passwords, unauthorised access to systems
Manipulation of data	Injecting false data, e.g. man-in-the-middle attack hiding true status from control centre modifying data e.g. tampering with sensor data to cause inappropriate load management resulting in unnecessary load shedding or generator trip out manipulating measurements undesired system behaviours
Unauthorised access	Access to private data identity spoofing, impersonating an authorised user e.g. man-in-the-middle attack, message replays intrusion affecting behaviour of system e.g. via open ports or malware
Sabotage	Embedding malware to launch an attack later
Asset replacement	Considerable lead times for replacing destroyed assets
Unintended consequences	Unknown consequences aggravated by evolving threats and interdependencies across diverse actors

consider would include the unauthorised access or potential data manipulation of the SCADA monitoring and notifications of thermal or power flow constraints [22].

The resolution of network constraints being either demand led or generation led would require secure access to flexibility resources for service activation or dispatch. The cybersecurity of control actions in the actuation of DER, aggregator services or active customers would need to minimise the risk of inappropriate control actions or unauthorised access. The assessment of the operational performance of flexibility services could require cybersecurity performance to be included in their reliability metrics [22].

Mapping the entire thread of activity for energy system functions onto the supporting processes, assets and roles in this way presents the impact of threats on essential functions. The aim is to apply mitigations to protect these functions and minimise the impact of events.

5 Resilience Efforts

To improve resilience across interdependent actors, cybersecurity expectations and requirements appropriate to each actor will need to be defined and agreed for [22].

- Aggregators supplying services to the power grid via DSOs from assets on the distribution network.
- Active customers and developers exporting power to and importing power from the distribution network.
- Increasing volumes of Distributed Energy Resources with connection arrangements via distribution networks, the cybersecurity aspects of their operational role and their participation in markets via DSOs or aggregators.
- Combined approaches for supply chain actors to engage with multiple DSOs.
- Transmission connected demand and generation, with cybersecurity and resilience actions included in their connection agreements.

Resilience efforts across all actors need to include activities such as:

- Testing changes to assets for cybersecurity or operational impact before deployment.
- Managing access and identity across human and IoT actors.
- Involving stakeholders in threat and vulnerability management for access to a more thorough threat landscape.
- Coordinating incident response activity with appropriate external entities.
- Constructing evidence, contracts, and agreements with third parties.
- Assigning and managing cybersecurity responsibilities across personnel and all relevant stakeholders [23]

Each stakeholder will hold a different level of interest in contributing to system resilience and differing degrees of influence on the cybersecurity level of the system. Considering the relative positions of different stakeholders would reflect how best to engage each actor in required resilience actions. Only 26% of security issues can be addressed by technology alone, leaving 74% requiring people or policies to form a solution to these issues [24].

To know and measure operational resilience requires defined and implemented processes. Processes offer the context for how to achieve a resilience activity with specifics related to roles, technology and operations. The processes that contribute to resilience need to be performing well to build a confident state of readiness in the face of new and different threats and risks. The supporting assets and interactions that enable the functionality of smarter grids need to be cybersecure and reliable. Processes aiming for operational resilience need to be embedded within functional activities to improve the security and resilience of essential services [25].

Reporting on assurance actions across organisations may be necessary where there are dependencies on other actors to deliver a function or service. Preparing combined resilience actions and measures per function would help to define clearer responsibilities for assurance and effective coordination across stakeholders.

6 Conclusions

This work enabled a thorough observation of the cybersecurity situation for the energy sector by inviting insights from different perspectives to be shared. The energy system is evolving into a complex web of demand and supply across diverse actors. It will increasingly rely on the security of the information infrastructure supporting it, and the resilience of a digitalised operating environment. To make sense of the latest threat landscape requires a wider sharing of knowledge and awareness among all stakeholders for organisations to make better informed decisions and actions. To construct a picture of the latest operating conditions and vulnerabilities requires knowing the resilience of different assets and interactions that make up the functions of the energy system. Along the thread of activities required to deliver each function, a change in vulnerability in one area could increase the threat affecting other areas. The number of instances of a vulnerable component will affect the scale of threat a function is exposed to. Processes and measures that allow for a greater transparency of cybersecurity activities will encourage preparations and build the necessary trust across interconnected stakeholders. This will enable a more robust response to changing events on the system.

This paper has provided an investigation of cybersecurity issues and concerns for utilities to provide an organisational and future energy system context for the ongoing design of cybersecurity improvements. Methods and approaches have been recommended for improving resilience across interdependent actors and to minimise the impact and consequences of cyber-attack. With smart digital technology deployed at scale, cyber governance must provide an essential foundation for our future energy scenarios with the capability to, repeatedly and reliably, assure the integrity of interconnected systems and users.

This work led the way to future cybersecurity projects at PNDC including improving incident response capabilities, asset discovery on power communications networks, identification and analyses of vulnerabilities in network assets and penetration testing of electric power assets.

References

1. Hurst, W., Merabti, M., Fergus, P.: A survey of critical infrastructure security. In: Butts, J., Shenoi, S. (eds) Critical Infrastructure Protection VIII. ICCIP 2014. IFIP Advances in Information and Communication Technology, vol. 441. Springer, Berlin (2014)
2. Glaser, B.G.: Theoretical sensitivity (1978)
3. Burns, M.: Participatory operational and security assessment on homeland security risks: an empirical research method for improving security beyond the borders through public/private partnerships. J. Transp. Secur. **11**, 85–100 (2018). https://doi.org/10.1007/s12198-018-0193-1
4. Charmaz, K.: Discovering chronic illness: using grounded theory. Soc. Sci. Med. **30**(11), 1161–1172 (1990)
5. Gjørv, G.H.: Security by any other name: negative security, positive security, and a multi-actor security approach. Rev. Int. Stud. **2012**(38), 835–859 (2012). https://doi.org/10.1017/S0260210511000751
6. Bradfield, R., Derbyshire, J., Wright, G.: The critical role of history in scenario thinking: Augmenting causal analysis within the intuitive logics scenario development methodology. Futures **77**, 56–66 (2016). https://doi.org/10.1016/j.futures.2016.02.002

7. Mead, N.R., Woody, C.C.: Cyber Security Engineering. Addison-Wesley, A Practical Approach for Systems and Software Assurance (2017)
8. Van der Heijden, K., Bradfield, R., Burt, G., Cairns, G. and Wright, G.: The sixth sense: Accelerating organizational learning with scenarios, John Wiley & Sons (2009)
9. National Grid ESO. Future Energy Scenarios (2021). https://www.nationalgrideso.com/future-energy/future-energy-scenarios/fes-2021
10. Dos Santos, D., Dashevskyi, S., Wetzel, J.: Amnesia: 33 How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices. Forescout Research Labs (2021). https://www.forescout.com/research-labs/amnesia33/
11. Piccalo, M.: How to Use Asset Management as the Foundation for OT Network Segmentation, Forescout, 21 10 2019. https://www.forescout.com/company/blog/how-to-use-asset-management-as-the-foundation-for-ot-network-segmentation/. Accessed 26 July 2021
12. Forum of Incident Response and Security Teams. Common Vulnerability Scoring System version 3.1: Specification Document, June 2019. https://www.first.org/cvss/specification-document#Environmental-Metrics. Accessed 26 July 2021
13. OfGem. Investigation into 9 August 2019 power outage (2019). https://www.ofgem.gov.uk/publications-and-updates/investigation-9-august-2019-power-outage
14. Department for Business Energy and Industrial Strategy, "Distributed Energy Resources - Cyber Security Connection Guidance," Energy Networks Association (2020). https://www.energynetworks.org/industry-hub/resource-library/distributed-energy-resources-(der)-cyber-security-connection-guidance.pdf
15. Bochman, A.A., Freeman, S.: Countering Cyber Sabotage. CRC Press, Boca Raton (2021)
16. Bochman, A.: The End of Cybersecurity, Harvard Business Review https://store.hbr.org/product/the-end-of-cybersecurity/BG1803
17. National Grid ESO. Bridging the Gap to Net Zero March 2021. https://www.nationalgrideso.com/future-energy/future-energy-scenarios/bridging-the-gap-to-net-zero. Accessed 27 July 2021
18. European Commission. Data protection impact assessment for smart grid and smart metering environment 27 September 2018. https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en#dpia-template-and-users. Accessed 27 July 2021
19. Congrès International des Réseaux Electriques de Distribution, RESILIENCE OF DISTRIBUTION GRIDS WORKING GROUP, in International Conference on Electricity Distribution 31.05.2018. http://cired.net/cired-working-groups/resilience-of-distribution-grids
20. Liu, R., Vellaithurai, C., Biswas, S.S., Gamage, T.T., Srivastava, A.K.: Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. IEEE Trans. Smart Grid **6**(5), 2444–2453 (2015). https://doi.org/10.1109/TSG.2015.2432013
21. Yang, Y., Littler, T., Sezer, S., McLaughlin, K. and Wang, H.F.: Impact of cyber-security issues on Smart Grid. In: 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp. 1–7 (2011). https://doi.org/10.1109/ISGTEurope.2011.6162
22. Energy Networks Association. Open Networks Future Worlds. Developing change options to facilitate energy decarbonisation, digitisation and decentralisation, 31 July 2018 https://www.energynetworks.org/assets/images/Resource%20library/ON18-WS3-14969_ENA_FutureWorlds_AW06_INT%20(PUBLISHED).pdf. Accessed 27 July 2021
23. US Department of Energy. Office of Electricity, Electricity Subsector Cybersecurity Capability Maturity Model v. 1.1., February 2014. https://www.energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014. Accessed 27 July 2021
24. Cisco. Cisco 2018 Annual Cybersecurity Report. https://www.cisco.com/c/en_uk/products/security/security-reports.html#~more-reports

25. Allen, J.H., Curtis, P.D., Gates, L.P.: Using Defined Processes as a Context for Resilience Measures. Software Engineering Institute. Carnegie Mellon University, December 2011. https://apps.dtic.mil/sti/pdfs/ADA610464.pdf
26. Allen, J.: Measures for managing operational resilience. EDP Audit, Control, Secur. **44**(6), 1–6 (2011). https://doi.org/10.1080/07366981.2011.643192
27. Whyte, W.F.: Learning from the Field. A guide from experience, Sage Publications (1984)
28. Beech, N., Arber, A., Faithfull, S.: Restoring a sense of wellness following colorectal cancer: a grounded theory. J. Adv. Nurs. **68**(5), 1134–1144 (2012). https://doi.org/10.1111/j.1365-2648.2011.05820.x