

Lessons Learned from a Cybersecurity Risk Assessment of OpenADR in Smart Grid Planning

Gencer Erdogan
Sustainable Communication Technologies
SINTEF Digital
Oslo, Norway
0000-0001-9407-5748

Aida Omerovic
Sustainable Communication Technologies
SINTEF Digital
Oslo, Norway
0000-0001-8868-597X

Eivind Solvang
Energy Systems
SINTEF Energy Research
Trondheim, Norway
0000-0002-5532-688X

Andreas Killingberg
Lnett AS
Sandnes, Norway
andreas.killingberg@l-nett.no

Are Kvinnesland
Lnett AS
Sandnes, Norway
are.kvinnesland@l-nett.no

Inge Abrahamsen
Avinor
Oslo, Norway
inge.abrahamsen@avinor.no

Abstract—Integrating OpenADR in smart grids enhances demand-response but introduces cybersecurity risks that must be addressed early in the planning phase. This paper presents a cybersecurity risk assessment case study for Lnett, a Norwegian DSO planning OpenADR implementation. Using a six-step, lightweight method, we identified 10 key cybersecurity risks. Stakeholder feedback highlighted the method’s structured approach, iterative process, and external expertise, while also noting challenges in defining the analysis object and tracking documentation. We derived six lessons and practical recommendations for DSOs implementing OpenADR or similar protocols, contributing to stronger cybersecurity resilience in demand-response systems and informing future smart grid risk assessments.

Index Terms—cybersecurity risk assessment, smart grid resilience, OpenADR protocol, critical infrastructure security, demand-response systems.

I. INTRODUCTION

The increasing reliance on digital technologies in modern power grids introduces new cybersecurity challenges that threaten operational reliability and security. As power grids become more interconnected and automated, they evolve into smart grids, which are attractive targets for cyber-attacks ranging from data manipulation [1] to large-scale denial of service attacks [2]. To facilitate grid flexibility and automate demand-response, electricity distribution system operators (DSOs) implement protocols such as Open Automated Demand Response (OpenADR), which enable real-time energy management [3]. However, integrating OpenADR into smart grid operations may introduce cybersecurity risks that need to be identified and mitigated early in the smart grid planning phase.

This paper presents a cybersecurity risk assessment case study of OpenADR within Lnett’s operational environment in Southern Norway. Lnett, a DSO, aims to implement OpenADR to enable demand-response flexibility for customers such as Avinor, a state-owned airport operator. As the implementation is still in the planning phase, Lnett seeks to identify cybersecurity risks early. However, assessing cybersecurity risks introduced by active digital measures during grid planning is

challenging, as planning occurs at a conceptual stage, often years before implementation, and lacks concrete details on digital components at this early phase. Traditional quantitative risk assessment methods are impractical at this stage, as they require detailed incident descriptions and precise risk quantification. Instead, lightweight, qualitative risk assessment approaches are needed to identify vulnerabilities and assess their impact during the smart grid planning phase [4].

In previous work, we developed a lightweight, six-step cybersecurity risk assessment method to help grid planners assess cybersecurity risks during the smart grid planning phase [4], which we also apply in the case study presented in this paper. The goals of the case study are to:

- Identify cybersecurity risks related to OpenADR integration in the planned Lnett-Avinor solution.
- Assess the feasibility of our risk assessment method based on stakeholder feedback.
- Derive lessons learned and provide practical recommendations for OpenADR implementation in similar contexts.

Our study identifies 10 cybersecurity risks related to OpenADR integration, presents stakeholder feedback on our method’s effectiveness, highlighting strengths and areas for improvement, and provides six practical recommendations for DSOs and practitioners implementing OpenADR or similar demand-response protocols in contexts similar to our study.

The remainder of the paper is structured as follows: Section II outlines our risk assessment method and case study execution. Section III describes the case study context and target of analysis. Section IV presents the identified cybersecurity risks and stakeholder feedback. Section V discusses lessons learned and practical recommendations. Section VI reviews related work, and Section VII concludes the paper.

II. METHODOLOGY AND EXECUTION

In the following, we provide a brief description of the six steps of our method. Additionally, for each step, we describe the specific outputs relevant to the case study. For a detailed

description of the method and the rationale behind each step, we refer to our previous work in [4].

Step 1: Describe the target of analysis. This step defines the scope and boundaries of the cyber risk assessment. High-level graphical system diagrams are created to illustrate relevant physical and digital components of the planned grid solution. Section III describes in detail the context and target of analysis.

Step 2: Identify assets to protect. This step determines the assets in the planned grid solution that require protection from cyber risks. In the case study, our primary concern is cyber risks that may compromise the reliability of electricity supply in the grid with the planned solution. Thus, we want to protect the smart grid from cyber risks such that electricity supply is not disrupted or harmed. This means that our primary asset is *reliability of electricity supply* for which we require protection, and we want to identify cyber risks that may impact this asset. All other relevant supporting assets, which—if compromised—may impact our primary asset, are listed in the column *What assets does it harm?* in Table IV.

Step 3: Define likelihood and consequence scales. This step defines likelihood and consequence scales for cyber risks. A frequency-based scale is used for likelihoods, while consequences are described in terms of qualitative impact values. For the case study, we defined together with the stakeholders the likelihood scale in Table II, and the consequence scale in Table III. Note that the consequence scale is defined for the primary asset *reliability of electricity supply*. Additionally, a risk evaluation matrix is created based on the defined likelihood and consequence scales. This matrix determines how different likelihood-consequence combinations map to one of three risk levels: {*High, Medium, Low*} (see Fig. 2). The risk levels were also defined together with stakeholders. For example, if a risk is classified as *Unlikely* in likelihood but has a *Major* consequence, the risk level is considered *High*. In the case study, risks classified as *High* or *Medium* were deemed unacceptable and required further evaluation for possible treatment, while *Low* risks were considered acceptable.

Step 4: Identify cyber risks. A structured brainstorming session, including relevant stakeholders, is conducted to identify potential cyber risks. High-level risk tables are created to list identified risks, their sources, and potential impacts. Section IV-A describes all the risks identified in the case study, while the high-level risk table is shown in Table IV.

Step 5: Estimate cyber risks. Identified risks are assessed using the likelihood and consequence scales from Step 3, based on expert judgment and additional resources such as security reports and scientific literature. Section IV-A provides a detailed description of the identified risks, including their likelihood and consequence estimates, which were assessed in collaboration with the stakeholders during the case study.

Step 6: Evaluate cyber risks. The risk evaluation matrix defined in Step 3 is used to determine whether a risk is acceptable or not. As explained in our previous work [4], the evaluated cyber risks serve as input to a broader risk assessment that considers additional factors, such as weather-related risks. Risk treatments are addressed within this broader

assessment, typically conducted as part of grid planning, and are therefore not considered as an explicit step in our method.

The case study was conducted over approximately seven months, from February 3, 2024, to October 21, 2024. During this period, we held seven meetings with the stakeholders, as shown in Table I. The columns *RA-Team*, *L-Team*, *A-Team*, and *RA Step* in Table I refer to participants from the Risk Assessment Team (SINTEF), Lnett’s Team, Avinor’s Team, and the Risk Assessment Step, respectively.

TABLE I
CASE STUDY EXECUTION MEETINGS

Date	Duration	RA-Team	L-Team	A-Team	RA Step
03.04.2024	1 hour	3 Pts.	2 Pts.	1 Pts.	Step 1
23.04.2024	1 hour	3 Pts.	3 Pts.	1 Pts.	Step 1
10.05.2024	2.5 hours	3 Pts.	4 Pts.	1 Pts.	Step 1&2
12.06.2024	2 hours	3 Pts.	3 Pts.	3 Pts.	Step 2&3
14.06.2024	4.5 hours	3 Pts.	6 Pts.	3 Pts.	Step 4
05.09.2024	4 hours	3 Pts.	4 Pts.	1 Pts.	Step 4&5
21.10.2024	2 hours	3 Pts.	3 Pts.	1 Pts.	Step 6

These meetings were mainly used to discuss the progress of the cyber risk assessment in relation to the steps in the method. They also provided a platform for all teams to clarify and confirm information regarding the target of analysis, identified risks, risk estimates, etc.

Two of the meetings (June 14, 2024, and September 5, 2024) were half-day workshops where all teams participated in brainstorming sessions to identify and estimate potential cyber risks. These workshops brought together a diverse group of participants: SINTEF contributed with two Senior Research Scientists specializing in risk analysis and cybersecurity, along with one Senior Research Scientist in energy systems. Lnett was represented by one ICT Security Coordinator, one Power System Analyst, two Solution Architects, and two Senior Engineers. Avinor’s team included one Head of Aviation Data Office, one Security Architect, and one IT Security Consultant. This combination of IT and OT professionals facilitated a comprehensive discussion on cybersecurity risks.

In terms of effort hours, the total time spent in meetings was 63.5 person hours. Additionally, the Risk Assessment Team spent an estimated 22.5 hours preparing content and processing new information before and after each meeting. Given seven meetings (counting both phases), this accounts for 180 person hours. Thus, the total person hours spent for the entire case study execution was: $63.5 + 180 = 243.5$ person hours.

III. CASE STUDY CONTEXT

Fig. 1 illustrates the planned solution for electricity demand-response flexibility between Lnett and Avinor (target of analysis) in the case study. Lnett’s objectives include enhancing electricity grid flexibility while ensuring cybersecurity and operational continuity. Avinor is responsible for responding to OpenADR signals they receive from Lnett to manage energy loads at their facilities. Avinor’s role also includes

ensuring that incoming signals are authenticated and acted upon without compromising critical airport operations. Third-party technology providers are also part of the case study context, but they are not named due to confidentiality reasons and because they did not directly participate in the case study. The third-party technology providers include a tool provider and an IT infrastructure provider, which introduce dependencies that must be considered in the risk assessment.

The stages outlined in the following paragraphs correspond to the processes depicted in Fig. 1, focusing on the specific case of communication between Lnett and Avinor using the OpenADR protocol.

Stage 1: Defining signals. Supervisory Control and Data Acquisition (SCADA) operators at Lnett define OpenADR signals that include parameters such as setpoints, power levels, and time intervals. These signals can be generated either manually or automatically. Automatic generation relies on measurements from the power grid, which flow from SCADA to Lnett’s Supervisory Control System. While the current solution involves data exchange with GridTools, a modular decision support tool designed to improve the operation of regional and local distribution grids, the long-term plan is for automated input into the SCADA systems. GridTools enables Lnett to forecast potential problems in the grid by using flexible resources through its automated processes. Currently, all incoming traffic to Lnett is filtered by their firewall.

Stage 2: Generating signals. Lnett’s Supervisory Control System acts as a bridge between SCADA and Lnett’s server hosted by the IT infrastructure provider. The server has the OpenADR protocol installed and enables communication via REST API. Although this setup is not yet implemented, GridTools is a temporarily solution with the desired functionality. In the planned setup, Lnett’s Supervisory Control System generates OpenADR signals based on SCADA input and predefined rules. Additionally, it can send warnings back to SCADA if a customer fails to respond to a signal. The intermediary system with GridTools compensates for missing functionality in Lnett’s current SCADA setup.

Stage 3: Signal exchange with Avinor. Lnett’s server uses a REST API with OpenADR to send the generated signals over the open internet to Avinor’s Supervisory Control System. Lnett expects one of three response types from Avinor: (a) confirmation or rejection of load reduction, including potential adjustments to power levels, (b) continuous updates during the reduction process, (c) reports on actual power usage. Lnett’s server processes Avinor’s responses, verifying their correctness. If a rejection is received, the server forwards the rejection to the SCADA operators, who re-evaluate the response and adjust the signal for a new request iteration.

Stage 4: Signal reception and processing at Avinor. Avinor’s Supervisory Control System receives signals and initiates workflows. This system serves as a central information hub, integrating data from multiple components at Avinor’s facilities. It features a dashboard for visualization and limited command capabilities, such as forwarding commands to the Central Operations System. An operations engineer must review the

signal and forward it to the Central Operations System without altering it. The engineer can also define groups of energy components to disconnect for reducing energy consumption.

Stage 5: Load Reduction. Based on received signals, Avinor’s Central Operations System decides whether to reduce load. The goal is to lower peak power usage in non-critical systems such as ventilation, heating, and cooling. This process helps optimize energy consumption and supports grid stability during high-demand periods.

IV. RESULTS

A. Identified Cybersecurity Risks

This section presents the identified cybersecurity risks (R) along with their assessed likelihood and consequences. The likelihood and consequence scales used in the risk assessment are in Table II and Table III, respectively. Fig. 2 illustrates the risk evaluation matrix, which maps all identified risks based on their likelihood and consequence values, categorizing them into three risk levels: High, Medium, or Low. A high-level summary of all identified risks is provided in Table IV.

TABLE II
LIKELIHOOD SCALE

Likelihood	Description	Definition
Likely	Two to five times per year	[2, 5>: 1y
Possible	Less than twice per year	[0.5, 2>: 1y
Unlikely	Less than once per two years	[0, 0.5>: 1y

TABLE III
CONSEQUENCE SCALE FOR RELIABILITY OF ELECTRICITY SUPPLY

Consequence	Description
Major	Severe disruption with long-term consequences.
Moderate	Significant but manageable disruption.
Minor	Minimal disruption to grid operations.

R1: Communication interception and manipulation via Man-in-the-Middle (MitM). MitM attacks are relatively common and technically feasible given that the OpenADR signals are transmitted over the "open Internet" and an open API is used [1]. However, the use of HTTPS for end-to-end encryption reduces the likelihood, and the motivation for this type of attack must be high. The likelihood is therefore assessed to be *unlikely*. On the other hand, if such an attack is carried out and succeeds, the consequences would be *major* because of the potential for compromised data/signal integrity, breaches of confidentiality, and operational disruptions.

R2: Distributed Denial-of-Service (DDoS) attack. DDoS attacks are common and relatively easy to execute, with such attacks even being purchasable from established hacker networks [2]. The likelihood of this risk is therefore *likely*. If such an attack occurs, the consequences would be *major* as it disrupts communication and operations, which affects

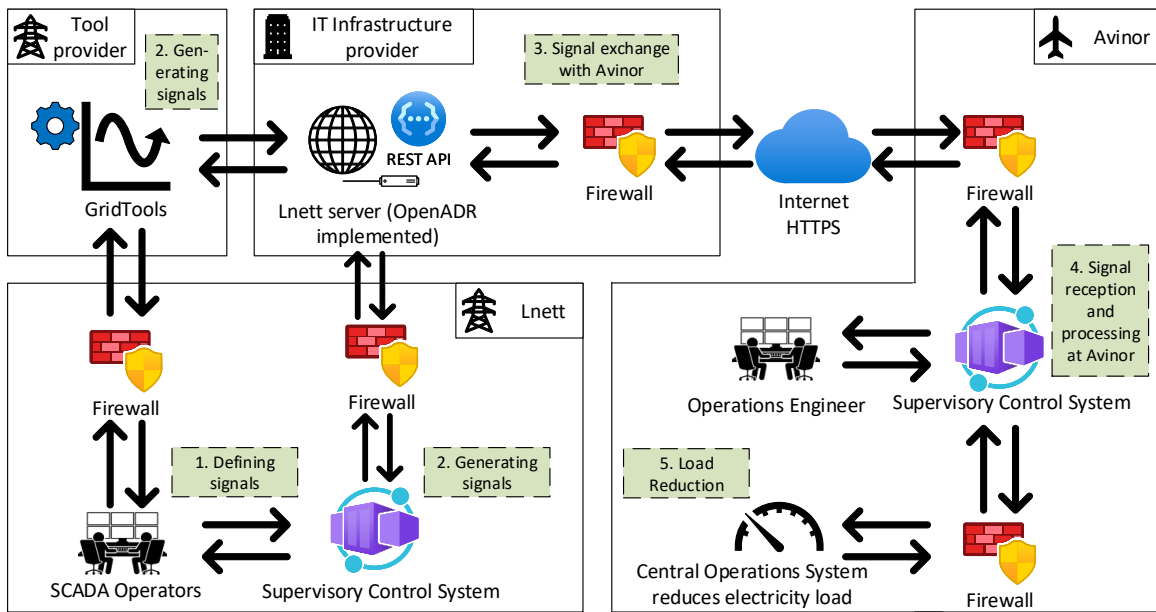


Fig. 1. Case study target of analysis (planned solution for electricity demand-response flexibility between Lnett and Avinor).

the overall reliability of Lnett’s OpenADR based demand-response service. Prolonged unavailability of the demand-response service could impact the security of electricity supply. Additionally, the third-party tool provider or IT infrastructure provider could also be a target of DDoS attacks, further affecting Lnett’s demand-response service.

R3: Increased attack surface through SCADA Internet/network integration. SCADA systems are known to have vulnerabilities and are frequently targeted by attackers [5]. The long-term plan involves the automatic flow of information into SCADA from tools such as GridTools. This may increase the attack surface, making the system more vulnerable to cyber threats, raising the likelihood of this risk to *possible* [5]. If an attack occurs, the consequences would be *major*, as it could compromise safety and operational integrity, with the potential for catastrophic impacts on both infrastructure and security. To reduce the likelihood of compromise in future solutions, communication must be secured, however, the consequences will always remain high.

R4: Increased attack surface due to customer growth. The likelihood of this risk increases with more customers and connections, as a larger user base introduces complexity and potential vulnerabilities. However, implementing and enforcing appropriate measures can mitigate this risk, keeping the likelihood at *possible* [6]. The consequence is *moderate*, as added complexity does not necessarily lead to immediate or severe impacts. This is because there are inherent limitations to what an individual customer can do within the system regarding OpenADR signals, and the attack surface does not necessarily scale proportionally with the number of customers (e.g., increasing from 10 to 100 customers).

R5: Unauthorized access and manipulation of OpenADR signals via IT Infrastructure provider. If an attacker gains

unauthorized access to the Lnett server where the REST API is implemented, OpenADR signals could be altered or stopped, leading to major disruptions in the demand-response service [7]. The third-party IT infrastructure provider is a trusted partner of Lnett, with strong security routines and no such incidents reported in the past, which keeps the likelihood of this risk *unlikely*. However, the consequence of this risk is *major*, as it could impact operational stability and create a “single point of failure.” For instance, if Lnett’s server fails, Avinor could lose part of its power supply, potentially leading to severe consequences. This risk scales up if Lnett has a larger customer base relying on the demand-response service.

R6: Manipulation of signal in transit. The likelihood of manipulation of signals in transit is *unlikely* because end-to-end encryption is used. However, advanced threats may still be able to decrypt traffic and carry out MitM attacks on encrypted communication [8]. Moreover, even without decrypting the communication, attackers could infer sensitive information through traffic analysis techniques, especially in restricted application areas such as energy distribution [9]. While encryption provides end-to-end security, manipulation remains possible before a signal is sent from the IT infrastructure provider to Lnett’s customers. If such manipulation occurs, the consequences are *major*, because incorrect actions resulting from manipulated signals could destabilize the security of electricity supply and lead to significant operational and safety-related impacts.

R7: An insider threat at IT infrastructure provider sends malicious signals to customers. The likelihood of this risk is *unlikely*, depending on the IT infrastructure provider’s internal security controls and employee practices. However, based on a survey from 2024, insider threats pose significant challenges for cyber-physical systems and 74% of organizations acknowl-

		Consequence		
		Minor	Moderate	Major
Likelihood	Unlikely	Low	Low: R10	High: R1, R5, R6, R7
	Possible	Low	Medium: R4	High: R3, R9
	Likely	Medium	High: R8	High: R2

Fig. 2. Risk evaluation matrix for the risks R1-R10.

edge an increase in insider attacks [10]. If malicious signals are sent to Lnett’s customers, the consequences are *major* due to significant operational disruptions and a potential loss of trust, particularly if agreed load reductions are not implemented. However, executing such an attack would require a high level of domain knowledge. For instance, individuals managing servers at the IT infrastructure provider may lack understanding of the system’s operational context.

R8: Updates or upgrades cause system failures. The likelihood of this risk is *likely* because system failures due to updates or upgrades have historically occurred regularly. This is a common problem in smart grids [11]. The consequences are *moderate*, as such disruptions are typically short-term and lead to temporary service interruptions, but they could escalate if multiple interdependent systems, including OpenADR, are affected simultaneously. Lnett has experienced many instances where upgrades or changes have caused unavailability and errors, such as expired certificates leading to system failures.

R9: API tokens compromised. The likelihood of this risk is *possible*, particularly if HTTPS is implemented but not sufficiently secured [8], [12]. If OpenADR API tokens used for identification are compromised, the consequences are *major*, as unauthorized individuals could impersonate legitimate customers, leading to breaches of confidentiality and operational disruptions. When Lnett and a customer communicates for the first time, a token is exchanged and remains valid as long as the customer remains active. However, uncertainty exists regarding token storage practices, including whether Lnett’s tokens are unique to each customer or remain static. It is assumed that the risk of an unauthorized individual impersonating Lnett is higher than impersonating an individual customer.

R10: Intentional or unintentional attacks via API signals. The likelihood of this risk is *unlikely*, provided the API content is adequately validated [12]. If the API content is exploited to perform attacks, the consequences could be *moderate*, due to the potential for system compromise. Input validation of JavaScript Object Notation (JSON) objects received by Lnett’s API server is currently in place, helping to mitigate this risk.

B. Stakeholder Feedback

Stakeholders (Lnett and Avinor) viewed our method positively, noting that it resembled existing approaches but introduced new perspectives to cybersecurity risks they had not previously identified during the smart grid planning. They appreciated the iterative process, which allowed for multiple rounds of reflection. Compared to previous internal assess-

ments, the structured framework and documentation stood out as beneficial to serve as input to broader risk assessments.

The risk assessment process yielded new insights that might not have emerged otherwise. The stakeholders noted a higher number of unacceptable risks than anticipated (see Fig. 2). Additionally, they acknowledged that certain aspects of the planned solution (see Fig. 1) had not been thoroughly evaluated beforehand, leading to a greater awareness of potential vulnerabilities. Furthermore, they noted that the risk assessment process encouraged them to reflect on and reevaluate the cybersecurity and resilience of their planned solutions.

Some areas for improvement were highlighted, including the need to define the analysis object more clearly before starting the risk assessment. Participants noted that the context description had to be revisited and clarified during the meetings, which caused some delays. This issue may have stemmed from the uncertainties inherent in the smart grid planning phase.

The stakeholders emphasized the value of having outside perspectives, particularly from those experienced in risk assessment and management (i.e., the authors from SINTEF). According to the stakeholders, this external expertise helped identify risks and events that might otherwise have been overlooked. Additionally, conducting the risk assessment during the planning phase was an advantage, as it allowed for early adjustments based on the findings.

In terms of documentation, the approach was considered familiar and practical, aligning with existing practices for assessing likelihood and consequences of cybersecurity risks. However, the stakeholders noted challenges in tracking changes and maintaining logs. They suggested that adding features such as version history could enhance the ability to analyse risks retrospectively. Despite these limitations, the documentation style was regarded as suitable for ongoing use.

The resource use required for the process was acknowledged as significant by the stakeholders, suggesting room for optimization. Participants proposed involving fewer people in each session and consolidating findings afterward. However, they also recognized the benefit of having a diverse group, as less engaged participants in initial discussions often contributed valuable insights later in the process. This balance between inclusivity and efficiency was highlighted as a key consideration for future iterations.

The process was regarded as clear and easy to follow, with well-explained steps and effective presentations. The stakeholders expressed confidence in using the results, viewing the assessment as a solid foundation for addressing cyber risks related to electricity flexibility in future smart grids. They found the results useful for tracking past cybersecurity decisions, especially where previous assessments lacked documentation. Overall, the method was described as efficient and thorough given its lightweight approach, with a preference for longer, focused meetings over shorter sessions. Maintaining a historical record of the analysis was considered to be important, though participants acknowledged the challenges of re-engaging with the risk assessment material after time had passed.

TABLE IV
IDENTIFIED CYBERSECURITY RISKS (R). L = LIKELIHOOD. C = CONSEQUENCE. RL = RISK LEVEL.

No.	How? What is the incident?	What assets does it harm?	What is the risk level?
R1	An attacker intercepts and potentially alters communication between Lnett and Avinor via Man-in-the-Middle (MitM) attack.	Integrity of OpenADR signals. Confidentiality of communication. Security of internal systems.	L: Unlikely. C: Major. RL: High.
R2	An attacker orchestrates a Distributed Denial of Service (DDoS) attack to overwhelm Lnett’s servers with traffic, causing a denial-of-service event.	Availability of communication infrastructure. Security of internal systems.	L: Likely. C: Major. RL: High.
R3	Connecting the SCADA system to the network or Lnett’s server introduces vulnerabilities that attackers could exploit to compromise the SCADA system.	Integrity of SCADA data. Security of internal systems (e.g., SCADA, Supervisory Control System).	L: Possible. C: Major. RL: High.
R4	As Lnett scales its service to accommodate more customers, the attack surface expands, potentially introducing new vulnerabilities.	Integrity and confidentiality of communication. Availability of communication infrastructure. Security of internal systems.	L: Possible. C: Moderate. RL: Medium.
R5	An attacker gains unauthorized access to Lnett’s API server, potentially altering or stopping OpenADR signals, leading to disruptions.	Integrity of OpenADR signals. Confidentiality of communication. Availability of communication infrastructure.	L: Unlikely. C: Major. RL: High.
R6	An attacker manipulates transmitted signals, leading to incorrect actions by the demand-response service.	Integrity of OpenADR signals. Safety of personnel and customers.	L: Unlikely. C: Major. RL: High.
R7	Insider threat at IT infrastructure provider disrupts power consumption by sending malicious signals to customers.	Integrity of OpenADR signals. Security of internal systems. Trust in Lnett.	L: Unlikely. C: Major. RL: High.
R8	Updates or upgrades performed by IT infrastructure provider or tool provider cause system failures.	Availability of communication infrastructure. Operational continuity.	L: Likely. C: Moderate. RL: High.
R9	Tokens used for identification in API messages may be compromised, potentially allowing unauthorized individuals to impersonate legitimate customers.	Confidentiality of communication. Integrity of OpenADR signals.	L: Possible. C: Major. RL: High.
R10	Intentional or unintentional attacks via OpenADR API content (signals).	Integrity of OpenADR signals. Security of internal systems.	L: Unlikely. C: Moderate. RL: Low.

V. LESSONS LEARNED AND RECOMMENDATIONS

Lesson 1: Harden SCADA integration through network segmentation to reduce cybersecurity risks. One key finding is that integrating OpenADR signals into SCADA expands the attack surface, allowing attackers to laterally move from external IT systems to SCADA and exploit vulnerabilities (R3) [5]. To reduce the attack surface, network segmentation can be used to isolate the OpenADR signals from general IT networks [13]. This also helps protect against man-in-the-middle attacks (R1) and signal manipulation (R6), as attackers cannot move laterally from external interfaces into SCADA [13]. However, network segmentation introduces latency, potentially impacting the demand-response service’s real-time communication. Thus, balancing network segmentation with performance is important to maintaining an efficient OpenADR implementation.

Lesson 2: Strengthen credential and token management to prevent impersonation attacks. A major risk in OpenADR-based demand-response systems arises from compromised API tokens (R9) and manipulation of signals (R5). Strengthening credential and token management requires frequent token rotation, strong encryption [3], and secure storage (e.g., hardware security modules) [14] for all OpenADR authentication credentials and token exchanges. Relying only on HTTPS for encryption is insufficient, as token compromise is still possible

even if HTTPS is implemented [8], [12]. The most severe case occurs if an attacker obtains the token of a Distribution System Operator (DSO), such as Lnett, allowing them to impersonate the DSO and send false OpenADR signals to its customers.

Lesson 3: Adopt a balanced approach to logging and monitoring by clearly defining stakeholder responsibilities. Several high-impact risks, e.g., man-in-the-middle (R1) and signal manipulation (R6), unauthorized access (R5) and insider threats (R7), and compromised tokens (R9) and attacks via API signals (R10) are detectable early via comprehensive logging, log analysis, and monitoring [15]–[17]. This requires collecting and analysing logs from OpenADR servers, SCADA connections, and endpoints of customer and third-party tool/IT-infrastructure providers for suspicious traffic patterns or anomalies (see Fig. 1). However, this not a task a DSO, such as Lnett, can handle alone, but it is rather a shared responsibility among all stakeholders. In our case, this includes Lnett, the IT-infrastructure provider, the tool provider, as well as Avinor (the customer). Thus, clearly defining shared responsibilities is critical to achieving a balanced and effective approach to logging and monitoring.

Lesson 4: Implement rolling or phased updates to minimize disruptions. Managing software updates in an OpenADR environment can be risk-prone (R8) if the entire system is taken offline or updated on a large scale. To mitigate such risks,

rolling or phased updates must be implemented to address the software update rollout problem as pointed out in R8. Effective strategies include prioritizing updates based on system sensitivity [11], dependency-aware scheduling to prevent cascading failures [18], and real-time monitoring and fallback mechanisms [19]. As in Lesson 3, this not a task a DSO can handle alone, but it rather requires shared responsibility among stakeholders. The tool provider and IT infrastructure provider have a special responsibility to make sure updates do not cause operational disruptions, as DSOs typically rely on third-party solutions for tools and IT infrastructure.

Lesson 5: Plan for DDoS resistance to protect demand-response continuity. OpenADR and similar demand-response implementations in smart grids depend on continuous system and network availability. Thus, Distributed Denial-of-Service (DDoS) attacks (R2) pose a major risk because targeted DDoS attacks on OpenADR servers (see Fig. 1) or other infrastructure that OpenADR depends on can disrupt energy load balancing and degrade grid resilience. As shown in Fig. 2, the risk R2 is ranked as the most critical risk given its likelihood (*Likely*) and consequence (*Major*) values compared to other identified risks in the case study. This ranking reflects the fact that DDoS attacks are common, have severe disruptive consequences, and are relatively easy to execute [2]. To mitigate DDoS attacks, it is essential to plan for DDoS resistance by implementing multi-layered DDoS protections, such as cloud-based scrubbing [20], rate-limiting and redundant communication paths [21].

Lesson 6: Establish a scalable onboarding process for new customers to limit attack surface growth. As more customers connect to a demand-response system, the attack surface expands due to the increasing number of endpoints (R4). To mitigate potential vulnerabilities at an early stage that may arise from the expanded attack surface, it is important to develop and implement consistent onboarding procedures for each new customer [14]. These procedures help enforce baseline security measures, e.g., correct firewall configurations and secure token exchange (R9), and provide clear guidelines on securely handling OpenADR signals.

VI. RELATED WORK

State-of-the-art decision support for cybersecurity is primarily guided by risk management frameworks, most notably the ISO standards [22] and the NIST frameworks [23]. The traditional risk analysis approaches often assume that the nature and impact of the unwanted incidents are known, requiring detailed and specific descriptions of unwanted incidents and precise risk quantification.

We have in our earlier work [24], [25] developed customized approaches to cybersecurity risk assessment of smart grids. Given the early stages of the smart grid technologies and lack of their operational experience, those studies focused on vulnerabilities of the digitalized power grid, rather than quantified risks. However, as risk level estimation was one of our objectives in this study, the leveraged approach to risk assessment [4] enabled us to both estimate risks and also to

semi-qualitatively express the risk levels. In that manner, we were able to reflect the uncertainty of the estimates in the granularity of the likelihood and consequence scales applied.

In terms of risk assessment for smart grids, a variety of approaches exist. The main distinction between them is: quantitative approaches, approaches based on simulation or virtualization, and high-level approaches. For example, Markov decision process and Markov chains [26], as well as Bayesian networks [27] support calculation of quantitative risk severity levels. In contrast to our method, these approaches rely on quantitative and probabilistic inputs, which are typically not available during the smart grid planning phase.

An approach for migrating smart grid OT services to cloud computing architectures based on security risk assessment is proposed in [28], while [29] presents a method for assessing cybersecurity risks and vulnerabilities in smart grids with integrated solar photovoltaic. Both approaches share similarities with our work, particularly in their use of high-level graphical diagrams to describe the target of analysis. However, unlike [28] and [29], which assess likelihoods solely through qualitative descriptions, our approach use frequency intervals in addition to qualitative likelihood assessments. While these methods align with ours to some extent, they fundamentally differ in their application domains and specific focus areas.

None of the related approaches mentioned above are tailored to the smart grid planning phase. In contrast, our method is specifically designed to assist grid planners in assessing cybersecurity risks early in the planning process [4].

Several studies have explored potential cybersecurity risks associated with the OpenADR protocol and its implementation, with discussions dating back to 2012 [30]. However, research on industrial applications, such as in our case study, remains limited. To the best of our knowledge, only one other study is closely related to ours: [31] investigates OpenADR's role as an open, secure, two-way communication protocol facilitating information exchange between electric vehicles (EVs) and the electricity grid. It highlights OpenADR's significance, together with other similar protocols, in balancing grid supply and demand while addressing cybersecurity concerns in the context of EV charging infrastructure. This study and ours are complementary, as both assess cybersecurity risks in OpenADR-enabled systems but in different domains. While [31] focuses on EV charging, our study examines OpenADR's cybersecurity risks in a DSO-airport operator setting, where demand-response signals affect critical infrastructure.

VII. CONCLUSION

We conducted a cybersecurity risk assessment case study during the smart grid planning phase for Lnett, a DSO in Southern Norway, as they planned to integrate OpenADR to enable electricity flexibility for their customers. Assessing cybersecurity risks during grid planning is challenging due to its early, conceptual nature, making lightweight, qualitative risk assessment methods more suitable than traditional quantitative approaches. To address this, we applied our previously developed six-step cybersecurity risk assessment method [4].

The case study aimed to: (1) identify cybersecurity risks related to OpenADR integration, (2) assess the feasibility of our risk assessment method, and (3) derive lessons learned and practical recommendations for DSOs and practitioners implementing OpenADR or similar demand-response protocols in contexts similar to our study.

We identified 10 key cybersecurity risks related to OpenADR integration in the case study provided by Lnett. Stakeholder feedback was positive, highlighting the value of the structured method, iterative process, and external expertise. The assessment revealed more unacceptable risks than expected, encouraging stakeholders to reflect on and reevaluate the cybersecurity and resilience of their planned solutions. Challenges included defining the analysis object clearly and improving documentation tracking.

Finally, we derived six key lessons for OpenADR implementation, emphasizing SCADA integration through network segmentation, credential and token management, logging and monitoring, phased updates, DDoS resistance, and scalable onboarding of new customers. Our findings contribute to strengthening cybersecurity resilience in demand-response systems and smart grid planning.

ACKNOWLEDGMENT

This work is supported by the projects CINELDI (RCN 257626/E20), NEMECYS (EU 101094323), and the SINTEF GUARDIAN project (RCN basic funding).

REFERENCES

- [1] S. Banik, T. Banik, S. M. M. Hossain, and S. K. Saha, "Implementing Man-in-the-Middle Attack to Investigate Network Vulnerabilities in Smart Grid Test-bed," in *2023 IEEE World AI IoT Congress (AlloT)*, 2023, pp. 0345–0351.
- [2] I. Ortega-Fernandez and F. Liberati, "A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning," *Energies*, vol. 16, no. 2, 2023.
- [3] OpenADR, "OpenADR In a Nutshell," OpenADR Alliance, Summary, 2022. [Online]. Available: https://www.openadr.org/assets/ADR_InNutshell_1-2022a.pdf
- [4] G. Erdogan, T. A. Zerihun, I. B. Sperstad, and O. Gjerde, "A Light-Weight Tool-Supported Method for Cyber Risk Assessment in the Planning of Cyber-Physical Smart Grids," in *2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2024, pp. 314–320.
- [5] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100433, 2021.
- [6] A. Zibaeirad, F. Koleini, S. Bi, T. Hou, and T. Wang, "A comprehensive survey on the security of smart grid: Challenges, mitigations, and future research opportunities," *arXiv preprint arXiv:2407.07966*, 2024.
- [7] S. Acharya, Y. Dvorkin, and R. Karri, "Causative Cyberattacks on Online Learning-Based Automated Demand Response Systems," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3548–3559, 2021.
- [8] F. Wilkens, S. Haas, J. Amann, and M. Fischer, "Passive, Transparent, and Selective TLS Decryption for Network Security Monitoring," in *ICT Systems Security and Privacy Protection*. Springer, 2022, pp. 87–105.
- [9] O. Eigner, H. Schölnast, and P. Tavalato, "How to find out what's going on in encrypted smart meter networks - without decrypting anything," in *Proc. 19th International Conference on Availability, Reliability and Security (ARES)*, 2024, pp. 1–6.
- [10] M. N. Al-Mhiquani, T. Alsbou, T. Al-Shehari, K. H. Abdulkareem, R. Ahmad, and M. A. Mohammed, "Insider threat detection in cyber-physical systems: a systematic literature review," *Computers and Electrical Engineering*, vol. 119, p. 109489, 2024.
- [11] K. C. Sou and H. Sandberg, "Resilient Scheduling of Control Software Updates in Radial Power Distribution Systems," *IEEE Transactions on Control of Network Systems*, vol. 11, no. 3, pp. 1465–1477, 2024.
- [12] P. Gowda and A. Gowda, "Best Practices in REST API Design for Enhanced Scalability and Security," *Journal of Artificial Intelligence, Machine Learning and Data Science*, vol. 2, no. 1, pp. 827–830, 2024.
- [13] E. Wai and C. K. M. Lee, "Depth in defense: A multi-layered approach to cybersecurity for scada systems in industry 4.0," *Science and Technology - Recent Updates and Future Prospects Vol. 2*, p. 124–144, 2024.
- [14] OpenADR, "OpenADR Alliance Certificate Policy, OpenADR-CP-I02-211103," OpenADR Alliance, Policy, 2021. [Online]. Available: https://www.openadr.org/assets/OpenADR-CP-I02-211103_2021.pdf
- [15] H. M. Koth, T. Gaber, S. AlJanah, H. M. Zawbaa, and M. Alkhatami, "A novel deep synthesis-based insider intrusion detection (DS-IID) model for malicious insiders and AI-generated threats," *Scientific Reports*, vol. 15, no. 1, p. 207, 2025.
- [16] Z. Wei, U. Rauf, and F. Mohsen, "E-Watcher: insider threat monitoring and detection for enhanced security," *Annals of Telecommunications*, vol. 79, pp. 819–831, 2024.
- [17] U. O. Obonna, F. K. Opara, C. C. Mbaocha, J.-K. C. Obichere, I. O. Akwukwaegbu, M. M. Amaefule, and C. I. Nwakanma, "Detection of Man-in-the-Middle (MitM) Cyber-Attacks in Oil and Gas Process Control Networks Using Machine Learning Algorithms," *Future Internet*, vol. 15, no. 8, p. 280, 2023.
- [18] J. Liu and H. Shen, "Dependency-Aware and Resource-Efficient Scheduling for Heterogeneous Jobs in Clouds," in *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2016, pp. 110–117.
- [19] P. Krishnamurthy, A. Rasteh, R. Karri, and F. Khorrani, "Tracking Real-time Anomalies in Cyber-Physical Systems Through Dynamic Behavioral Analysis," 2024. [Online]. Available: <https://arxiv.org/abs/2406.12438>
- [20] D. M. A. A. Afraji, J. Lloret, and L. Peñalver, "Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments," *Cyber Security and Applications*, vol. 3, p. 100085, 2025.
- [21] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, "A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid," *IEEE Access*, vol. 8, pp. 177 447–177 470, 2020.
- [22] ISO, "ISO/IEC 27005:2018 - Information technology - Security techniques - Information security risk management," ISO, Standard, 2018.
- [23] NIST, "SP 800-30 - Guide for Conducting Risk Assessments," NIST, Standard, 2012.
- [24] A. Omerovic, H. Vefsnmo, G. Erdogan, O. Gjerde, E. Gramme, and S. Simonsen, "A Feasibility Study of a Method for Identification and Modelling of Cybersecurity Risks in the Context of Smart Power Grids," in *Proc. 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS)*. SciTePress, 2019, pp. 39–51.
- [25] A. Omerovic, H. Vefsnmo, O. Gjerde, S. T. Ravndal, and A. Kvinnesland, "An Industrial Trial of an Approach to Identification and Modelling of Cybersecurity Risks in the Context of Digital Secondary Substations," in *Proc. 14th International Conference on Risks and Security of Internet and Systems (CRISIS)*. Springer, 2020, pp. 17–33.
- [26] A. Bashar, S. Muhammad, N. Mohammad, and M. Khan, "Modeling and Analysis of MDP-based Security Risk Assessment System for Smart Grids," in *Proc. 4th International Conference on Inventive Systems and Control (ICISC)*, 2020, pp. 25–30.
- [27] A. AlMajali, Y. Wadhawan, M. S. Saadeh, L. Shalalfeh, and C. Neuman, "Risk assessment of smart grids under cyber-physical attacks using Bayesian networks," *International Journal of Electronic Security and Digital Forensics*, vol. 12, no. 4, pp. 357–385, 2020.
- [28] B. Jelacic, I. Lendak, S. Stoja, M. Stanojevic, and D. Rosic, "Security risk assessment-based cloud migration methodology for smart grid OT services," *Acta Polytech. Hung.*, vol. 17, no. 5, pp. 113–134, 2020.
- [29] F. A. Rahim, N. A. Ahmad, P. Magalingam, N. Jamil, Z. C. Cob, and L. Salahudin, "Cybersecurity Vulnerabilities in Smart Grids with Solar Photovoltaic: A Threat Modelling and Risk Assessment Approach," *International Journal of Sustainable Construction Engineering and Technology*, vol. 14, no. 3, pp. 210–220, 2023.
- [30] G. Ghatikar, E. L. Koch, and J. Boch, "OpenADR Advances," *ASHRAE Journal*, vol. 54, no. 11, p. B16, 2012.
- [31] I. Skarga-Bandurova, I. Kotsiuba, and T. Biloborodova, "Cyber Security of Electric Vehicle Charging Infrastructure: Open Issues and Recommendations," in *2022 IEEE International Conference on Big Data (Big Data)*, 2022, pp. 3099–3106.