Security Architecture for Distribution System Operators: A Norwegian Perspective

Vahiny Gnanasekaran and Martin Gilje Jaatun

SINTEF Digital, Trondheim, Norway
{vahiny.gnanasekaran, martin.g.jaatun}@sintef.no

Abstract. Power distribution is becoming increasingly vulnerable to external cyber threats due to the interconnectivity between the OT and IT systems at the Distribution System Operator's (DSO) premises. Security architectures provide a system overview and simplify the implementation of security measures. However, few works explain the development and design of such a security architecture for the DSO. This paper proposes a future-oriented security architecture for Norwegian DSOs, based on interviews and meetings with the industry, existing security standards, and smart grid guidelines by applying a design science approach. The architecture includes national systems, (e.g., Elhub), and near-future smart grid developments (e.g., Advanced Distribution Management Systems). The architecture signifies the need to consider implications of the DSO's future digital developments, responsibilities, and functionalities in other countries. Future research should investigate the people and processes related to DSO premises to complement the technology perspective.

Keywords: Smart Grid · Security Architecture · Cybersecurity · Critical Infrastructure

1 Introduction

The concept of a Smart Grid emerged around the turn of the century [18], with "smartness" seemingly transitioning slowly from the transmission side to the distribution side of the grid, and reaching the attention of the general public with the deployment of smart electricity meters in private homes. As has become clear in later years, "if it's smart, it's vulnerable" [11], highlighting the need for a smart grid security reference architecture.

Such an architecture presents a broader system understanding by highlighting challenges with possible solutions [1]. At the same time, such solutions should adapt to the system and external changes. Conversely, the security architecture is expected to provide *a detailed description of all aspects of the system that relate to cyber security, along with a set of principles to guide the design.* [4]. Hence, the objective is to organize technical security elements to ensure the robustness of the DSO's system functions regardless of cyber attacks.

This paper presents a security architecture based on previous work [7,17,27], major smart grid security architectures, such as NISTIR 7628 [24], the IEC

62443[1] standards series [12], and interviews and meetings with the industry, perceived from a Norwegian perspective. First, a high-level architecture demonstrates how the DSO's control room and interacting systems from other domains (such as secondary substations; Transmission System Operator (TSO) facilities; consumer premises; and service providers) are connected. Second, a high-level threat assessment is conducted using the MITRE ATT&CK ICS framework[2], where the relevant mitigation strategies are applied to the architecture. The result is a security architecture adapted to a typical Norwegian DSO control center. It does not consider random failures and faults occurring besides cyber attacks (e.g., accidental malfunction, weather), only those originating from a cyber attack. The paper's objective is to (1) provide a security architecture addressing the Norwegian DSO control center with future developments, and (2) present implications of future smart grid developments for the Norwegian DSOs.

Norwegian smart grids are highly digitalized, with a complete rollout of smart meters, all connected to a centralized data hub for metering values [6]. The increased digitalization results in effective smart grid usage and an extended attack surface. A security architecture for the Norwegian DSO can also be applied in future European counterparts. Future modifications of the smart distribution grid, including the Advanced Distribution Management System (ADMS), and integration of the Advanced Metering Infrastructure head-end system (AMI HES) as a third-party cloud service and distribution grid sensors, are considered. The architecture targets OT security employees in DSOs and researchers within cybersecurity in critical infrastructure.

2 Background and Related Work

This section introduces smart grid security architectures, use cases, and relevant standards. In addition, we briefly present some of the pressing tasks and responsibilities the Norwegian DSO might face soon, based on the current technological advancements observed in the industry and research.

2.1 Smart Grid Reference Architecture Models

The literature suggests different development approaches of a smart grid architecture [8,17,20,21,24]. The major smart grid architectures, NISTIR 7628 [24] and the European Smart Grid Architecture Model (SGAM) [21] were created in the 2010s. NISTIR 7628 consists of three volumes. The first explains a risk assessment process and introduces a logical reference architecture. The logical reference architecture includes *logical interfaces* classified into *logical interface categories*, depicting logical connections between the different actors. Each logical interface category contains several high-level security requirements based on the CIA triad. The authors identified 48 actors/systems within one of the

[1] IEC 62443 represents the most important standardization effort on security in Industrial Control Systems, and is thus relevant for smart grid security.

[2] `https://attack.mitre.org/`

22 logical interface categories across seven smart grid domains: transmission, generation, markets, distribution, service providers, operations, and customers.

While NISTIR 7628 focuses mainly on mapping the logical devices in the smart grid into a logical reference architecture, the SGAM [21] separates the business processes and systems into five different interoperability layers (i.e., business, function, information, communication, and component layer), domains, and zones, creating a broad view on smart grid operations. The reference architecture was created by the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) to develop a standard for European standardization organizations to conceive smart grid architectures within all layers. Information security is not assigned a separate layer in the model, since it is argued to be a property of each layer and domain. SG-CG continued its work within information security and outlined relevant industry standards for each layer and domain [23].

Several papers [5,8,17] follow the SGAM architecture model. Foros [8] presents a generic, and simplified description of a smart distribution grid to conduct a cyber-risk analysis. Langer et al. [17] present an approach used to map the Austrian reference security architecture and develop a conceptual and implementation-based risk analysis of the proposed architecture. The conceptual risk analysis consists of four steps:

1. Developing a reference architecture.
2. Mapping the relevant security threats, resulting in a threat matrix for the DSO.
3. Performing a security risk assessment and populating a risk matrix.
4. The risk assessment provides input regarding the relevant security measures that need to be implemented by the DSO.

However, the work does not include recent technological advancements in the smart grid (e.g., ADMS) and state-of-the-art frameworks (e.g., IEC 62443, MITRE ATT&CK), since it is from 2016. Although NISTIR 7628 is widely used in American governmental reports and documents, few academic papers adopt it. Griffin et al. [9] attribute the lack of use to the absence of a systematic approach for smart grid actors. In addition, the framework possesses too few identification and response strategies for cyber attacks. NISTIR 7628 is an internal report and considered guidelines for the smart grid, thus not possessing the same level of authority as the Federal Information Processing Standards (FIPS). SGAM, on the other hand, provides a framework to compare and examine different implementations at different levels. Since the scope of this paper only considers the DSO's industrial and enterprise systems, it is not necessary at this stage to consider all levels, but sufficient to provide an overview. NISTIR 7628 and SGAM have become outdated since they have neither included smart grid developments from the past decade nor future ones. The two guidelines are based on American and European power grids, respectively. Geographical differences in the power grids reduce the transferability to the Norwegian power grid.

2.2 IEC 62443 Standard

The IEC 62443 standards series [12] is the OT complement of the ISO/IEC 27000 series [13]. It provides more state-of-the-art security measures than the two guidelines, but the NISTIR 7628 and SGAM are specific to the smart grid. The standard considers a scope (System under Consideration (SuC)) with an initial security assessment, and placing *Zones and conduits* as a part of the network segmentation. Zones represent a collection of systems in the industrial context that possess the same security requirements, while conduits protect the communication links between the zones [12]. The security requirements are linked towards a Security Level (SL), stating the need for countermeasures in the respective zones and conduits. Some requirements are already established [14]:

- Separate the IT and OT systems.
- Separate Safety Instrumented Systems (SIS) from other OT systems.
- Place temporary connected systems (e.g., field devices) into one zone.
- Wireless communication should be separated from wired communication.

Kern et al. [14] introduce data flows for the SL classification in the zones and conduits in architecture by segmenting the system into a logical functional, security, and network layer. The SuC is derived from the logical functional layer, defining the data flows. After determining the SL from the initial security assessment, the data flows are used to decide the SL for the components in the network layer. The highest SL specifies the target SL for the zone.

2.3 Tasks and Responsibilities of a Norwegian DSO

The remaining section provides input on the latest smart grid developments for the Norwegian DSOs using the existing literature. Currently, the tasks and responsibilities of a Norwegian DSO are twofold. First, they are responsible for sufficient grid coverage and capacity for all customers. Second, they facilitate the customer's energy consumption or production in their grid, provided they pay for it [3]. Significant changes to fundamental components in the Norwegian grid (and elsewhere) have occurred in recent years. Traditionally, fewer monitoring and measuring units on the lower voltage grids (11kV-22kV) have been the case. The most used system for measurement is the Advanced Metering Infrastructure (AMI), where smart meters are installed in all customer households and most secondary substations. However, this is changing, and multiple monitoring solutions are offered for the lower voltage power grid (e.g., IoT sensors).

Centralized control systems in the power distribution grid are being integrated into the Advanced Distribution Management System (ADMS). Such integrations are already present in some European countries, but Norwegian regulations keep them separated to prevent misuse or accidental changes to the breaker functions. Nonetheless, changes are emerging in the Norwegian DSO market. Some solutions already offer an Energy Management System (EMS) and an Outage Management System (OMS) as a part of the DMS. The system

provides a seamless transition between situation awareness by observing the potential capacity changes in traditional DMS and transmitting the control signals to SCADA and AMI, all in one system. Such an integrated system is exposed to potential unwanted access, and exploitation of security vulnerabilities [2], and requires more attention from the DSOs to ensure secure grid operation.

Operating the smart grid demands interaction and collaboration between the TSO and all DSOs for maintenance, planning, and data management. However, many system services are deemed to change in the future. The imbalance settlement in the Nordic countries is changing from 60 to 15-minute intervals, suggesting that DSOs should adjust their measurements to meet the upcoming requirements [25]. In addition, energy production is increasingly generated from renewable, Distributed Energy Resources (DER). This demands greater frequency and voltage control over larger areas [19,20], increasing the need for improved communication between DSO and TSO to manage capacity issues in the grid. It is further expected of the DSO to manage some of the TSO's tasks and responsibilities [3], which also requires increased collaboration between TSO and DSO on systems facilitating the interaction.

Digital Twins (DT) is referenced in the literature [16] as a promising solution to monitor all nodes in the DSO's power grid. DT is a digital representation enabling dynamically updating the representation based on the incoming data [29]. The combination of weather data, load indications on different paths, and the power grid usage predictions in the short-term future results in a highly accurate DSO power grid model. Previous work [28] discusses the distinct degrees of automation enabled by DT. However, the regulations from the Norwegian Water Resources and Energy Directorate of the SCADA and ADMS might still be in effect, making automated decisions unavailable.

An increasing use of distributed, wireless sensors by the DSOs is predicted in the years to come. These sensors can be expected to be located inside substations or secondary substations, and outdoors (e.g., attached to power lines). The vendors are expected to maintain such sensors, i.e., issuing software updates where appropriate. This requires DSOs to pay attention to the cyber security procedures of the vendor's products and in turn to their vendor's supply chains. In some cases, vendors themselves are expected to operate the infrastructure needed to provide the data. Regardless, it will be challenging for the DSO to verify the security of third-party infrastructure providing sensor data. At the same time, this data could in many cases measure physical quantities in the DSO's grid. DSOs are therefore likely to increasingly grow accustomed to basing their operational decisions on third-party provided data.

The DSOs' ability to ensure sufficient security controls is also predicted to be a potential issue. The DSO might have to devote more resources to implementing and maintaining these security controls, in addition to all their other responsibilities [27]. A report [15] reflecting on potential far-future scenarios in the Norwegian smart grid development predicts a heavy investment in security competence and measures to ensure power availability in the next 20 years. All components will be available from the control room, so updates and patches

may be deployed directly from the center. However, it is suggested that grey areas within the systems interacting between the transmission and distribution network might be vulnerable to potential Man-in-the-Middle (MITM) attacks, affecting the data integrity between the TSO and DSOs. The increasing digitalization of the grid and the novel solutions stress the need to prepare for potential state-actor cyber attacks that could collapse parts of the energy supply.

3 Designing the Security Architecture

The security architecture provided in Section 4 is developed based on design science research. Design science was selected as the preferred method, considering the security architecture as an artifact for securing the future distribution grid. In addition, the research was based on the future, Norwegian smart grid functionalities, where the literature is rather limited. The study followed the design science approach described by Hevner et al. [10] (see Fig. 1).

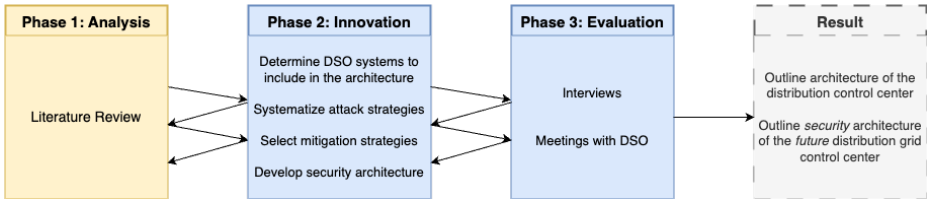

Fig. 1. The design science approach with three phases [10], adapted from [26].

The first architectural designs were developed based on a theoretical view of the security architecture, adapted from the first volume of NISTIR 7628 [24], and SGAM [21]. Since the framework only considered the American electric power system, it needed adaptation to the Norwegian power grid. For instance, there is only one Independent System Operator (ISO)/Regional Transmission Organization (RTO), which is also the only Norwegian transmission system operator (TSO). The retail energy market was excluded since the control room has limited interaction with the energy market.

The SINTEF report [8] served as a guideline to understand the Norwegian DSO's scope and current tasks. The data connections between the Norwegian centralized IT solution to store energy consumption and customer production data, *Elhub* [6], and AMI HES were included. Elhub is responsible for the storage, calculation, and availability of accurate meter data. Retail service providers, and aggregators that calculate the electricity bill retrieve data from the hub. Norwegian DSOs only need to consider the connection to the centralized solution for transmitting and receiving meter data for billing.

Interviews with four relevant experts were conducted to provide feedback and validation of the architecture, with subsequent adaptation to their comments.

The discussions lasted approx. one hour via video conference. The sample was characterized by knowledge of certain areas or smart grid actors; one vendor representative, one DSO representative, one TSO representative, and one power grid researcher were included. In addition, two meetings with a Norwegian DSO were also conducted to compare their existing control center architecture and discuss their planned updates. Based on the comments, the security architecture was improved, with another round of validation later.

The empirical data gave insights into how the DSO systems were currently placed in the control center. This stage was critical for identifying the security elements. The zones and conduits concepts from IEC 62443 were leveraged to identify security zones and conduits to partition the sub-systems into different Security Levels (SL). The System Under Consideration (SuC) is the marked area in Figure 3, addressing the control center. All systems placed into a security zone are expected to comply with the same requirements the targeted SL prescribes. Identifying zones and conduits requires performing an initial security risk assessment of the smart distribution center, including threats, consequences, and likelihood, thereby providing a risk matrix to verify the selection of zones.

Since some functionalities are unavailable, only a high-level risk assessment of the future distribution control center is possible. Therefore, the focus is on the *data flow* between the potential zones. Data flow in this context means sent and received information. For instance, DSO SCADA receives control signals from TSO SCADA, sensor data, and breaker status from AMI HES, DER, secondary substation, switching schedules from ADMS and sends control signals to AMI HES, secondary substation, and DER, and other values to TSO SCADA.

The threats are based on the MITRE ATT&CKs ICS framework[2]. The framework was leveraged to verify the architecture. The techniques and mitigation strategies were selected based on pre-defined inclusion and exclusion criteria (see Table 1). 92 techniques were present on the webpage (per March 2024). After a calibration session, two researchers sorted the techniques from low, medium, and high relevance using the criteria. Of 81 relevant techniques, 26 were regarded as high, and 21 as medium relevance. The associated mitigation strategies resulted in 101 highly relevant, and 97 medium relevant strategies. Fig. 2 displays the most frequent mitigation strategies. Table 2 summarizes the techniques and mitigation strategies.

Table 1. Inclusion and exclusion criteria for selecting relevant mitigation strategies.

Inclusion criteria	**Exclusion criteria**
Network topology	Social engineering attacks
Primary asset location (in the architecture)	User privileges at the endpoint level.
Configuration of API that affects the architecture	Endpoint protection and correct configuration.
Configuration of security elements	
Remote control	
Data historian location	

Table 2. Summary of the MITRE techniques and the associated mitigation strategies.

Selected MITRE techniques	**Associated MITRE mitigation strategies**
Blocking communication or messages.	Network filtering, and segmentation.
Network sniffing, monitoring, collecting information, MITM-attack.	Network allow/denylists, and configuring static connections.
Denial of view, service, or control of the DSO systems.	Include network security elements (e.g., firewalls, Network IDS, etc.)
Remote service misuse.	Out-of-Band Communications Channel.
Spoofing malicious network traffic using standard ports and protocols.	Redundancy of service, network, security elements, and data backup for quick restoration.
Modification and suppression of alarm settings.	Access and user account management on the network level.
Device restart/shutdown by manipulating system functions. Modification and/or deletion of critical data.	Authenticating critical connections, devices, and messages. Encryption on network level.

4 The Security Architecture

This section presents the proposed security architecture. First, the broader smart grid architecture of the Norwegian power grid, with a focus on the distribution control center (Fig. 3) is presented. This architecture is based on interviews, meetings with a Norwegian DSO, NISTIR 7628's logical reference architecture, and SGAM. It is simplified by excluding security systems, and maintenance servers. Subsequently, the selection of high-level threats and mitigation strategies from MITRE ATT&CK ICS[2] is analyzed within SuC: the distribution control center with its out- and inbound connections. Table 3 provides more details on the most relevant subsystems involved in the security architecture.

Table 3: List of power grid subsystems applied in the architecture.

System	**Subsystem**	**Description**
DSO enterprise layer	AMI HES	Collect all measurement data from Advanced Metering System (AMS) meters.
	Work Management System (WMS)	Schedules the workers and tools to plan grid maintenance or extensions.
	Customer Information System (CIS)	Applications allowing utility companies to manage customer relationships.
	Network Information System (NIS)	Provides information about network assets and the overall grid condition.

DSO operation layer	ADMS	Traditional Distribution Management System support real-time grid monitoring and control, but the advanced version contains EMS and OMS functionalities.
	DSO Supervisory Control and Data Acquisition (SCADA)	Collection of tools contributing to DSO grid control and data accumulation.
	Demand-Response Management System (DRMS)	Predicting flexibility needs, and requests users to adjust consumption/production.
Primary and secondary substation	Remote Terminal Units (RTUs)	Obtain grid sensor data and apply SCADA control commands to measure e.g., voltage.
	Merging Unit (MU)	Transmit measurement and control data to the control systems.
Distribution grid	Grid Sensors	Measures temperature, voltage, and other grid parameters.
Consumer Premises	AMI	Measures the energy consumption from each household.
	Data concentrator	Collects smart meter data from several households and transfers to AMI HES.

The proposed zones are depicted in Fig. 4 with the target SL from the initial threat assessment. Conduits are established between the communication channels in different zones and are assigned the maximum value between those zones. One such conduit is exemplified in the security architecture. Since the conduit starts and ends in a zone with target SL-4, the conduit should satisfy the same target SL. The complete security architecture with mitigation strategies is shown in Fig. 5. Some assumptions are present to define the scope of the smart grid security architecture:

- Since the architecture scope is the DSO's control room, all systems are directly connected to the control center.
- The smart meter system is simplified by only including the communication with the AMI HES. In addition, only one AMI is shown in Fig. 3.
- DMS, EMS, and OMS are all assumed to be a part of the future ADMS.
- For simplicity, field devices are not included in the architecture.
- Even though distributed energy resources are emerging (e.g., prosumers), microgrids enabling "Island mode" are not included in the architecture's scope [8].
- AMI HES is located at the DSO enterprise network, in contrast to the traditional location within the control room, due to the assumption of AMI becoming a third-party service.

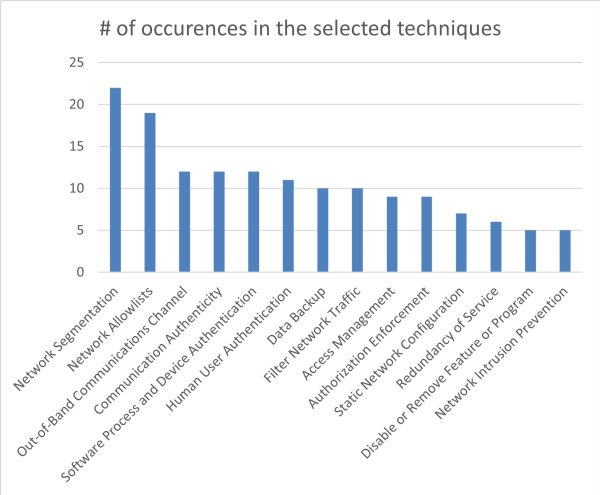

Fig. 2. Most frequently selected MITRE mitigation strategies from the high and medium relevant techniques.

- DSO applies grid sensors and sensors at the substation level to provide information on e.g., temperature, voltage, wind speeds, and frequency.
- Data Historians are simplified in the security architecture, but they are applied to store AMI and sensor data (both on-grid and substation level).
- To the best of our understanding, the DT will have a similar placement as the ADMS and is therefore excluded from the architecture.
- Network Intrusion Prevention Systems (NIPS) and Network Intrusion Detection Systems (NIDS), previously based on pure IT networks, are assumed to be available for industrial networks in the coming years.

Based on the input from MITRE ATT&CK, the identified mitigation strategies were applied to the architecture (e.g., network segmentation, redundancy of service). The control center should have its own IAM to protect against compromise of the enterprise's IAM infrastructure. However, the majority of the mitigation strategies relate to network security elements configuration (e.g., host-based allow-lists, removing access to certain ports, denying specific application-layer protocols), and personnel, software, or device authentication (e.g., Message Authentication Codes, signatures, Multi-Factor Authentication (MFA)). Although the architectural design is provided, it is a prerequisite to configure and maintain network security elements and access management infrastructure, ensuring continuous security protection. Further, incident response (IR) plans should include alternative communication paths (e.g., using pre-defined mailing lists, mobile phones, etc.). Nonetheless, mitigation strategies for configuration, maintenance, and IR plans are not covered in this paper.

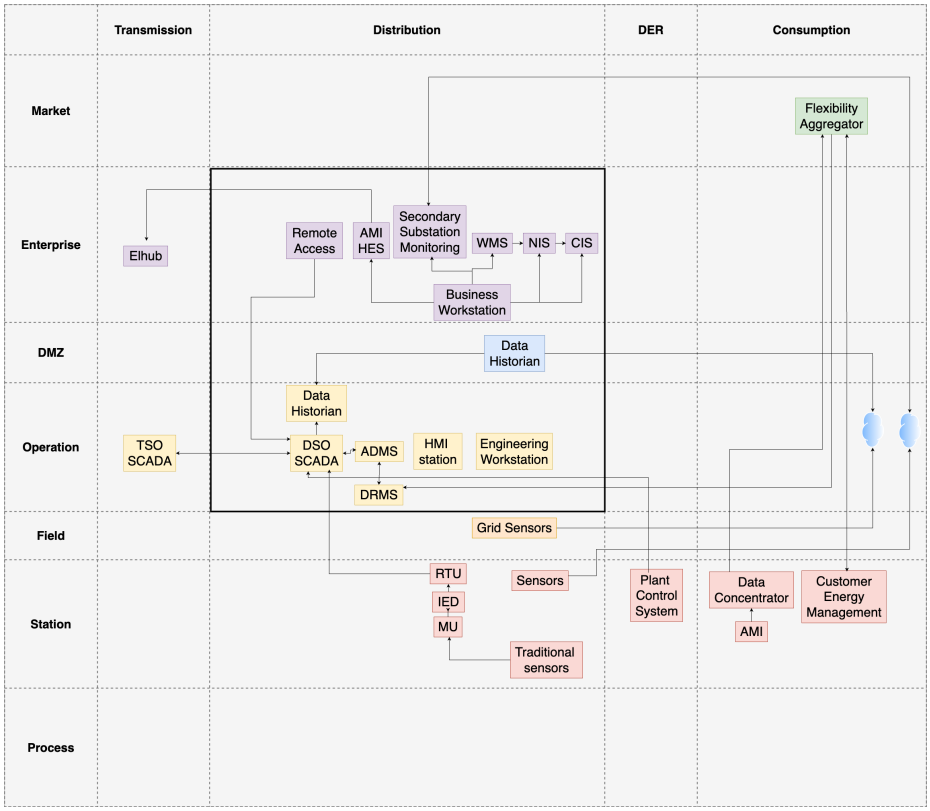

Fig. 3. The proposed smart grid architecture perceived from the Norwegian distribution control center.

5 Implications of Future Smart Grid Developments

The security architecture for the future DSO suggests one way to secure the robustness of the DSO system functions during a cyber attack. The design advantage is the adaptation to the future Norwegian DSOs' needs and developments. To mitigate the shortcomings of NISTIR 7628 and SGAM, IEC 62443 and previous work [8,17] are applied to provide state-of-the-art security measures to recent threat vectors. The architecture provides defense-in-depth while leveraging upcoming system changes at the control center. The disadvantage is the potential of deprecated functionalities or transition to more advanced technologies. Similar studies on current architectures include several smart grid actors (e.g., DER, TSOs, end customers) [17]. This research design contributes to other practitioners or researchers investigating relevant smart grid security controls.

MITRE ATT&CK ICS leverages publicly available threat intelligence and incident reporting, indicating that our threat assessment is mostly limited to historical data. It is not given that previous threats and attacks would occur again.

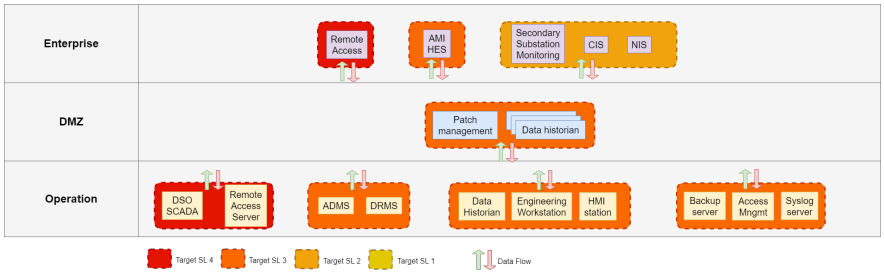

Fig. 4. The proposed zones and conduits on the security architecture.

Nonetheless, being protected against previous attacks may limit "low-hanging" techniques. The combination of patching and applying the current mitigation strategies may grant sufficient coverage. Future work should investigate specific attack scenarios addressed in the security architecture.

Security Levels: The majority of the zones in the architecture are placed within SL-2 and SL-3 (i.e., safeguarding against adversaries with low/moderate resources). The reasons for this are two-fold; economic factors and resources. The DSOs vary in size and security maturity level. For the smallest DSOs, it might be too unrealistic to pursue a target SL-4, which requires protection against advanced, organized actors, and thorough security monitoring. Although the DSOs benefit from using a Managed Security Service Provider (MSSP), they might not have the right competence, sufficient personnel, or economic power to follow up on e.g., false positives, Security Operation Centre (SOC) service, or Security Information and Event Management (SIEM).

The Role of the Cloud: During the discussions with industry representatives, it was suggested that cloud services are becoming available for the future smart grid. For instance, the HES system is already being delivered by some vendors as a third-party cloud service. If the system includes breaker functionality, the HES security will shift from the DSO to a third party. The implication of DSO entrusting another party to provide secure and accurate information while sharing access to the breakers indicates huge security concerns. Anyone with unauthorized access could misuse the breakers, and turn off the power for large communities through the cloud solution. Even if security controls are implemented, the security might become the cloud service provider's responsibility.

Another critical aspect is determining the DSO boundaries' sphere of influence. For instance, with cloud-based HES, the DSO needs to export HES data to their on-premises systems, and possibly to the control room. This implies that the HES data represents a potential path into more privileged systems, and security mechanisms to prevent abuse are necessary. The same case is relevant for the NIS and DT if they are based on generic available Geographic Information Systems (GIS) or publicly available weather services. The remaining question is the maintenance and security responsibility of such services; is it the cloud service or the DSO?

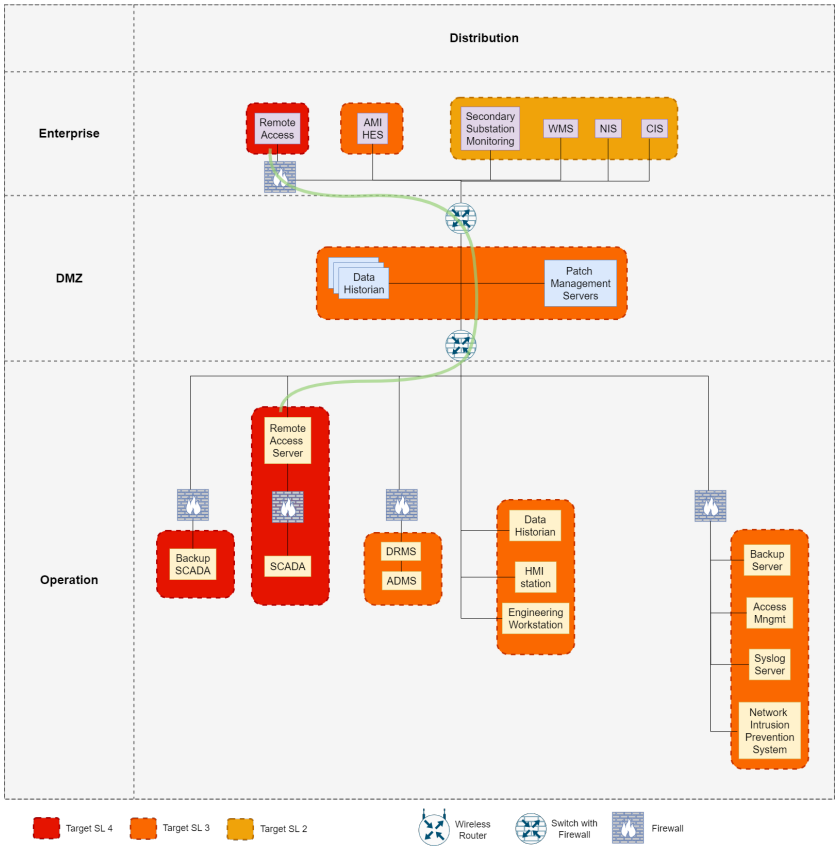

Fig. 5. The proposed security architecture for Norwegian DSOs, applying IEC 62443 zones and conduits.

IoT: Introducing IoT devices into the smart distribution grid has further implications. Several vendors will provide the entire digital value chain (e.g., from integration, data collection, and analysis) available in a cloud solution, not on-premises. The vendors expect to access the sensors and other components directly through the control room to retrieve the data and maintain the service. Such access could be misused by the vendor, and compromise the power availability. The industry representatives emphasized the concerns of enabling more automation. Hence, DSOs should be more wary of allowing third-party vendors direct access and can benefit from a proxy server between their components and the vendors. The balance between introducing additional latency to the operation, and possessing more control of the service is a tradeoff that could be favorable for the power grid.

Are Regulators Doing Enough? The Norwegian Energy Regulatory Authority expects Norwegian DSOs to take greater responsibility for their grid re-

garding all aspects of operation (maintenance, 24/7 control rooms, information sharing, etc.). This demands continuous grid monitoring, which is challenging to expect from small and middle-sized DSOs with economic and organizational restrictions [3]. They might need more automation and remote control, increasing the need for improved security controls. However, DSOs struggle to find the relevant competence and knowledge to secure such systems, making the control room more vulnerable. Due to the lack of knowledge, most DSOs require more support to meet the security requirements proposed by The Norwegian Water Resources and Energy Directorate. However, an audit report [22] revealed insufficient cybersecurity audits. DSOs' substations or control systems risk security exposure without properly regulating the implemented security controls.

Limitations: Although our study has been performed in the context of the Norwegian energy system, we believe that the resulting security architecture should be equally applicable in other European countries. The Norwegian smart grid is technologically well-advanced and can serve as an inspiration to other markets. More participants to verify the architecture could provide useful insights from the industry. Further, only two researchers were used to verify the exclusion/inclusion criteria of the mitigation strategies. Using another researcher to strengthen the validity could reduce the subjectivity bias from the other researchers. IEC 62443 [12] requires performing a detailed cybersecurity risk assessment. However, due to the availability of the distribution systems, it only provides a high-level security assessment based on information gathered from the interviews and meetings with the industry. Hence, it can only be considered from a conceptual level.

Whenever presenting an architecture, there is a trade-off between being too specific (getting bogged down into details) and being too generic (glossing over important details). Closely basing the architecture on existing infrastructure increases recognisability for industry stakeholders, but may raise confidentiality concerns, and run the risk of being more quickly outdated due to the continuous inclusion of new technology and solutions. However, a too-generic architecture could risk potential stakeholders not identifying their systems. Discovering the silver lining in such an environment requires close interaction with multiple industry representatives and DSOs.

The paper only considers the technical systems of the control center. Poorly established incident response, or (un)intentional misconfigurations from employees could still cause security breaches. Future work should also address organizational factors and processes in the future distribution control center by introducing security training from management to the workers at the sharp end.

6 Conclusion and Future Work

This paper has presented the development of a security architecture for Norwegian DSOs, derived from NIST guidelines, SGAM, IEC 62443, and meetings and interviews with industry representatives. The architecture includes future developments and tasks of the DSO and explains some of the implications of

these advancements in the smart grid. Future work will address the human factors of the control center, involving relevant processes and roles in the security architecture.

Acknowledgement. This research was funded by the Research Council of Norway through FME CINELDI (project no. 257626). We are grateful to the anonymous industry representatives and our colleagues Henning Taxt, Maren Istad, Oddbjørn Gjerde, and Santiago Sanchez-Acevedo from SINTEF Energy Research, who contributed through interviews and discussions.

References

1. Awadid, A.: Reference architectures for smart grids: Towards a standard-based comparative framework. In: 7th International Conference on Engineering and Emerging Technologies, ICEET 2021. IEEE (2021). https://doi.org/10.1109/ICEET53442.2021.9659739
2. Bernsmed, K., Jaatun, M.G., Frøystad, C.: Is a smarter grid also riskier? In: Security and Trust Management. vol. 11738 LNCS, pp. 36–52. Springer (2019). https://doi.org/10.1007/978-3-030-31511-5_3
3. Bjørndalen, J., Løken, I.B., Berntsen, C.L., Bjørkli, R.B., Gimmestad, I., Sletten, K.: Fra brettet til det smarte nettet - Ansvar for driftskoordinering i kraftsystemet (In Norwegian: From the board to the smart grid - responsibility for coordination in the power system). Tech. rep., RME (2020)
4. CEN/CENELEC/ETSI Joint Working Group: Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids. Tech. rep., CEN/CENELEC/ETSI (2011)
5. Degefa, M.Z., Lundkvist, H., Sanchez-Acevedo, S., Gregertsen, K.N.: Challenges of TSO-DSO voltage regulation under real-time data exchange paradigm. IEEE Open Journal of the Industrial Electronics Society **4**, 75–84 (2023). https://doi.org/10.1109/OJIES.2023.3239946
6. Elhub AS: Elhub, `https://elhub.no/en/`
7. Flå, L.H., Jaatun, M.G.: A method for threat modelling of industrial control systems. In: Cyber Science 2023. Springer (2023)
8. Foros, J.: Reference system for a general risk analysis of smart distribution grids. Tech. rep., SINTEF (2020)
9. Griffin, R.W., Langer, L.: Chapter 7 - Establishing a Smart Grid Security Architecture. In: Skopik, F., Smith, P. (eds.) Smart Grid Security, pp. 185–218. Syngress, Boston (2015). https://doi.org/10.1016/B978-0-12-802122-4.00007-9
10. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS quarterly pp. 75–105 (2004). https://doi.org/10.2307/25148625
11. Hypponen, M.: If It's Smart, It's Vulnerable. Wiley, 1st edition edn. (Aug 2022)
12. IEC: IEC 62443: Industrial communication networks - Network and system security
13. ISO: Information technology – security techniques – information security management systems – overview and vocabulary. ISO/IEC Standard 27000:2018 (2018), `https://www.iso.org/standard/73906.html`
14. Kern, M., Taspolatoglu, E., Scheytt, F., Glock, T., Liu, B., Betancourt, V.P., Becker, J., Sax, E.: An architecture-based modeling approach using data flows for zone concepts in industry 4.0. In: 2020 IEEE International Symposium on Systems Engineering (ISSE). pp. 1–8 (2020). https://doi.org/10.1109/ISSE49799.2020.9272013

15. Kjølle, G.: Drivkrefter og miniscenarier for fremtidens elektriske distribusjonsnett (in Norwegian: Drivers and mini scenarios for the future ditribution grid) (2022)
16. Köhler, C., Kersten, R., Schöpf, M.: Cloud-based digital twin for distribution grids: What is already available today. IEEE Power and Energy Magazine **22**(1), 72–80 (2024). https://doi.org/10.1109/MPE.2023.3336255
17. Langer, L., Skopik, F., Smith, P., Kammerstetter, M.: From old to new: Assessing cybersecurity risks for an evolving smart grid. Computers and Security **62**, 165–176 (9 2016). https://doi.org/10.1016/j.cose.2016.07.008
18. Line, M.B., Tøndel, I.A., Jaatun, M.G.: Cyber security challenges in smart grids. In: ISGT Europe, 2011 2nd IEEE PES International Conference (12 2011). https://doi.org/10.1109/ISGTEurope.2011.6162695
19. Morch, A.Z., Sæle, H.: Interaction DSO-TSO Overview. Tech. rep., SINTEF (2018)
20. Perez, N.R., Domingo, J.M., Lopez, G.L., Avila, J.P.C., Bosco, F., Croce, V., Kukk, K., Uslar, M., Madina, C., Santos-Mugica, M.: ICT Architectures for TSO-DSO Coordination and Data Exchange: A European Perspective. IEEE Transactions on Smart Grid **14**, 1300–1312 (3 2023). https://doi.org/10.1109/TSG.2022.3206092
21. Reference Architecture Working Group: Smart grid reference architecture. Tech. rep., CEN-CENELEC-ETSI (2012)
22. Riksrevisjonen: Riksrevisjonens undersøkelse av nves arbeid med ikt-sikkerhet i kraftforsyningen (in Norwegian: NVE's work on ICT security in the power supply). Tech. rep., Norwegian Office of the Auditor General (2021)
23. Smart Grid Coordination Group: Document for the M/490 Mandate Smart Grid Information Security. Tech. rep., CEN-CENELEC-ETSI (2014), `ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf`
24. Smart Grid Interoperability Panel: NISTIR 7628 Revision 1: Guidelines for Smart Grid Cybersecurity. Tech. rep., National Institute of Science and Technology (9 2014). https://doi.org/10.6028/NIST.IR.7628r1
25. Statnett: Quarterly resolution and the energy markets. `https://www.statnett.no/en/for-stakeholders-in-the-power-industry/system-operation/the-power-market/quarterly-resolution-and-the-energy-markets/` (2022)
26. Stølen, K.: Teknologivitenskap : forskningsmetode for teknologer (2019)
27. Tøndel, I.A., Borgaonkar, R., Jaatun, M.G., Frøystad, C.: What Could Possibly Go Wrong? Smart Grid Misuse Case Scenarios. In: 2020 International Conference on Cyber Security and Protection of Digital Services. IEEE (2020). https://doi.org/10.1109/CyberSecurity49315.2020.9138892
28. Wagner, T., Kittl, C., Jakob, J., Hiry, J., Häger, U.: Digital twins in power systems: A proposal for a definition. IEEE Power and Energy Magazine **22**(1), 16–23 (2024). https://doi.org/10.1109/MPE.2023.3328581
29. Wright, L., Davidson, S.: How to tell the difference between a model and a digital twin. Advanced Modeling and Simulation in Engineering Sciences **7**, 1–13 (2020). https://doi.org/10.1186/s40323-020-00147-4