Identification of cyber threats and vulnerabilities in Norwegian distribution networks*

Martin Gilje Jaatun[1] [0000−0001−7127−6694], Jørn Foros[2] [0000−0003−3596−569X], and Maren Istad[3] [0000−0001−6866−5402]

[1] SINTEF Digital, Trondheim, Norway martin.g.jaatun@sintef.no
[2] Safetec, Trondheim, Norway jorn.foros@safetec.no
[3] SINTEF Energy Research, Trondheim, Norway maren.istad@sintef.no

Abstract. This paper presents cyber threats and vulnerabilities in Norwegian power distribution networks identified from historical incidents and practical experiences over the last decade.

Keywords: cyber security, power systems, smart grid

1 Introduction

Smart grids are the distribution grid of the future, with increased use of digital solutions and communication that increases the functionality of the grid, both in terms of monitoring, operation and control. Such a cyber-physical network may contain many subsystems and functions that interact and together allow for a more efficient and flexible operation of the network [5].

The increased number of digital systems in smart grids also increases the number of possible cyber threats, both by increasing the number of points of attack, and by exacerbating the consequences of incidents. The latter is due to increased interaction between subsystems, where events in one system can spread to several systems, impacting the security of supply.

Norway is relatively advanced in terms of the digitalization of the power grid, and it is therefore relevant to study historical data on incidents with impact on the security of supply, and contrast that with known incidents internationally.

The rest of the paper is structured as follows. Section 2 introduces the assets that need protection in the power industry, and Section 3 discusses threats to these assets base on historical data. Section 4 highlights international incidents from the last decade. Section 5 revisits the identified assets and discusses specific threats. Section 6 summarises the results.

* At the time this research was performed, Dr. Foros was employed by SINTEF Energy Research

2 Assets to protect

A mapping of assets is key information when threats are to be identified. Critical assets in distribution networks may include both the value of information and/or the value of a subsystem within the network itself.

We conducted a workshop with DSOs [6] that resulted in the identification of a large number of assets, where the following were particularly highlighted: Operational control systems for control and monitoring are of high value, but are regarded as little exposed. The AMI system as a whole has a high value, although individual components of the AMI system are not necessarily that important. The AMI system are more exposed than the operational control system. Customer information and personal data about employees require protection and are considered valuable. Usernames/passwords in IT systems have a high value and to a certain extent high exposure (for example when passwords have been reused and data breaches occur at other services). Credential stores such as Active Directory have high value and would be an attractive target for an attacker. Communication infrastructure is important. Some types of data are considered particularly sensitive (examples are distribution network information, condition of individual components, geolocation of critical objects). Systems used for access control are important, but even more vulnerable are the employees themselves and their equipment. Sensors and sensor data are important, and sensors are more exposed than many other components in the system. Test environments must be secured, exemplified by Distribution Management System (DMS) test environment.

In addition, one can observe the following from the results: Breaker functionality in AMI has high value and high exposure. DMS is considered to have higher exposure than SCADA. Third parties/suppliers are considered to have high exposure, but relatively low value. However, it is not specified what is meant by third party/supplier, e.g. whether this means the equipment/systems they have/deliver.

3 Identification of cyber threats and vulnerabilities from national historical data/experiences

Sources of historical information on cyber threats and vulnerabilities in distribution networks in Norway are primarily the Norwegian Water Resources and Energy Directorate (NVE), the Norwegian Infrastructure CERT (InfraCERT or KraftCERT) and FASIT [3]. In addition, there are more general sources that not only discuss cyber threats and vulnerabilities in the power supply, but more generally for organisations in Norway. In the following, cyber threats and vulnerabilities from these sources are reviewed. Most of the sources focus on intentional/malicious actions, but the FASIT is mostly focused on unintentional events. Attempts are made in the review to distinguish between threats and vulnerabilities even though this is not always a clear distinction, and this is not always done in the sources.

3.1 NVE

The Power Emergency Preparedness Regulations require Norwegian DSOs to report undesirable incidents that have or could have reduced security of supply to the NVE, including incidents related to IT systems [17]. This report is not limited to cyber-threats, and includes the entire power supply, not just utilities. The following categories for adverse events are used:

1. Challenging weather (11)
2. Technical failure (11)
3. Burglary & Sabotage (7)
4. Information Security (5)
5. District heating (1)
6. ICT Malware & System Errors (1)
7. Human error (1)
8. Other events (2)

The number of events per category is given in parentheses. It is primarily categories 4 and 6 that contain cyber threats. In addition, categories 3 and 7 may also be relevant. As we see, not many incidents related to cyber threats have been reported. The Category 6 incident was a cyber threat – this was a failed attempted intrusion into computer systems by phishing. There was only one incident in this category in 2018, but there were more incidents in both 2017 and 2016 (16 in total over the three years). The incidents in category 4 concern a lack of protection of power-sensitive information, i.e. vulnerabilities that can be exploited to acquire such information. The incidents reported in category 3 concern physical break-ins and sabotage in facilities, and not break-ins to computer systems. But physical break-ins can be the first step on the road to accessing computer systems. The Category 7 incident was related to excavation work that damaged a power cable and had nothing to do with cyber threats. There are no reports that any of the incidents had any consequences for security of supply.

In order to obtain more information about the cyber security status of the power supply in Norway, the NVE sent out a survey to Norwegian companies in 2017. 88 companies responded to the survey, of which 25% of these are grid companies and 32% are corporations. merger of several companies. The report that was prepared afterwards provides a broader picture of cyber security in the Norwegian energy supply [16]. It also contains descriptions of the results of penetration tests carried out by three Norwegian grid companies. Two types of tests were performed:

- Outside test: Vulnerability scan from the internet
- Insider test: Simulated targeted threat actor with access to management networks

The report provides a picture of both the threats enterprises in the Norwegian power supply sector experience being exposed to, and the vulnerabilities they have in their systems and processes. The report also provides a picture of the consequences of undesirable incidents, but few enterprises have reported serious consequences for their operations and security of supply.

Threats Nearly 70% of organisations responded that they have had unwanted incidents related to cyber threats. 59% responded that they have had incidents they perceived as serious. The report [16] shows that there have been clearly more threats targeting the administrative systems (customer system, financial system, maintenance system, etc.) than operational control system (SCADA etc.). Most of the incidents against operational control systems have occurred in smaller organisations (1-19 employees). The most widespread incident is fraud, which mainly involves fraudulent attempts via e-mail. Other common occurrences are virus/malware infection, attempted data breach/hacking and computer damage.

Data damage includes unauthorised alteration/deletion of data, targeted actions aimed at reducing data availability, ransomware, etc.

Vulnerabilities The organisations were also asked [16] about their security practices, and the answers to this provide some information about where the organisations may be vulnerable. The following three topics were asked about:

- Outsourcing
- Supplier dependency
- Information Security Management System

65% of enterprises fully or partially outsource their administrative IT systems, while 32% fully or partially outsource their operational control systems. None of the large enterprises (more than 100 employees) outsource operational control systems. Of those who outsource administrative systems or operational control systems, 11% respond that they use services abroad, while 5% respond that they do not know this. 74% of organisations respond that they are medium or strongly dependent on their IT supplier to handle incidents. This includes both incidents in administrative systems and operational control systems. Similar figures apply if one limits the question to operational control systems. 24% of the enterprises respond that they do not have an information security management system or do not know if they have one. This applies primarily to the smaller enterprises with few employees.

Penetration tests carried out at three Norwegian grid companies [16] also provide relevant information about vulnerabilities. From these tests, the NVE report [16] points out in particular that many vulnerabilities can be linked to lack of supplier control, inadequate security updates of operating systems and software, and inadequate decommissioning of services that are no longer in use. The test results also showed that an attacker with access to the management system can exploit this to penetrate deeper into the systems, and that operational control systems are generally better protected than AMI systems.

Consequences Although many have perceived undesirable incidents as serious, few enterprises have reported serious consequences for operations and security of supply. 13% answered that they have had events that have had negative consequences such as lost production, financial losses, reputational loss or weakened market position.

This amounts to 77 incidents across the 13% establishments (out of a total of 88 organisations). Only three of the incidents have involved operational control systems.

62 of the enterprises (out of a total of 88 responses) have provided further descriptions of the most serious incident they have experienced. An overview of the consequences of the most serious incident is shown in Fig. 1. None of the enterprises have had incidents that have resulted in customer disruptions.

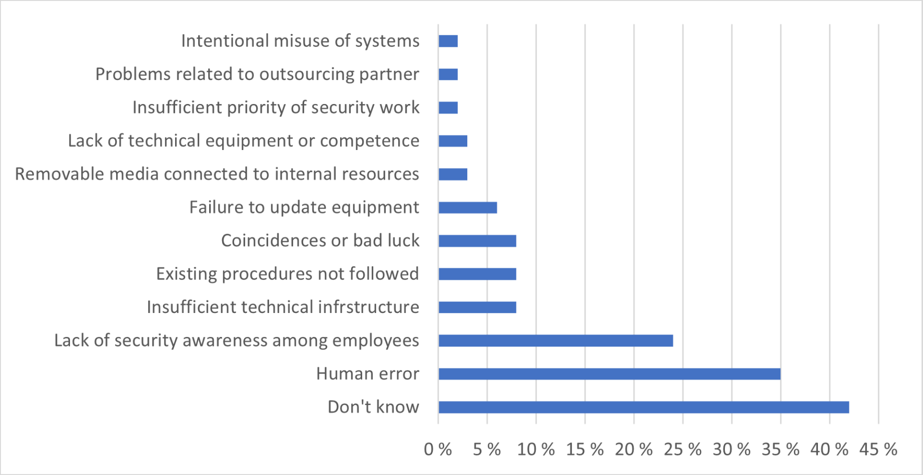

Fig. 1. Contributing factors to incidents according to respondents [16] (n=62)

Risk-reducing measures The NVE report [16] summarizes by recommending measures to limit the risk. In general, good basic security of IT systems, an information security management system, and good training of employees in security culture is recommended. Furthermore, the following are highlighted:

- Good security includes both monitoring one's systems for detecting undesirable incidents, and security barriers that ensure that the incidents do not entail serious consequences
- Good security must include suppliers [9], as many services are outsourced today[4]
- It is important to have good routines for security updates, as threat actors can be quick to take advantage of new known vulnerabilities
- It is important to have a good overview of services that are exposed to the internet.

[4] A recent example is the attack on the company SolarWinds in 2020, which spread to their customers

3.2 KraftCERT

NVE has also delegated information gathering on IT security to KraftCERT, which publishes an annual report[5] describing security incidents in the power supply in Norway that they have been involved in handling. In the report, KraftCERT highlights the following types of incidents that they have handled during the year:

- Compromise of ICT networks, both administrative networks and control networks
- Login attempts against exposed login services
- Malware attachments and malware links
- Compromised suppliers and supply chain attacks
- Compromises due to misconfigurations
- Attacker-proof domains
- Reconnaissance to obtain information
- Phishing with extortion malware or for information retrieval
- Leakage of information.

KraftCERT also alerts the industry to relevant vulnerabilities.

3.3 FASIT

According to the Regulations relating to system responsibility in the power system, all licensees must report operational disruptions and interruptions (including planned outages that have resulted in interruptions) in the transmission grid, regional grid, distribution grid and production facilities in FASIT [3]. This includes operational disruptions and disruptions caused by cyber-threats (and other causes). However, this reporting is not designed to gather data useful for assessing cyber security, and the value of the data for this purpose is therefore limited. The answer is not focused on detecting intentional/malicious actions, but more on unintentional events. In addition, we know from the reporting to NVE and KraftCERT described above, that although there have been some unwanted cyber-related incidents, few have caused operational disruptions.

In order to investigate to what extent the FASIT may contain relevant information, we can check what opportunities FASIT gives the user to indicate cyber-threats when reporting. This is given by the requirement specification of FASIT [3]. FASIT gives the user the opportunity to, among other things, specify which plant part failed and what caused the failure, in the form of predefined response options. Most response alternatives are specified for faults in the physical electrical power equipment out in the grid. Few response alternatives directly relevant to cyber threats have been specified. Of the plant parts that it is possible to select, the following are those that are seemingly most relevant to potential cyber threats: protection, signal transmission, control and automation equipment, and remote control. FASIT specifies few response alternatives for the cause of error that are directly relevant to IT-related error events.

[5] This report, published in 2020, is unfortunately not available to the public.

Based on the registrations in FASIT, statistics are published on operational disruptions and outages in Norway every year. The Norwegian Water Resources and Energy Directorate (NVE) publishes annual outage statistics, while Statnett publishes annual statistics on operational disturbances and errors. None of these provide sufficient detail to conclude whether there have been incidents within the categories of plant parts and causes of failure with IT relevance identified above. But this can be investigated by extracting data directly from the FASIT database. In Table 1, the number of registered permanent faults in FASIT in the period 2019-2020 is shown for the selected plant parts from 10 kV up to and including 420 kV. Of these errors, none were registered with the cause of error, software/hardware failures or vandalism/sabotage. A total of 59 were registered as incorrect configuration and 13 as installation errors. In comparison, a total of 21 275 faults were registered from 1 kV and above (excluding the low-voltage grid).

Table 1. Number of registered permanent errors in FASIT in the period 2019-2020 for some selected plant parts

System component	Number of permanent errors
Remote control	10
Control and automation equipment	53
Signal transmission	20
Protection devices	133

3.4 Other

In addition to NVE, KraftCERT and FASIT, there are more general sources that not only discuss cyber threats and vulnerabilities in the power supply (including distribution networks), but more generally for businesses and society in Norway.

Every year, the Norwegian authorities publish three public threat and risk assessments. These are published by the Norwegian National Security Authority (NSM), the Norwegian Police Security Service (PST) and the Norwegian Intelligence Service and contain, among other things, assessments of cyber-related risks to society. The assessments are complementary and partly overlapping. Broadly speaking, they can be described as follows: The intelligence service's assessment focuses on external threats outside our national borders, PST's assessment focuses on internal threats within national borders, while NSM's assessment focuses on vulnerabilities in Norwegian enterprises.

In both the Intelligence Service's [13] and PST's [15] assessments, foreign states' espionage in cyberspace is highlighted as a significant threat to Norway. This includes digital mapping of Norway's infrastructure, including the distribution grid. NSM's latest annual report on the digital risk picture for Norwegian public and private enterprises [14], concludes that the digital risk picture is sharper and that there are clearer risks associated with complex threats that affect across sectors. Threats can come from several different quarters, both from foreign states and criminal actors. In particular, vulnerabilities related to long digital value chains, dependence on suppliers, cloud services and data centers, IoT and sensors, inadequate control of user accounts and passwords, insiders, and known digital and human vulnerabilities that can be exploited in the event of e.g. missing security updates.

Every two years, the Norwegian Business and Industry Security Council publishes a survey which estimates the number of unreported incidents [11], mapping the extent of IT security incidents in Norwegian private households and public businesses, as well as how companies are prepared for such incidents. The survey deals with much of the same as NVE's survey of the IT security status in the power supply, but for a larger sample of different businesses. It is therefore not discussed in detail here, but a couple of interesting results can be noted from the survey:

- A large proportion of the incidents are discovered by chance
- There appears to be a general positive development in Norwegian enterprises' work on information security since the earlier survey in 2018.

The Norwegian Centre for Information Security (NorSIS) supports both individuals and small and medium-sized Norwegian enterprises with advice on information security. They publish an annual "threats and trends" report [12] which identifies the most serious threats to private individuals and small and medium-sized enterprises based on inquiries to NorSIS as well as a selection of assessments and reports from other actors. The report highlights the following threats:

- Ransomware
- Account hijacking
- Supply chain attacks
- Fraud/phishing.

4 Identification of cyber-threats from international historical data/experiences

In the following we mention some relevant intentional cyber threats that have been experienced internationally, either in the power industry or other industries with cyber-physical systems. Some of these have been directly aimed at operational control systems, and some at management systems.

4.1 Incidents in power grids

There have by now been quite a large number of security incidents in power grids [8]. In 2014, large parts of Europe, including the Norwegian power industry, were subjected to a massive campaign known as Dragonfly [20]. This campaign used multiple attack vectors to try to infect various players in the power industry with the malware Havex including so-called waterhole attacks (where control system vendors had their websites compromised, and updates and drivers replaced with ”trojanized” versions). Havex caused no direct damage, but collected information about the topology etc. of infected systems. An interesting aspect of this malware was that it had built-in remote update functionality, which could allow it to be modified to take more destructive actions at a later time.

On Christmas Eve 2015, nearly a quarter of a million Ukrainian electricity subscribers were blacked out for six hours and more [10]. Ukrainian online companies had been infected (using spear phishing) with the Blackenergy 3 malware, and malicious actors had long been able to penetrate deep into the Ukrainian distribution network. From their beachhead in the DSOs' administrative networks, attackers could access DMS via their operators' legitimate VPN connections, and on the day of the attack, they could then use DMS to disconnect substations from the network. In addition, automatic recovery was prevented by uploading malignant updates which ”bricked” Remote Terminal Units (RTUs), as well as deleting Human-Machine Interface (HMI) machines via so-called ”killdisk” functionality. The loss of access to SCADA meant that the possibility of automatic control in some locations was lost for up to a year, and recovery was only possible by manual effort.

On December 17, 2016, Ukraine suffered another attack. This time it was the Pivnichna substation in the transmission grid that was allowed to escape. Parts of Kyiv were without power for up to an hour, and although there were similarities to the incident the previous year, there was speculation that there was a new type of malware in the picture. The following year, analysts from eSET [1] and Dragos [2] reported that they had identified the new malware that they named respectively Industroyer or CrashOverride (two different names for the same malware). Interesting features include that the malware targeted control systems, was module-based, and had modules for communication via protocols IEC 60870-5-101, IEC 60870-5-104 and IEC 61850. The modular design indicates that like Havex, Industroyer is likely to be updated with new protocols and functionality in the future. The 2016 attack focused on reducing the visibility and controllability of the operating system [18], and also made an attempt to remove protection in the substation.

In June 2017, a large number of international businesses were affected by an encryption virus with worm-like properties, which was called NotPetya [7]. Among the affected businesses were reportedly Ukrainian power companies. This attack went through the supply chain, when a software company that provided widely used accounting software was compromised. The attacker put code on a company's update servers, allowing customers to download malware when attempting to download software updates. Many computers and files were made inaccessible.

In 2020, a large number of international businesses were also affected by a supply chain attack. This time it was the American software provider Solar-

Winds [21] that was affected. The attacker established a backdoor into updates to the SolarWinds Orion software, which is used for information system management, causing customers to include this backdoor when downloading software updates. This malign version of SolarWinds Orion has been installed in Norwegian companies, but no injuries have been reported in Norway as a result.

In May 2021, the Norwegian company Volue (formerly Powel) [19] was exposed to the Ryuk ransomware. This caused internal operational disruptions, but so far there is nothing to indicate that Norwegian grid companies had their information compromised [22].

4.2 Incidents in other industries

There have also been a number of incidents in cyber-physical systems other than power grids over the past decade with great potential for damage. The public became seriously aware of the threat posed by the Stuxnet virus that became widely known in 2010 [4] (later information suggests that the campaign started as early as 2007), and is considered to be the first case of a real cyber-attack causing physical damage to a facility. Stuxnet directly targeted control systems and infected the HMI of Siemens Simatic PLCs in the Iranian uranium enrichment plant Natanz as a "man-in-the-middle" attack. By quickly manipulating the speed of rotation of centrifuges used in the enrichment process, it caused mechanical breakdown in a large number of centrifuges. Due to the manipulation of the HMI, the behavior of the centrifuges appeared completely normal, so that nothing was discovered until it was too late.

The 2017 Trisis/Triton malware [18] targeted a specific version of the Schneider Electric Triconex Safety Instrumented System (SIS), causing the Triconex SIS to stop working. There is no reason to believe that Schneider was more vulnerable than other vendors, but rather that the attackers had targeted a victim, and that victim had Schneider equipment. Trisis/Triton gave the attackers a way to connect and perform changes to equipment. Exactly who the target was in this case is not publicly known, but it is said to have been a refinery, and reportedly resulted in a number of individual systems being put out of action. However, experts believe that Trisis/Triton had ambitions of even greater damage, which was not realized.

5 Identification of cyber-threats in workshops with DSOs

As mentioned in section 2, we organised a workshop [6] where assets in the distribution grid were identified. After the identification of assets, cyber threats that can harm the assets were identified. Finally, the threats were assessed according to likelihood and consequence.

The workshop resulted in the identification of a large number of cyber threats, and not everything can be reproduced here. The following were particularly highlighted in the summary of the workshop:

- One envisions different attack vectors. The most likely are considered to be third parties/suppliers, as well as physical access to equipment and various types of malicious code and phishing.
- Attacks on communications infrastructure are also highlighted.
- Attacks on SCADA are considered to have high consequence, but are not perceived as likely.
- Some types of attacks on AMI infrastructure are considered to have high consequence, but it is unclear how to view the likelihood of such attacks. One group considers attacks on AMI less likely than attacks on SCADA systems, while the other group considers it more likely. This may be due to the fact that there was a preponderance of employees with an IT background in one group, and a preponderance of employees who worked with power infrastructure (OT systems) in the other group.
- The extent to which an attack is detected affects the consequence.
- Employees are an important attack vector, and it is therefore important to work with threats such as social engineering, blackmail and unfaithful servants. Some roles, such as admin user, may be at higher risk than others.

It may also be mentioned that the workshop identified many of the threats discussed earlier. The workshop also identified a number of other threats, such as:

- Attack on DMS
- Manipulation of sensors
- Deactivation of components
- Customer information changed or gone astray

6 Summary and conclusions

From the review in the previous sections, it is clear that Norwegian DSOs are and will be exposed to cyber threats. Incidents have been observed both nationally and internationally that show this. There are motives, willingness and abilities among several different actors to carry out attacks against the power industry, both by foreign states and criminal actors. Attacks can occur against both administrative systems and operational control systems. Access to administrative systems can be a way forward to operational control systems.

In the reviewed sources, several intentional/malicious acts have been documented. Few unintentional incidents have been documented. Unintended incidents are reported in FASIT if they lead to disruption or interruption. However, most of the response alternatives in FASIT are specified for faults in the physical electric power equipment out in the grid. Few response alternatives directly relevant to cyber threats have been specified. This makes it difficult to catch such threats in FASIT.

Based on the review in this paper, a simple assessment of known potential cyber threats to Norwegian DSOs has been made in Fig. 2. Here are the cyber-threats known from the historical sources described in previous sections included.

A rough assessment of them according to probability and consequence has also been made. This assessment is based on information in the reviewed sources, supplemented by the assessments made in the 2019 workshop for similar cyber threats. This should only be seen as a rough assessment of the threats, as the threats are not very specific, and both probability and consequence depend on several factors, such as who the attacker is, where the point of attack is, when the attack is detected, etc.

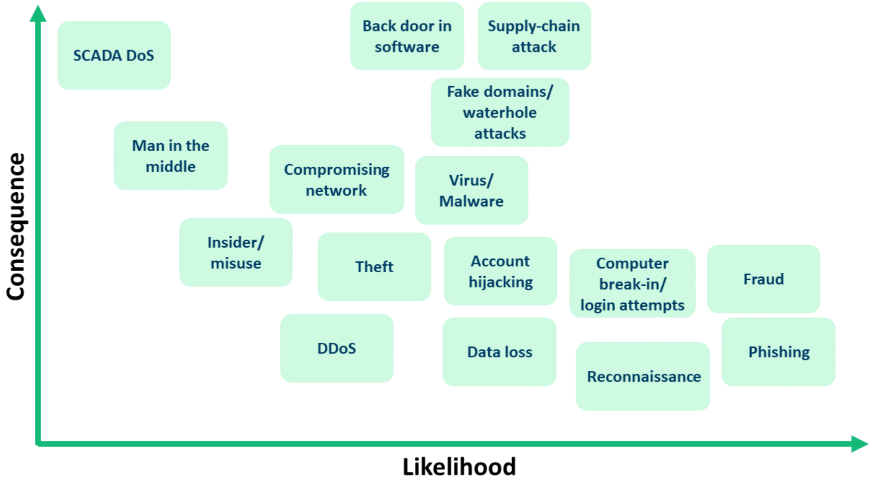

Fig. 2. Rough assessment of known potential cyber threats to Norwegian DSOs

Although several intentional cyber-threats to the power industry have been documented, this has not led to serious consequences in Norway yet. Therefore, one cannot expect to find any intentional cyber-threats reported in FASIT. This shows that the Norwegian power supply is relatively well protected. However, there are several observations that give cause for some concern. International incidents show that the attackers are advanced and have the capabilities to attack operational control systems. The Survey on unreported incidents [11] shows that a large proportion of incidents are discovered by chance. Technological and organisational developments can lead to new or enhanced vulnerabilities, such as:

- Vulnerabilities related to long digital supply chains
- Service outsourcing and dependency on suppliers
- Increased number of services exposed to the Internet
- Cloud services and data centers
- IoT and sensors

One must also not forget more traditional and known vulnerabilities that can still be exploited, such as:

- Inadequate control of user accounts and passwords
- Missing security updates
- Inadequate discontinuation of services that are no longer in use
- Misconfigurations
- Human error
- Lack of security awareness or security work
- Lack of equipment/processes to support good security.

It is a challenge for the industry that the power supply on the one hand is well protected and has good reliability, while on the other hand it is known that it is exposed to several new threats, as described above. It is difficult for grid companies to verify that they have made adequate risk assessments and taken sufficient account of potential threats. The risk assessments that are currently carried out related to ICT are often focused on individual systems and information security, even though systems today are becoming more and more integrated, interacting and far-reaching. The challenge is to understand how the various systems are interconnected and find out how risk in one system affects another, or how the risk of one player in the value chain affects another.

Acknowledgements

The research in this paper was supported by the Research Council of Norway through the Intersecure project (project number 296381) and the Cineldi FME (project number 257626).

References

1. Cherepanov, A., Lipovsky, R.: Industroyer: Biggest threat to industrial control systems since stuxnet. WeLiveSecurity by eset (2017). URL https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-\-stuxnet/
2. Dragos Inc.: CRASHOVERRIDE – Analysis of the Threat to Electric Grid Operations (2017). URL https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
3. Eggen, A.O., Heggset, J., Sagen, K., Aabakken, C., Hjartsjø, B.T., Østingsen, E.A., Gjerstad, S.O.: FASIT, the Norwegian reliability data collection system - experiences and utilitarian values. In: 27th International Conference on Electricity Distribution (CIRED 2023), pp. 2243–2247 (2023). https://doi.org/10.1049/icp.2023.1214
4. Falliere, N., Murchu, L.O., Chien, E.: W32.Stuxnet Dossier (2011). URL http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
5. Foros, J.: Referansesystem for overordnet risikoanalyse av smarte distribusjonsnett (in Norwegian: Reference system for overall risk analysis of smart distribution grids. Tech. Rep. AN 12/20/48, SINTEF Energy Research AS (2020)
6. Foros, J., Istad, M., Jaatun, M.G.: Identifisering av cyber-trusler og sårbarheter i distribusjonsnett i norge basert på historiske data og erfaringer (in Norwegian). Tech. Rep. AN 21.12.52, SINTEF (2022)

7. Greenberg, A.: The untold story of NotPetya, the most devastating cyberattack in history. Wired, August **22** (2018). URL https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
8. Jaatun, M.G., Moe, M.E.G., Nordbø, P.E.: Cyber security considerations for self-healing smart grid networks. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (2018). https://doi.org/10.1109/CyberSecPODS.2018.8560668
9. Jaatun, M.G., Sæle, H.: A checklist for supply chain security for critical infrastructure operators. In: The International Conference on Cybersecurity, Situational Awareness and Social Media, pp. 235–249. Springer (2023)
10. Lee, R.M., Assante, M.J., Conway, T.: Analysis of the cyber attack on the ukrainian power grid, defense use case. SANS ICS and E-ISAC white paper (2016). URL https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
11. Norwegian Business and Industry Security Council: Mørketallsundersøkelsen (in Norwegian: Survey on unreported incidents) (2022). URL https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2022-web-sider.pdf
12. Norwegian Centre for Information Security: Trusler og trender 2021 (in Norwegian: Threats and trends 2021) (2022). URL https://norsis.no/content/uploads/2022/05/NorSIS_Trusler_Trender_2021_Digital.pdf
13. Norwegian Intelligence Service: Fokus 2023 – etterretningstjenesten (2023). URL https://www.etterretningstjenesten.no/publikasjoner/fokus/innhold
14. Norwegian National Security Authority: Risiko 2023 – Økt uforutsigbarhet krever høyere beredskap (in Norwegian: Risk 2023 – increased unpredictability requires increased preparedness) (2023). URL https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf
15. Norwegian Police Security Service: National threat assessment 2023 (2023). URL https://www.pst.no/globalassets/2023/ntv/ntv_2023_eng_web.pdf
16. NVE: Informasjonssikkerhetstilstanden i energiforsyningen (in Norwegian: The state of information security in the energy supply). Tech. Rep. 90-2017, Norwegian Water Resources and Energy Directorate (2017). URL http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf
17. NVE: "oppsummering av uønskede hendelser 2018 i energiforsyningen (in Norwegian: Summary of undesirable incidents 2018 in energy supply)". Tech. Rep. Fact Sheet No. 4/2019, Norwegian Water Resources and Energy Directorate (2019). URL http://publikasjoner.nve.no/faktaark/2019/faktaark2019_04.pdf
18. Slowik, J.: Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the history and future of integrity-based attacks on industrial environments. Dragos whitepaper (2019). URL https://dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf
19. Stupp, C.: Energy tech firm hit in ransomware attack. Wall Street Journal (2021). URL https://www.wsj.com/articles/energy-tech-firm-hit-in-ransomware-attack-11620764034
20. Symantec Security Response: Dragonfly: Cyberespionage attacks against energy suppliers (2014). URL https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
21. Tidy, J.: Solarwinds: Why the Sunburst hack is so serious. BBC News (2020). URL https://www.bbc.com/news/technology-55321643
22. Volue: Volue releases postmortem report on cyberattack (2021). URL https://www.volue.com/news/volue-releases-postmortem-report-cyberattack