

The Effect of Regulation and Audits on Implementation of Cybersecurity Controls in Norwegian Grid Companies

Jon-Martin Storm

Department of Informatics, University of Oslo, Norway. E-mail: jonmartp@ifi.uio.no

Janne Hagen

Department of Informatics, University of Oslo, Norway. E-mail: jannehag@ifi.uio.no

Sigrid Haug Selnes

Department of Informatics, University of Oslo, Norway. E-mail: sigrihse@ifi.uio.no

In 2011, Stuxnet became a game-changer concerning Industrial Control Systems Security. By manipulating process system software, attackers changed the physical processes of enriching uranium in a nuclear power plant in Natanz, Iran. Since then, the methodological sophistication of cyber-attacks has evolved. The need for intrusion detection capability has grown accordingly. Critical infrastructures, like the energy sector, are operated with the support of industrial control systems, and there are urgent demands for securing these systems. Governmental regulations, supervisions, and reviews are measures to enforce cybersecurity in critical infrastructures. However, it is not well studied how effective such regulation is. This paper examines the impact of prescriptive statutory requirements for cybersecurity in the Norwegian electric power system. For about ten years, the Norwegian government has enforced detailed cybersecurity regulations for electric utilities. The study examines and discusses the change in the industry's implementation of cybersecurity measures, emphasizing intrusion detection systems. Based on audit reports and survey data, the study reveals an improvement in implementing intrusion and detection systems during the last ten years.

Keywords: cybersecurity, regulation, industrial control system, intrusion detection

1. Introduction

Expanding the production of renewable and clean energy has become urgent as the conflict in Ukraine has worsened, and the EU and other countries sanctioned Russian trade. Years before the conflict, developing intermittent energy production was already emphasized in European energy politics. Integration of unregulated renewables such as the production of wind power and photoelectric voltage power demands digitalization of the power system for situational awareness and reliable system operations.

Advanced data analytics of information from smart meters, sensors measuring technical status, and cross-border data sharing is argued to be another precondition for the green deal and the stability and reliability of the energy system. However, while digitalization and data analytics provides excellent opportunities for improved sit-

uational awareness of the power system state and optimization of production due to market demand, digitalization comes with an increased risk of failure and malfunctions.

Looking to Norway, current energy system malfunctions are caused by natural incidents or technical system failures mainly due to implementation issues or embedded software vulnerabilities. So far, cyberattacks have not influenced the system's performance. However, internationally, several cyberattacks on critical infrastructures have caused system failures. The attacks on the power system in Ukraine showcase a worst-case scenario. Lee, Assante, and Conway 2016. Although technical failures have not achieved the same attention, such incidents are more common and thus also important to mitigate. We understand that building a security culture and awareness and protecting systems against cyberattacks must be regular business practices. The mutual dependency

2 *Jon-Martin Storm, Janne Hagen and Sigrid Haug Selnes*

that exists and is evolving between digital systems and the energy system, and the ongoing war in Ukraine, calls for revitalized attention on securing critical infrastructures like the power system against cyberattacks.

Risk assessment is the foundation of good security work, followed by prevention, detection, response, and recovery controls, as shown in well-known cybersecurity frameworks, ISO 2013; NIST 2020. The Norwegian regulation of security and contingency of the power supply system covers requirements following these frameworks.

This paper discusses how statutory regulation and audits have pushed the implementation of cybersecurity controls, with the specific example of detection systems.

The first section introduces the background and research question.

Section two presents the state of the art regarding auditing and incident detection effectiveness in Industrial Control Systems (ICS).

Section three describes the methodology; section four presents the findings, section five discusses, and section six summarizes the conclusion.

2. The State of the Art

2.1. *The regulation of cybersecurity in the Norwegian energy sector*

The Norwegian electric energy sector is mainly hydro-based, with 90% of the electric generation being hydropower, 7% is wind power, and total electric energy production was 153,2 TWh in 2020. "Electricity production in Norway" 2021. The energy generation is distributed on 1682 hydropower plants and 60 wind farms and delivered to Norwegian consumers through 353 441 km of the electric grid. Norwegian household energy consumption is electricity-based, with bio-fuel (firewood) and district heating being the leading alternatives.

The Norwegian Energy Act, OED 1990, covers contingency requirements applicable to the Norwegian electric power and district heating market. The law delegates the responsibility to develop and maintain contingency regulations to the Norwegian Water Resources and Energy Directorate

(NVE). NVE is also in charge of supervising the power sector's compliance with the statutory contingency requirements. Norway has enforced security regulation for electric utilities since 1948, OED 1948, with specific cybersecurity requirements since 2003, OED 2002. This was further detailed in 2013, OED 2012, with specific cybersecurity regulations covering requirements for prevention, detection, response, and recovery controls for ICS. The last expansion of the regulation came in 2019, OED 2018, which expanded the cybersecurity requirements to apply to all digital information systems owned and operated by energy utilities.

New guidelines for the contingency regulation came in 2020, and these guidelines reference international standards, like ISO/IEC 27000 and IEC 62443. ISO/IEC 27000 is a series of international standards covering information security, where the most known standard has requirements for establishing, implementing, and maintaining an information security management system (ISMS). IEC 62443 is a series of standards covering cybersecurity in automation and control systems. IEC 62443 is rewritten to work well alongside the ISO/IEC 27000 series.

The regulation and ISO/IEC 27000 and IEC 62443 cover detailed requirements for monitoring digital information systems for intrusions or attacks.

2.2. *Intrusion detection in industrial control systems (ICS)*

Intrusion detection systems are digital systems designed to collect and analyze data from a digital system to detect and alert on possible intrusions or attacks.

Such systems need to be adjusted to work well in ICSs. Although ICSs have some common features with normal IT systems, there are key differences that need to be accounted for, Knapp and Langill 2014. Examples of differences are the need for real-time communication, a larger ratio of embedded systems, and direct control of physical processes.

Retrospectively, the first studies on intrusion detection systems for ICS were published in 2003,

Storm, Hagen, and Arntzen Toftegaard 2021. Zhu, Joseph, and Sastry 2011 surveyed nine proposed detection systems for ICS and found that the intrusion detection technology was immature and that there was a need to empirically ground further research. This view was further supported by later reviews, Mitchell and Chen 2014; Hu et al. 2018.

Storm, Hagen, and Arntzen Toftegaard 2021 reviewed 239 papers on intrusion detection in ICS and concluded that while most proposed detection systems addressed the specific features of ICSs, most of the research had never been tested in live testbeds or in real production environments. While there existed commercial intrusion detection systems targeting ICSs, the research suggested that intrusion detection for ICS was still in the early stages of implementation.

2.3. Effect of audits on regulatory compliance

Governments issue a regulation and enforce regulated units to be compliant with practice detailed rules. Compliance is checked using internal or external audits or inspections. In our research, we have only found a small body of knowledge on research into the effects of regulation and governmental audits, and these studies do not cover energy and cybersecurity. There might, however, be some takeaways from other applications.

Askim et al. 2013 found that audits improved compliance; however, the lack of resources set aside for correcting findings from the audit report led to low internalization in organizations under audit. Husabø et al. 2020 evaluated the effects of external inspections on clinical care. They found significant improvements in the proportion of patients examined and issues detected after external inspections.

Research into the effect of Occupational Safety and Health Administration (OSHA) inspections showed that inspections generally had a deterrent effect, Gray and Scholz 1993.

Internal audits have been studied by several researchers. A study of 108 Israeli organizations documented that support from top management was the main determinant of internal audit effectiveness, with some impact from the organiza-

tional independence of the internal audit team had an impact, Cohen and Sayag 2010.

Research on external audits' impact on quality assurance in universities in Australia found that while external audits improved systems and processes in the audited universities, audits had not necessarily improved the student experience, Shah 2012. Our literature search provided no studies on the effectiveness of cybersecurity regulation in the energy sector.

3. Method

In this study, we apply an exploratory research strategy. The study is based on three primary sources of data, a 2021 Norwegian national survey on the state of cybersecurity within the Norwegian electric utilities, Tøien et al. 2021, results from on-site audits of Norwegian grid companies from 2015-2021, and results from a 2015 audit of the largest grid companies in Norway. The scope of the study is compliance with the Norwegian cybersecurity regulation for electric utilities and includes questions addressing intrusion detection in ICS.

The 2021 survey was conducted to measure the state of cybersecurity in Norwegian electric utilities. Every company within the Norwegian electric power sector was invited to participate. Out of about 300 companies, 117 responded and filled out a questionnaire on implementing cybersecurity measures.

NVE conducted the 2015 audits to check compliance with the detailed cybersecurity requirements that went into force in 2013. The 2015 audit covered the 30 largest grid companies in Norway. NVE conducted the audit as a survey where the companies were required to answer twelve questions corresponding to specific statutory cybersecurity requirements. Companies received an audit report. They were given a deadline of three months to reply and explain ways to get compliant with the requirements. Every audited company complied by the end of 2016.

NVE conducted six on-site audits on ICS from 2015 until 2016 in grid companies that had previously reported compliance. The on-site audits validated compliance in practice by asking more

detailed questions.

After gathering the data, we extracted the answers to questions focusing on monitoring and detection and used these to compare the two datasets. Data were furthermore sorted according to company size where applicable.

Studying changes over time is challenging due to restructuring and mergers during the ten years. We did manage to link most companies due to the unique organization number. Another weakness is the few observations. However, the observations represent the most important grid companies in the sector. The 30 grid companies represent one-third of all grid companies in Norway and include every large grid company.

4. Results

Figure 1 shows the use of detection or monitoring for intrusions or attacks in ICS for the grid companies included in the 2015 audit, the on-site audits, and the survey.

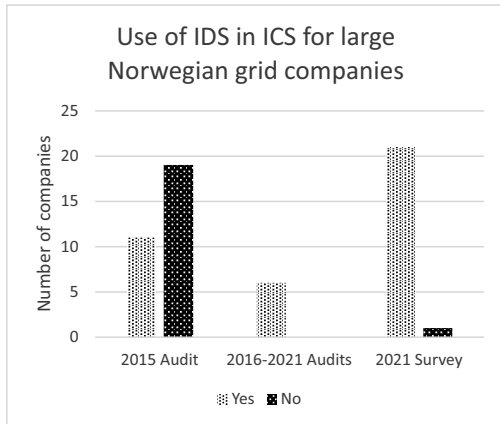


Fig. 1. The use of intrusion detection systems (IDS) in ICS for large Norwegian grid companies from 2015 until 2021.

The 2015 audit revealed that 19 grid owners were in non-compliance with the requirements on intrusion detection in ICS, and 16 grid companies were in non-compliance with registering all security breaches.

All the six on-site audits from 2015 to 2021 found that the companies complied with the in-

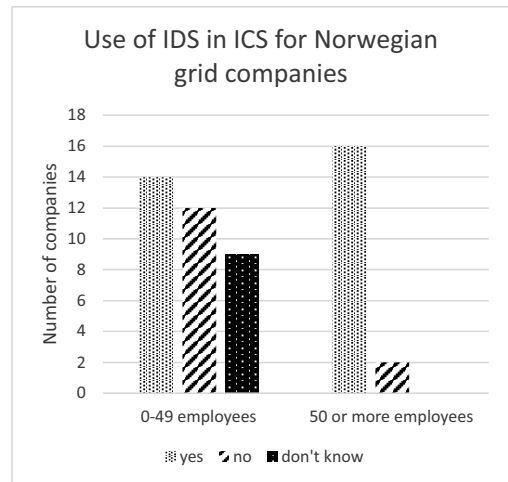


Fig. 2. The use of intrusion detection systems (IDS) in ICS for Norwegian grid companies according to a 2021 survey.

trusion detection requirements.

Out of the 30 companies in the 2015 audits, 22 answered the 2021 survey. Every grid company that was uncompliant in the 2015 audits answered that they had implemented an intrusion detection system in their ICS. One company that had been compliant with the requirements in the 2015 audit now answered that they did not have an intrusion detection system in their ICS.

The 2021 survey includes answers from 117 energy utilities, including 53 grid companies. Figure 2 shows the answers to the question on the use of intrusion detection in ICS, split by company size. We have chosen to split at 50 employees, as this matches the requirements that apply to the companies. Of the 35 grid companies with less than 50 employees, 14 answered that they had intrusion detection systems in their ICS, 12 answered no, and nine did not know. Of the 18 grid companies with more than 50 employees, 16 answered yes, and two answered no.

5. Discussion

The study shows that after two years of enforced detailed cybersecurity regulation on intrusion detection in ICS, most of the audited grid companies were not compliant. During these two years, NVE executed multiple informational events to

inform the companies under regulation about the requirements and how to comply. All six grid companies complied with the requirements in the on-site audits in the years after the 2015 audit. This suggests that regulation without audits has little effect, even when companies have access to extended information about the regulation and how to comply.

Comparing the 23 companies audited in 2015 and participating in the 2021 survey shows that they comply with the regulation six years after the 2015 audit. This result follows earlier research in other sectors that shows that audits and inspections increase compliance, Askim et al. 2013; Husabø et al. 2020; Gray and Scholz 1993. Auditors from NVE experience that management participates in on-site auditing meetings and are also engaged in the follow-up work after auditing. Studies show that management commitment is a driving force for compliance, Cohen and Sayag 2010.

While higher compliance is an improvement, it does not explain how the companies have handled the immaturity of IDS in ICSStorm, Hagen, and Arntzen Toftegaard 2021. One explanation is that the regulation requires detection but does not specify ICS-specific tools. Grid companies could then use an IT-system-based IDS and still be compliant. NVE should investigate the capabilities of installed IDSs and evaluate if IT-system-based IDSs are adequate or if they are used as compliance for compliance's sake.

The results from the 2021 survey show that while larger grid companies mostly comply with the requirements for intrusion detection in ICS, a significantly lower number of smaller grid companies do. We believe that multiple facts can explain this:

- (1) Smaller grid companies have less detailed requirements for implementing intrusion detection in their ICS, as their power lines, substations, and power plants are of lower importance to the energy system.
- (2) Smaller companies were not audited in 2015.
- (3) Smaller companies might have a lower level of cybersecurity maturity and fewer human

and financial resources, which hinders higher-level hardware and software analytics.

6. Conclusion

Prescriptive statutory requirements to detect intrusions in ICS came into force in Norway by January 2013. Two years later, in 2015, NVE conducted an audit of the 30 most important grid companies. The audit revealed that intrusion detection capabilities were missing among most audited companies. NVE followed up with all audited grid companies until they were compliant, and the following on-site audits did not reveal any noncompliance.

In June 2021, NVE conducted another survey, now covering energy utilities of all sizes. The results showed a significant improvement in intrusion detection capabilities. 89% of large and medium-sized grid companies monitored data network traffic in their ICS compared to 40% of smaller grid companies. The implementation level seems to have stayed high after the audits in 2015, and we believe that audits contribute to compliance. For smaller companies that have not been audited, we observe a lower level of compliance, which suggests that regulation without audits seems to have less effect. We plan to conduct another survey in a few years after NVE has audited smaller grid companies on the use of intrusion detection to test this hypothesis.

We want to remark that the increased adoption of logging and detection systems is not just a question of regulation, audits, and compliance with statutory requirements but also about cybersecurity maturity in the security market and the power industry, a development unfortunately pushed by an increased amount and sophistication of cyberattacks. Based on this observation, we would claim that it is vital for regulators to understand technology and business trends and update requirements accordingly.

Acknowledgement

We would like to thank the Norwegian Water Resources and Energy Directorate (NVE) for funding this study. We would also thank Head engineer Helge Ulsberg and Head engineer Amir Zaki Mesiha at NVE for comments. We would also thank the ESREL2022 reviewers

for excellent feedback.

References

- Askim, Jostein, Harald Baldersheim, Jan Erling Klausen, Helge Renå, Eivind Smith, and Hilde Hatleskog Zeiner. 2013. *Hvordan påvirker det statlige tilsynet kommunene og det lokale selvstyret?* <https://hdl.handle.net/20.500.12199/5474>.
- Cohen, Aaron, and Gabriel Sayag. 2010. "The Effectiveness of Internal Auditing: An Empirical Examination of its Determinants in Israeli Organisations" [in eng]. *Australian accounting review* (Melbourne, Australia) 20 (3): 296–307. ISSN: 1035-6908.
- "Electricity production in Norway." 2021. Norwegian Ministry of Petroleum and Energy, May. Website. Accessed March 29, 2022. <https://energifaktanorge.no/en/norsk-energiforsyning/kraftproduksjon/>.
- Gray, Wayne B., and John T. Scholz. 1993. "Does Regulatory Enforcement Work? A Panel Analysis of OSHA Enforcement" [in eng]. *Law & society review* (Beverly Hills, Calif) 27 (1): 177–213. ISSN: 0023-9216.
- Hu, Yan, An Yang, Hong Li, Yuyan Sun, and Limin Sun. 2018. "A survey of intrusion detection on industrial control systems" [in eng]. *International journal of distributed sensor networks* (London, England) 14 (8): 155014771879461. ISSN: 1550-1477.
- Husabø, Gunnar, Roy Miodini Nilsen, Erik Solligård, Hans Kristian Flaatten, Kieran Walshe, Jan C Frich, Gunnar Tschudi Bondevik, et al. 2020. "Effects of external inspections on sepsis detection and treatment: a stepped-wedge study with cluster-level randomisation" [in eng ; nor]. *BMJ open* (LONDON), Original research, 10 (10): e037715–e037715. ISSN: 2044-6055.
- ISO. 2013. *Information technology — Security techniques — Information security management systems — Requirements*. Standard. Geneva, CH: International Organization for Standardization, October.
- Knapp, Eric D., and Joel Langill. 2014. *Industrial Network Security, 2nd Edition* [in eng]. Syngress. ISBN: 9780124201149.
- Lee, Robert M., Michael J. Assante, and Tim Conway. 2016. *Analysis of the cyber attack on the Ukrainian power grid*. Technical report. Washington DC, USA: Electricity Information Sharing and Analysis Center (E-ISAC).
- Mitchell, Robert, and Ing-Ray Chen. 2014. "A survey of intrusion detection techniques for cyber-physical systems" [in eng]. *ACM computing surveys* 46 (4): 1–29. ISSN: 0360-0300.
- NIST. 2020. *Security and Privacy Controls for Information Systems and Organizations*. Standard. Gaithersburg, USA: National Institute of Standards and Technology, September.
- OED. 1948. *Lov om forsvarsmessig sikring av kraftforsyningen*. Norway. <https://lovdata.no/dokument/NLO/lov/1948-06-25-8>.
- . 1990. *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)*. Norway. <https://lovdata.no/dokument/NL/lov/1990-06-29-50>.
- . 2002. *Forskrift om beredskap i kraftforsyningen*. Norway. <https://lovdata.no/dokument/SFO/forskrift/2002-12-16-1606>.
- . 2012. *Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)*. Norway. <https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157>.
- . 2018. *Forskrift om endring i forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften)*. Norway. <https://lovdata.no/dokument/LTI/forskrift/2018-11-01-1641>.
- Shah, Mahsood. 2012. "Ten years of external quality audit in Australia: evaluating its effectiveness and success" [in eng]. *Assessment and evaluation in higher education* (Abingdon) 37 (6): 761–772. ISSN: 0260-2938.
- Storm, Jon-Martin, Janne Hagen, and Øyvind Anders Arntzen Toftegaard. 2021. "A Survey of Using Process Data and Features of Industrial Control Systems in Intrusion Detection." In *2021 IEEE International Conference on Big Data (Big Data)*, 2170–2177. <https://doi.org/10.1109/BigData52589.2021.9671325>.

- Tøien, Fredrik Karlsen, Johannes Fagermyr, Glora Treider, and Hanna Remvang. 2021. *IKT-sikkerhetstilstanden i kraftforsyningen 2021*. Technical report. Oslo. https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf.
- Zhu, Bonnie, A Joseph, and S Sastry. 2011. "A Taxonomy of Cyber Attacks on SCADA Systems" [in eng]. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 380–388. IEEE. ISBN: 9781457719769.