Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P588-cd

Lessons learned from performing cyber-security research on critical infrastructures.

John Eidar Simensen

Security and Risk, Institute for Energy Technology, Norway. E-mail: John.Eidar.Simensen@ife.no

Aleksander Lygren Toppe

Security and Risk, Institute for Energy Technology, Norway. E-mail: Aleksander.Lygren.Toppe@ife.no

Per-Arne Jørgensen

Security and Risk, Institute for Energy Technology, Norway. E-mail: Per.Arne.Jorgensen@ife.no

The last 5 years has marked a paradigm shift when it comes to focus and awareness on cyber security across industries. In Norway this has been strongly motivated by governmental influence through updated rules and regulations. One initiative addressing cyber challenges has been the 4-year cyber research program CybWin (2019-2022) which has had a holistic, practical approach to cyber security of Norwegian critical infrastructures. A cyber security centre (CSC) research infrastructure was established at the Institute for Energy Technology in Norway. The infrastructure was developed iteratively with the needs of increasingly developing cyber research requirements of CybWin, resulting in capabilities to perform controlled cyber-attack experiments on TRL9 system enclaves in Air Traffic Management and Energy grid control systems. The paper presents experiences from cyber research in the CSC in the period 2019-2022 covering technical aspects of the centre, experimental lessons learned regarding target stakeholders such as red-team and blue-team with regards to research focus and experiment fidelity. The experience from performed research indicates a strong need for access to expertise in information technology and operational technology systems and operations, cyber-attack and cyber defence competence, human factors knowledge and experimental research competence for complex systems.

Keywords: Cyber security, critical infrastructure, cyber infrastructure, operational safety & security, cyber attack

1. Introduction

The last years have marked a paradigm shift when it comes to the focus and awareness on cyber security across industries, heavily triggered by events such as the cyber-attacks on the 2015 Ukraine power grid (Lee et. al. 2015) (Cherepanov and Lipovsky 2016), and the malware attacks on Norwegian Hydro in 2019 to name some. In Norway, this shift is partially motivated by governmental influence with updated rules and regulations (NorGov 2019). Security and cyber-security as topical areas have brought challenges when integrating with safety, as discussed in (Simensen and Gran 2021). Currently, the European Union NIS2 directive (NIS 2023) is being either prepared for or gradually implemented in the EU, providing a set of minimum requirements for both critical infrastructure owners, as well as for critical service providers with regards to e.g., supply chains, maintenance, monitoring and response, and the use of crypto with regards to cyber security. When written into law it is expected (NorGov 2021) the NIS2 directive requirements will mean both increasing costs in compliance activities as well as in enforcement efforts for both governments and public and private companies subject to NIS2. It is expected that this will have a negative impact on the availability of cyber security professionals, which is already found lacking by 3.4 million globally in 2022 (ICS2 2022). A way to support and strengthen both industry and society in addressing cyber security is public research projects nationally and internationally through e.g., EU projects. One initiative addressing cyber challenges has been the 4-year cyber research program CybWin (2019-2022) which has had a holistic, practical approach to cyber security of Norwegian critical infrastructures (CI). The project produced a Cyber

Security Centre infrastructure (Katta et. al. 2019) consisting of a technical platform for performing cyber security research, supported with multi-domain competence enabling holistic approaches. Moreover, the project performed cyber research on several CI systems, resulting in both up- and downstream cyber security results, new approaches as well as product improvements. Previous reporting and publications on the project have included the organization, setup and challenges concerning laboratory infrastructure and how experiments were conducted (Simensen et. al. 2022), knowledge and training need for critical infrastructure stakeholders, and recent lessons learned from performing realistic cyber exercises on CI with licensed operators (Gran et. al. 2023).

This paper is organised as follows: Chapter 2 presents a background for the work including the CybWin project and an introduction to the technical laboratory infrastructure, as well as use cases and experiments performed on cyber security. Chapter 3 provides observations and experiences concerning both technical and practical challenges when performing cyber security research experiments. In chapter 4, we discuss main experiences on human, technological and organisational factors on cyber security last five years with regards to improving the facilities and research capabilities. Summary and next steps can be found in chapter 5.

2. Background

A motivation for the *Cybersecurity Platform for Assessment and Training for Critical Infrastructures – Legacy to Digital Twin* project (Cybwin 2018) was the unavailability of cyber ranges, cyber security infrastructures and systems, and relevant cyber security data sets pertaining to CI. An updated survey (Conti et. al. 2021) provides an overview of existing systems and infrastructures for cyber research and highlights both variability in types and size of data sets available as well as system and infrastructure realism. It is the same experience that motivated the establishment of the cyber security centre (CSC) research infrastructure at the Institute for Energy Technology in Norway.

The CSC was developed iteratively with the needs of increasingly developing cyber research requirements of CybWin, resulting in capabilities to perform controlled cyber-attack experiments on TRL9 system enclaves in both Air Traffic Management and Energy Grid systems.

2.1. *CSC infrastructure*

The CSC infrastructure is specifically constructed for hardware in the loop systems, supporting both information technology (IT) systems and operational technology (OT) systems such as e.g., PLC-based systems. Built as a separate (air-gapped) technology stack, the CSC provides a full technical infrastructure stack to support cyber security research without either affecting or being affected by the systems of the organization. In practice, this allows more freedom when configuring systems to achieve the functionality needed, as well as supporting a broader range of adaptable security functions to both enable research and protect systems. The CSC is, like many cyber ranges, based on design in depth principles (Figure 1).

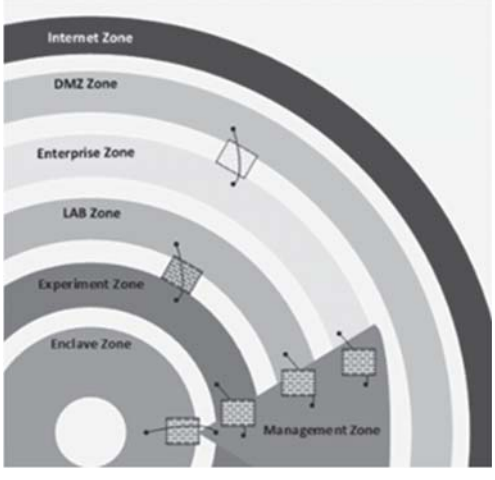

Fig. 1. SANS Design-in-depth principles. Source: Infrastructure Security Architecture for Effective Security Monitoring, SANS, 2015.

In the CSC the laboratory zone is configured as a large-scale segmented enterprise network and the experiment network is configured as a semi-hardened IT/OT landscape with multiple network segments on both IT and OT sides. Each system under consideration is placed within its own testbed architecture configured to the individual need of the specific experiment. VLANs are used extensively to divide internet DMZs. Extranets, intranets and the different management networks

and multiple BSD-software firewalls provide filtering with stateful inspection and routing. A more detailed overview of the CSC infrastructure including enclaves can be found (Jørgensen et. al. 2022). The CSC has had several different enclave systems such as 1. a nuclear turbine pressure control system with PLC and field devices from ABB, 2. An air traffic management surveillance tracker system, 3. an energy digital power grid distribution control system (Digital Station), 4. An Industry 4.0 Fischer Technik factory system controlled by a Siemens Simatic S7-1500 PLC. In addition, the CSC provides a penetration testing and backup operation facility for the Security Operation Centre services.

2.2. *Digital Station use-case*

The Digital Station (DS) infrastructure performs the function of down-voltage operation in the Norwegian electricity grid. The DS is owned and operated by the Norwegian power grid system operator Statnett, is considered CI, and consists of digital instrumentation and control systems, communication protocols and network infrastructure as described in (IEC 2009, 2013, 2020). The DS provides a highly relevant Technological Readiness Level (TRL) 9 system for cyber security research – which in turn provided valuable requirements to the CSC infrastructure and operation. For more detail on the DS components and performed experiments see (Simensen et. al. 2022).

2.3. *Aviation use-case*

The Air traffic management surveillance tracker and server (ARTAS) system is a "*European-wide distributed Surveillance Data Processing System offered by EUROCONTROL that is capable of processing surveillance data reports from classical radar, Mode-S, WAM and ADS, providing its Users with the best possible real-time air traffic situation, with a high level of accuracy and reliability.*" (ARTAS 2023). ARTAS comprises software and hardware components and takes as input a range of data and signals from e.g., radar sources to calculate and present air situation data to air traffic controllers. The same enclave concept was provided for the ARTAS system in CSC, following EUROCONTROL guidance on HW setup, and by configuring ARTAS in the same way of a participating European Air Navigation Service Provider, realistic operational traffic data sets could be employed for a realistic hardware and software behaviour, thereby providing realistic system cyber behaviour for human operators. Where the DS comprised full stack IT and OT components, ARTAS setup comprised more traditional IT hardware and software and OT and sensor side behaviour was provided in the form of input data streams in such a way that they could be manipulated. A detailed overview on air traffic management architecture and supply chain cyber security challenges can be found in (de Haan 2020).

2.4. C*yber experiments in the CSC*

The CSC has hosted different sets of technical cyber security experiments as well as in conjunction with the Hammlab (HAMMLAB 2022) (Skjerve and Bye 2011) performed operator targeted cyber security experiments in nuclear. The approach has thus far consisted of first performing 1. Cyber security attacks on respective systems to identify the attack effects and system behaviours (Erdődi et. al. 2022), and based on the 'successes', either the attacks have been improved, vulnerabilities have been patched, or the laboratory infrastructure has received new functionality to better support research. When there is a confidence that the observed cyber behaviour is realistic, and the experiment when repeated yields the same results, then 2. the system behaviour is replicated in experiments investigating operator performance and understanding (Nystad et. al. 2021) (Nystad et. al. 2020). Experiences from these experiments have motivated the industry to apply a similar approach internally and e.g., in Q4 2022 EUROCONTROL implemented cyber-scenarios in their full-scale Air Traffic Control simulators as a step to better understand operator behaviour and provide training. In addition, the lessons learned from the CybWin project are used to design realistic system behaviours within nuclear cyber research performed in the OECD NEA Halden HTO project.

3. Observed and experienced challenges

The CSC infrastructure has so far been geared towards performing technical cyber-attack tests and experiments. As experiments were performed and improvements made to either the

enclaves/use-cases or the laboratory infrastructure, the system complexity and the resource loads reached a point of congestion. For example, with the use of several Incident Detection Systems (IDS) in parallel simultaneously, there are challenges with potential cross-IDS effects and with the different Security Information and Event Management (SIEM) systems struggling to handle all recorded data. The different performed cyber experiments have identified both generic and specific challenges which are reported on in the following.

3.1. *General technical challenges*

The following presents experienced technical challenges with the CSC infrastructure.

3.1.1 Mixed virtual-physical infrastructure, network data flow and monitoring

The monitoring/IDS infrastructure for an enclave was required to support hybrid hardware and virtualized environment, including networking, as well as itself being a mix of both hardware and virtualized. Attacks were initiated both from the virtualized infrastructure connected to virtual switches, as well as physical machines connected to physical enclave switches.

The type of network traffic that is observed in OT environments is often of a "local" multicast or broadcast variant including link layer protocols. Careful setup of both the virtual and physical network and computer infrastructure is required to ensure that all the IDS solutions have access to identical data, but also that the attackers in the network can see and 'affect' the correct traffic. Some attack scenarios cannot easily be virtualized and require physical connectivity to a local switch. IDS systems either work with network TAP traffic or data from individual hosts by a host agent.

The mixed hardware and virtual infrastructures meant that we had to feed network mirror data from the physical hardware into the virtual infrastructure for the virtual software-based IDS, and at the same time also do the opposite to ensure that all the traffic from the virtual switches would reach the physical IDSs systems.

VMWare ESXI has two switch types, standalone and distributed, and as we were using the former, we needed to enable promiscuous functionality on the switch level, and then use port groups on the same VLAN to restrict promiscuous access for types of machines on the same subnet/vlan. Physical switches were configured with Remote SPAN ports to ensure that all data were available for both the physical and virtualized IDS. A monitoring session using the SPAN functionality is a limited resource on a switch, especially for remote sessions. Remote SPAN functionality is also a vendor specific implementation, meaning that a RSPAN session on Cisco will not be able to deliver data to a HP/Aruba switch. We addressed this in the hardware-in-the-loop part of the enclave by utilizing an aggregation of mirror ports, and utilizing physical network taps, such as Shark Tap, to duplicate traffic streams.

3.1.2. *Cross IDS traffic contamination - Host agent network traffic*

Multiple IDS systems in a network mean that the laboratory setup is vulnerable to one IDSs traffic being picked up by another, and in the case of behaviour/learning based IDSs, their training might be affected and conditional on the behaviour of other IDS in the network. This is caused by clients in the network with an IDS host agent, resulting in a data stream being sent over the network from that client to the central receiving endpoint for the IDS. This was mitigated by sending all such data to a specific monitoring/IDS-subnet, meaning traffic was easier to filter in each IDS, but also where applicable, clients were dual-homed in both their respective LAN and an "out of band" monitoring LAN to eliminate traffic contamination. Physical IDSs also require a management machine or a central server, and traffic between these was also VLAN isolated to reduce contamination impact.

3.1.3. *Attack types and the impact to the IDS infrastructure*

The attacks performed, ranged from generic attacks on various infrastructure parts, to sophisticated man-in-the-middle protocol implementation attacks. Very high bandwidth and/or packet per second DoS attacks could manage to saturate the monitoring session bandwidth in the network, but this was seen as acceptable as these types of attacks were done controlled. Some higher sophistication attacks were also run over multiple weeks, putting higher

stress on packet capture logs, IDS storage systems, and experimental operational procedures.

3.2. *Stakeholder roles and experiment fidelity*

As mentioned in section 2.4, the blue teams have had a passive function in performed experiments in the CSC, ensuring correct sampling of data for the purpose of after-attack analysis. The red teams have had more active roles, but as there has been no active blue team there are unexplored adversary potentials for future experiments.

3.2.1. *Red team (attackers)*

In all performed attacks in the CSC the red team has been provided with a point of access, such as a compromised computer in different parts of the network. The argument has been that a hacker will find a way in through compromised, unpatched, or e.g., zero-day exploits. As an example, in experiments performed on the DS, the red team had access to a computer on the same network as the system targeted for attack in one case.

Through different projects in the CSC a returning discussion has been the realism in this approach versus the attacks starting from the 'outside' and working through the 7 steps of the kill chain to gain the necessary rights and accesses. As mentioned, the red team has consequently not had to plan for an active cyber security event response action, i.e., an active security operations centre or blue team.

3.2.2. *Blue team (defence)*

In performed experiments the blue team has had a passive role, i.e., monitoring the output and performance of IDS and ensuring that logging and data gathering performs as planned to have necessary data for performing post-experiment analysis. In the earliest experiments, this made sense as the goal was to identify system cyber behaviour under successful attack conditions. Moreover, the configuration of the defence side in the CSC, as well as the tools and expertise level available for proper cyber security response, were not mature enough to warrant an active blue team role or Security Operation Centre function.

3.2.3. *Safety operator performance*

No operator performance research has been performed solely in the CSC. Instead, the CSC has been connected to the HAMMLAB [HAMMLAB 2022] nuclear control room simulator where safety operators have been subjected to scenarios showing digital instrumentation and control systems under cyber behaviour (Nystad et. Al. 2020). In such scenarios the CSC has represented a SOC function, albeit in all research performed thus far, the SOC function has been scripted and part of the scenario. The reasons for this are the same as for the blue team functionality, as provided in section 3.2.2. Additionally, the complexity of the dynamics increases when there is more than one "target" role which again poses several challenges to both how experiments are controlled and to the validity of results.

In previous CybWin research (Nystad et. al. 2021), a more low-fidelity approach was chosen for subjecting Air Traffic Controller Officers (ATCOs) to systems under cyber-attack behaviour. Here, a combination of still pictures showing the situation data display radar screen in a linear time evolving scenario was used in combination with pseudo-pilots providing answers to questions from the ATCOs. The goal of the research was to find at which point the ATCOs were able to identify that the experienced system behaviour was instigated by a cyber-attack. For the participating ATCOs, at the time of the experiment, they did not distinguish between different types of technical support available, hence cyber response and technical event resolution were out of scope.

3.2.4. *Security operator performance*

Experiments performed in the CSC have mostly been run with fully enclosed enclaves with all their support systems contained, including IDS systems and SIEM solutions. Operator performance research has mostly focussed on the safety operator. To expand research focus towards the security operator, the CSC has acquired additional hardware to securely extend the enclaves with SOC enabling solutions, both shared and instanced per enclave.

In cases where the SOC analyst role has been a part of existing experiments, their work environment has been very limited. To expand this role, exploration is done on incident response systems such as Malcolm from INL and CISA (INL 2023) and vulnerability management solutions such as (Greenbone 2023). The goal is to streamline work to support the SOC analysis to

perform their response function during experiments. E.g., Malcom also supports working with offline captured data, allowing for more direct repeatable experiments on the security operator roles. Supporting tools for SOC activities such as Threat Intelligence, Vulnerability management, assessment, and threat hunting, are also planned to be provided by default for an experiment enclave requiring SOC functionality.

4. Discussion

This chapter discusses some main experiences on human, technological and organisational factors on cyber security last 5 years.

4.1. *Research relevance and validity*

The two main use cases/enclaves referred to in this paper are current real CI established systems that are in use in the power grid and in air traffic management respectively. Observed system behaviours under cyber conditions have been considered realistic by participating system experts and with regards to the probability of attack types, successful malicious attacks of the same archetypes have occurred on several occasions on similar systems. When comparing to the cyber security data and infrastructure overview provided in (Conti et. al. 2021), we argue that the two use cases referred to in this paper are amongst the most realistic and advanced systems available for cyber research today. Despite that, the use cases have not yet been applied to their full research potential. In the future it is a goal to run real-time attack/defence exercises exploring both technical aspects together with operator performance.

4.2. *Supporting active response roles*

The main goal of current technical upgrades of the CSC is to better provide the capability to have an active response stakeholder. Section 3.2.4 describes supporting hardware and software for the SOC roles, and this set of open-source solutions functions as a SOC software template, enabling us to verify complete system functionality and ease integration with commercial solutions. The SOC analyst role is provided improved tools for handling live incidents, and threat hunting with intrusion prevention capabilities. The Security engineer can then use the reference SOC software template that can be adjusted to test different vendors or configuration impacts.

4.3. *Expanding on experiment complexity*

The HAMMLAB facility has through more than three decades provided controlled experiment research utilizing state of the art simulators in different domains (Skjerve and Bye 2011). The simulators currently in use provides not only the functionality of the plant or process they simulate, but also additional functionality such as the ability to simulate non-trivial equipment behaviour and scenarios beyond what is covered by standardised training scenarios. In addition, the use of licensed operators in both the HAMMLAB organising staff and in invited crews adds to the realism of scenarios and quality of results.

For the CSC, the long-term ambition has been to provide the capabilities to support advanced, realistic scenarios, controlled research experiments where the CSC enables cyber operators, and where the technical capability of the CSC supports integration and collaboration of remote simulator facilities such as the HAMMLAB to provide e.g., safety operators. To support this there is a need for supporting more non-scripted roles or stakeholders in scenarios. To mitigate increased dynamics, experiments need better planning, operator procedures must be established and/or refined, and facility staff need experience in running different types of experiments and scenarios. In addition, the technical systems available to the cyber operators need further refinement, e.g., more developed responses such as better trained IDS, automated response functionality, improved system behaviour estimations (models) etc.

4.4. *Involving stakeholders and systems in research*

Three prevalent challenges experienced regarding security and cyber security research are 1. availability of realistic use cases, 2. availability of experts, and 3. the overall willingness to share information. The lack of availability of real-world realistic CI use cases can be attributed to the sensitivity of the CI and a concern that information about the CI might be exploited. The availability of OT and process experts, as well as cyber competence, is a challenge for the industry with regards to costs and regarding prioritizing critical activities over research. Given the current

lack of experts combined with an increasing focus on cyber in industry, this challenges academia to change their approach to accommodate this reality.

Based on cyber experiments focussed on safety operators e.g., (Nystad et. al 2021) (Nystad et. al. 2022), we believe that current cyber security training and exercises should be targeted on operational system behaviour under cyber conditions. Today, cyber security training often focuses on IT-system threats such as phishing and virus emails. As reported in (Chowdhury 2022), training and awareness activities in the industry demonstrate limitations in both methods employed and contents of cyber training. To develop realistic and relevant cyber training for the operational side of CI, a practical approach supported by sufficient expertise is needed. We believe that research should pivot more towards the practical, addressing industry challenges in practical research and producing tangible results supporting and benefitting industry directly.

Lastly, the 'tradition' of not sharing security information, is as argued in (Simensen and Gran 2021) particularly challenging CI security, adding negatively to the overall risk of a system or solution. It is the authors experience that the criticality of the CI use cases motivate caution, and limiting both the people with access and each individual role or person has access to is often the starting requirement from the asset owners. In the work reported in this paper, a mix of competencies were needed, which meant participation of experts with different expertise, different backgrounds and nationalities, representing different companies and interests. In CybWin, use cases were treated as separate 'projects' with regards to access policies, personal non-disclosure agreements for involved participants, and technical platform for information exchange to name some. Before performing experiments on CI with e.g., remote connections, asset owner would approve activities based on either a risk assessment or a detailed description of sufficient security mechanisms and activated barriers. Ensuring and demonstrating the safe keeping of both assets and belonging information is the most important requirement from system and asset owners in general, and when adding cyber security research on these systems only adds more constraints.

5. Summary and conclusion

The paper has presented the IFE Cyber Security Centre, including the technical infrastructure, the main use cases employed, and the types of cyber security research and overall results achieved. Reported results cyber security research in the facility demonstrates that the CSC supports controlled experiments on real life CI. However, until now it has been capable to only have one stakeholder type (e.g., safety operator) having full freedom of operation at a time.

We have reported on recent and upcoming technical upgrades to the CSC, which shall support research with several non-scripted stakeholders participating in realistic scenarios simultaneously and provided experiences and suggestions on aspects concerning user and stakeholder involvement to foster cyber security research on real CI.

A recurring experience through the reported work has been the dependence on expertise and experience from industry, specialist knowledge on cyber security, technical knowledge and research competence, and support and trust from industry to allow for realistic and relevant cyber security research benefitting industry.

Acknowledgement

We acknowledge the work and support of the CybWin partners, in particular the provisioning of real-world CI, and providing access to licensed operators and specialist experience. CybWin was funded by Norwegian Research Council grant: 287808.

References

Lee, R. M., Assante, M. J., and Conway, T. (2016) "SANS ICS-analysis of the cyber attack on the Ukrainian power grid", report.

Cherepanov, A., Lipovsky, R. (2016), "Blackenergy– what we really know about the notorious cyber attacks", Virus Bulletin, October.

NorGov (2019), Ministry of Justice and Public Security: "Act relating to national security" and "Regulations relating to the protective security work of undertakings".

Simensen, J.E., Gran, B. A. (2021), "Information- and Cyber-Security Practices as Inhibitors to Digital Safety", in Proceedings of the 31st European Safety and Reliability Conference, 19-23 September 2021, Angers, France.

NIS2 (2023), ENISA – European Union Agency for Cybersecurity, NIS directive, Available: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

NorGov (2021) Norwegian Government – Ministry of justice – notes on the NIS2 directive, available: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/

ISC2 (2022), The Center for Cyber Safety and Education, "CyberSecurity Workforce Study 2022 - A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution", October 2022.

Katta, V., Sechi, F., Jorgensen, P-A., Strand, S., Wiig, P.A., Simensen, J.E. and Houmb, S.H. (2019): Establishing a Cybersecurity Centre for Industrial Control Systems, Proceedings of the 29th European Safety and Reliability Conference Hannover, Germany, 22-26 September 2019.

CybWin (2018) - Norwegian Research Council, project bank: "Cybersecurity Platform for Assessment and Training for Critical Infrastructures – Legacy to Digital Twin", https://prosjektbanken.forskningsradet.no/en/project/FORISS/287808

Conti, M., Doradel, D., Turrin, F. (2021), "A Survey on Industrial Control System Testbeds and Datasets for Security Research", in IEEE Communications Surveys & Tutorials.

Jørgensen, P-A., Waltoft-Olsen, A., Houmb, S. H., Toppe, A. L., Soltvedt, T., Muggerud, H. K. (2022), "Building a Hardware-In-the-Loop (HIL) Digital Energy Station Infrastructure for Cyber Operation Resiliency Testing", EnCryCiS workshop, in proceedings 44th Int. Conference on Software Engineering.

IEC 62443-1-1 (2009), Industrial communication networks - Network and system security, IEC 62443-1-1:2009 ed. International Electrotechnical Commission.

IEC 62443-3-2 (2020), Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design, IEC 62443-3-2 (2020) ed. International Electrotechnical Commission, 2020.

IEC 62443-3-3 (2013), Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, IEC 62443-3-3:2013 ed. International Electrotechnical Commission, 2013.

Simensen, J. E, Jørgensen, P-A, Toppe, A. L. (2022), "Experience from performing controlled technical cyber experiments on Critical Infrastructure as hybrid events", in Proceedings of the 32nd European Safety and Reliability Conference, Dublin, Ireland, 29th Aug-1st September 2022.

Gran, B. A., Simensen, J. E., Jørgensen, P-A., and Nystad, E. (2023), "Lessons Learned from performing Applied Cyber Exercises in Halden", 13th Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC&HMIT).

ARTAS (2023) – EUROCONTROL, Air Traffic management surveillance tracker and server, https://www.eurocontrol.int/product/artas

de Haan, J. (2020), "Specific Air Traffic Management Cybersecurity Challenges – Architecture and Supply Chain", EnCyCris '20, May 25, Seoul, South Korea.

HAMMLAB (2022) "Halden Advanced Man-Machine Laboratory", HAMMLAB laboratory facility, Institute for Energy Technology, accessed May, 2022, https://ife.no/en/laboratory/hammlab/]

Skjerve, A.B. and Bye, A. (2011) (Editors), "*Simulator-based Human Factors Studies Across 25 Years: The History of the Halden Man-Machine Laboratory*", Edition 1, Springer-Verlag London Limited 2011, ISBN 978-0-85729-002-1.

Erdődi, L., Kaliyar, P., Houmb, S. H., Akbarzadeh, A., & Waltoft-Olsen, A. J. (2022). Attacking Power Grid Substations: An Experiment Demonstrating How to Attack the SCADA Protocol IEC 60870-5-104. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-10).

Nystad, E., Simensen, J.E., C. Raspotnig (2021), "Investigating operative cybersecurity awareness in air traffic control", 14th International Conference on Security of Information and Networks, SINCONF 2021.

Nystad, E., Katta, V., Simensen, J. E. (2020), "What happens in a control room during a cybersecurity attack?: Preliminary observations from a pilot study", in ICSEW'20: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops.

INL (2023), Idaho National Labs - Malcolm - A Network Traffic Analysis Tool Suite, https://inl.gov/ics-malcolm/

Greenbone (2023), Greenbone Vulnerability Management, https://www.greenbone.net/en/

Chowdhury, N. et. al. (2022), "Cybersecurity Training in Norwegian Critical Infrastructure Companies", International Journal of Safety and Security Engineering (IJSSE), DOI: 10.18280/ijsse.120304