What happens in a control room during a cybersecurity attack?

Preliminary observations from a pilot study

Espen Nystad*, Vikash Katta, John Eidar Simensen,

Sector Digital Systems
Institute for Energy Technology
Halden, Norway

*espen.nystad@ife.no

ABSTRACT

Cyberattacks on the critical infrastructure is a growing concern for businesses, national authorities and public in general. The increasing complexity and connectivity of the critical infrastructure systems have made them susceptible to cyberattacks. The traditional notion of safety systems being isolated is no longer applicable, as we have seen ample examples on how these systems can be exploited through gaps in e.g. supply chain, physical security, insiders. This places greater importance on how the staff belonging to owners and operators of these critical infrastructure, e.g. operators, IT/security personnel, system engineers, management, are prepared to handle cyberattacks. This paper presents our ongoing research on investigating the preparedness of organisations to handle cybersecurity incidents and providing holistic solutions to improve cybersecurity posture. We present one experiment that has been conducted using our cybersecurity centre and man-machine laboratory to study how operators and security team of a power plant will handle a cyberattack. We highlight the main observations made through this experiment.

CCS CONCEPTS

• Security and privacy → Systems security; • Security and privacy → Human and societal aspects of security and privacy; • Security and privacy → Intrusion/anomaly detection and malware mitigation

KEYWORDS

Cybersecurity, Safety, Critical Infrastructure, Control room, Incident Response, Human factors

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICSEW'20, May 23–29, 2020, Seoul, Republic of Korea

© 2020 Copyright is held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-1-4503-7963-2/20/05...\$15.00

<https://doi.org/10.1145/3387940.3391454>

ACM Reference format:

Espen Nystad, Vikash Katta, John Eidar Simensen, Per Arne Jørgensen, Fabien Sechi, Alexander Lygren Toppe, and Christer Nihlwing. 2020. What happens in a control room during a cybersecurity attack? Preliminary observations from a pilot study. In *Proceedings of International Workshop on Engineering and Cybersecurity of Critical Systems*.

1 Introduction

Across industries there has been immense focus on digitalization of information and processes. This also applies to digitalisation of critical systems – safety, business, mission - where there is a move from analogue to digital systems. This digital transformation introduces new risks that must be understood and managed. With regards to cybersecurity, this transformation creates new, unintended and unknown vulnerabilities and risks. There is a need to ensure that organizations have the necessary capabilities for understanding the entire risk picture and for handling potential cyber threats.

Much research has been done on cybersecurity threats and how to prevent them. A lot less is known about the incident response side of it, and in particular what happens in a control room during a cybersecurity attack. Operators and controllers may in many cases act as the first line in detecting and responding to an attack. But there are challenges preventing the transfer of such knowledge gained from cyberattacks. It can be difficult to run cybersecurity simulations in the actual environment due to resource and security constraints. Organizations that have experience from real cyberattacks may be reluctant to share lessons learned for several reasons, including confidentiality and sensitivity of information.

A cybersecurity centre has been established at Institute for Energy Technology (IFE) with facilities and competence to investigate cybersecurity threats to operational technologies and to evaluate protection mechanisms. IFE also has a control room simulator (HAMMLAB) that is used to study human performance in complex and safety-critical domains. Together these two facilities provide a realistic environment to study how people, process and technology interact and together can provide holistic solutions for handling cybersecurity incidents. The facilities can be set up to simulate a wide range of cybersecurity threats based on hardware or software simulations and can study the incident

response of operators and cybersecurity teams in different domains.

This is a position paper presenting the results from ongoing research at IFE investigating cybersecurity concerns in control rooms of critical infrastructures

1.1 Study approach

The paper describes a pilot study conducted to test the response of a control room team and cybersecurity team on a cybersecurity scenario. The study had an exploratory approach and its objectives were:

- To better understand cybersecurity incidents in a control room setting, how operators react to such an incident, and what challenges need to be addressed regarding incident response.
- To explore the capabilities of IFE's experimental facilities for running cybersecurity studies and provide feedback to future studies.

Main take away is that this paper provides research and industrial community information on how researchers and engineers have employed their experimental facilities to perform realistic cybersecurity scenario-based experiments to investigate cybersecurity issues in a holistic way. One of the main motivations to share early stages of our research with the community is to: discuss the importance of the research problems we are addressing; evaluate the viability of our research approach; elicit suggestions for future work.

Figure 1: The HAMMLAB simulator facility

2 Experimental setup

2.1 Lab setup

The HAMMLAB (Halden man-machine laboratory) is a computer-based full-scope simulator facility (Figure 1). It consists of operator stations with computer displays that can present status and alarm information, and a large overview display for shared situation awareness and at-a-glance status information. The flexible facility can be used to simulate various operational situations from a range of industries. In this pilot study a nuclear power plant simulator of a boiling water reactor (BWR) was used.

An observer's booth allow researchers and observers to monitor scenarios and control simulator events, such as triggering faults in the simulated asset. It also has a broad range of data collection capabilities that support the analysis of operator performance [1].

Figure 2: Cybersecurity Centre

The Cybersecurity Centre (Figure 2) is a physical lab with workstations and large overview displays that can be used to simulate a cybersecurity incident response center. It also contains hardware components (e.g. PLCs) and software simulations that can be used for testing and simulating cybersecurity threats, as well as tools for supporting detection of and response to cybersecurity incidents. In the pilot study the security team in the cybersecurity centre were monitoring the state of the power plant systems and the environment using technical security controls. e.g. intrusion detection tools.

2.2 Participants

A crew of two persons manned the control room simulator. They had the roles of Turbine Operator (TO) and Reactor Operator (RO). The TO was an experienced nuclear power plant operator, the RO was a researcher with training in using the simulator. The TO was unaware of the purpose of the study, while the RO knew that it was a study about a cybersecurity incident but was instructed to act as if he had no knowledge of the scenario. The TO, due to higher experience, naturally took on the role of the more senior operator and made the decisions on what to do in the scenario.

The cybersecurity team placed in the cybersecurity centre consisted of three people. They were researchers and engineers, and all were aware of the nature of the scenario. In their interactions with the control room they acted as if they were unaware.

2.3 Data collection

Audio and video recordings were made of the participants in both the HAMMLAB and the cybersecurity centre. Screenshots of the two most recently accessed screens for each operator were captured three times per second. Process parameters (such as pressure and temperature values) were logged continuously, as well as operator interactions with the simulator, process events and alarms, and the log from the instructor system - in this case showing the progress of the cyberattack script.

3 Results

3.1 Data analysis

A preliminary analysis of the data from the study has been conducted, and this has provided some initial observations. A more thorough analysis remains to be performed. The data was analysed chronologically according to the scenario and a description was made of how the participants responded to the events in the scenario. The focus was on if and how the participants detected that a cyberattack was ongoing, and how they acted to contain the consequences of the attack. The

Fig. 3 Attack scenario description (from [1])

2.4 Scenario

The scenario simulated a man-in-the-middle attack that manipulated data transmitted between the PLC/OPS server and the HMI engineering workstation (see Figure 3). The attack sent false data to the operators' HMI so that some pressure values for turbine and reactor pressure were frozen. This was done in order to make it more difficult to detect the ongoing attack. The actual values were hidden from the operators. Because the system used the same frozen values to check if pressure was within acceptable limits, this manipulation also prevented the triggering of an alarm when the pressure increased. The attack also installed a backdoor to the PLC that was used to control valves on the high-pressure turbine so the turbine pressure increased gradually, in turn increasing the pressure in the reactor tank. See [2] for a more detailed description of the scenario.

interaction between the control room operators and the cybersecurity team was also an area of interest. The data analysis was supported by a tool that presents all the data together in a time-synchronized manner [3]. The tool shows video/audio recordings of the operators, the screens that they are working on as well as all the logged data (see 2.4). Selecting one piece of this time-stamped data will synchronize the other data to the same time, making it easy to get an overview of the operators' behaviour in relation to the simultaneous status of the process and the attack script.

3.2 Operators' handling of the incident

At the start of the scenario the operators were tasked with increasing reactor power from 85% to 100%. As soon as the power reached 99%, the attack script was initiated.

8 minutes after initiation of the script, the TO noticed some small fluctuations in trend graphs of the reactor power on the overview display. This was due to the increase in reactor pressure caused by the attack. The operators thought it was a strange phenomenon and they were not able to explain it. They tried to

change power regulation mode to see if the fluctuations stopped. Over the next minutes they observed the reactor power repeatedly increasing and decreasing. Still the operators did not understand the reason for the fluctuations. They therefore decided to do a partial reactor scram to reduce reactor power and avoid the risks of additional fluctuations in the reactor core.

Shortly after the partial reactor scram, the cybersecurity team got an alert from the intrusion detection system (IDS) that had detected unusual traffic between two machines in the process control network. The cybersecurity team called the control room to inform them about this, then continued monitoring and investigating the situation.

10 minutes later the TO noticed that some safety valves in the reactor pressure relief system were open. It looked like a leak through the main relief valve. However, after the information from the cybersecurity team of a possible cyberattack he was not sure if he could trust the valve indications (these indications were correct though). He recommended to trigger a reactor scram – to drop the control rods into the reactor core to stop the fission chain reaction – because this level of pressure may affect the reactor power, and because they did not fully understand what was going on. RO then initiated the reactor scram and they carried out a procedure to check status after scram.

The cybersecurity team again called the control room. They discussed status and the security team decided to escalate the incident to a higher level.

3.3 Primary observations

In this section, we highlight the main observations we have made from the experiment. We begin with a description of what we specifically observed, followed by our initial impressions of the state of practice in the industry/domain. Further work needs to be done to analyse the relevant cybersecurity challenges and solutions in detail.

Dependencies between safety/critical systems and non-safety/critical systems

The attack in the scenario targeted a turbine system which is generally not classified as a safety system. However, the attack scenario has shown that there was an impact on safety and business continuity of the plant. This raises several questions, one of which is on the isolation between safety and non-safety systems. One must investigate how to monitor the interaction between these systems.

Nuclear systems are distinctly divided into safety critical, safety relevant and non-safety systems. Safety systems, such as the reactor protection system, will function independent of other systems and operators' input. Reactor protection systems are often air-gapped from other systems and from operator control specifically and have their own sensors and redundancies to achieve safe operation and shutdown of a plant. However, until the reactor reaches a state where safety systems shut it down, the safety relevant and the non-safety systems play a central role in how operators manage the plant. Safety-relevant systems can include the plant control systems used to produce power and

balance the plant. For non-safety systems, e.g. plant health monitoring systems, security requirements are less stringent, and interconnectivity of systems is normal. For more information on nuclear legacy systems we refer to [4]. In most situations the operators rely on input from all systems, but with a preference for some information and systems for their decisions. Until the reactor protection system shuts the plant down, the control room is one dependency between the safety critical, the safety relevant and the non-safety systems. Lower safety and security requirements, and more allowed functionality in systems not critical to safety is one attack vector for exploiting this dependency. Recent standards, such as [5] and [6], address how to balance safety and security, but as it is fairly new its potential impact is not fully realized.

Further, as nuclear plant systems are not 'connected to the internet' and there are requirements in place to ensure that virus and malware is not physically introduced to the systems, there has not been a need for monitoring and diagnostic tools for cybersecurity events. Since cyber traditionally was not regarded relevant for nuclear installations cybersecurity has historically not been part of operator training either. In later years we see that there is more of a focus on cybersecurity, but as with most domains safety and security are considered differently and certainly not mutually important.

Non-existing or good enough monitoring and detection tools

For the control room operators there was little available information on the status of the Information technology (IT) or Operational Technology (OT) equipment other than indications as to if they are working or not (on/off). Traditional IT cyber detection and monitoring solutions are usually not available either, nor is it customary to have cyber support procedures for the operational side.

Efforts on cyber towards nuclear power plant workforce includes IT-side focused threats such as email scams and phishing, trojans and crypto viruses etc., very little in the way of threats to OT and potential impact on operation.

Incident handling process and procedures

Nuclear incident handling procedures are developed based on the physics and properties of the reactor. Further, the safety procedures are rigorously tested and part of operator training, a training that traditionally has remained solely safety focused. It is natural for operators to both stick to the mandated procedures and to have a natural safety focus, thus they are unable to identify and resolve cybersecurity events. Similarly, due to the predominantly analogue nature of most existing nuclear power plants and the low occurrence of cyberattacks (some nuclear facility attacks are described in [7]), the nuclear industry has not fully acknowledged the need for establishing procedures for handling cyberattacks, and there is also generally low focus on operator training and awareness in this area. This state of practice is reflected in the HAMMLAB setting. The procedures that are in place in the HAMMLAB, related to the NPP that is being simulated, would

not help the operators and other control room stakeholders to handle the cybersecurity attacks.

In case of a cyberattack, operators would typically not have a good overview of how to handle the situation, except for following safety procedures and bring the plant to a safe state. In case of an attack the organization should have plans for analysis and containment of the attack, eradication of malware and recovery of the plant systems. With minimal focus on cyber threats, these plans are likely also lacking.

Risk communication and visualization

In the experimental study we witnessed that the security team in the cyber operations centre and the operators in the main control room seem to have very different understanding of the situation and its impact. Although the security team could see plant status information from the control room and did identify that there was a cyber incident afflicting the plant, they were not able to communicate this in a meaningful way. On the other side, the operators in the main control room were not able to understand potential implications of what a cyber event would entail. The control room operators were actually the first to detect the effects of the attack when small fluctuations in the reactor power became visible in a graph on the overview display. They interpreted this as an anomaly and activated a safety precaution (partial reactor scram). The operators were open for the possibility that there was something wrong with a sensor and that numbers were incorrect, but they were not able to realize that there could be deliberate manipulation of information. And their response did not have an impact in terms of mitigating the security consequences of the attack. However, after the control room was informed about a possible cyberattack, this affected how they viewed the data in the control room, and they started mistrusting some of the data. Further, the visualization tools employed in the main control room and in the cyber operations centre were distinctly different. The security tools did not enable meaningful rationalization about plant status and the potential effects a cyber event can have on the operation, for instance how an attack on the turbine control system could impact the reactor system.

Awareness and training

Since the control room operators had no procedures for how to handle a cyberattack and no training in this, it is not surprising that their response was to handle the situation according to the safety procedures. Even in the case where procedures for cybersecurity incident response exists, personnel may be overcome by the urgency and gravity of the situation and not be able to act in the most optimal way. It is therefore necessary to train personnel for such situations. In the case of a cyberattack the burden on the control room crew may increase because there will be both safety and security aspects that they must consider. This may lead to increased stress and increased likelihood of errors. As with other emergency training, personnel should be so well trained that when the situation occurs, they know what to do and what not to do.

When a cyberattack has occurred, the main activities for immediate incident response are detection, analysis, containment, eradication and recovery [8]. Control room operators can have an important role in detecting an attack. In the pilot study the operators noticed early that something was not as it should be by looking at trends of process data. Good knowledge of the process and plant and what is normal plant behaviour can help in detecting when something abnormal is happening. This knowledge is also useful for analysing the incident. One aspect that will be useful to train for all phases of the incident response is communication between the control room staff and the cybersecurity team. This can increase the understanding on both sides of what the other team needs in order to handle the incident. It can also help in developing a common language to discuss an attack and its consequences. During an attack it is likely that the control room operators will have to focus on the safety aspects, and the cybersecurity team has the main focus on security. But both parts may have to consider their response from both the security and the safety perspective. Learning a little more about each other's domains can be helpful.

Observations about the experimental facilities for cybersecurity experiments

This first pilot study allowed us to get some insights into how the IFE's experimental facilities, Cybersecurity Centre and HAMMLAB, worked for running cybersecurity scenarios. The study showed that a realistic cyberattack could be simulated in the cybersecurity centre and HAMMLAB and it provided the intended effects on the plant systems. The facilities can be used to run similar experiments and to create a repository of attacks and their effects on different components and systems. The integration between the cybersecurity centre and the HAMMLAB allowed for studying the interaction between the security team and the control room team. The well-tested methods for analysing operator behaviour in safety-related scenarios were applicable also for the cybersecurity scenario. This integrated experimental environment provides a unique experimental setup to study the cybersecurity attack scenarios in a holistic way (people-process-technology). Moreover, IFE's researchers and engineers with cross-disciplinary expertise - cybersecurity, safety engineering, system engineering, process engineering, industrial psychologists, operators - together can design, execute and analyse realistic cybersecurity scenarios.

3.4 Future work

As mentioned in Section 1.1, the work presented in this paper is exploratory, with the purpose of: understanding cybersecurity incidents in a control room setting; explore the capabilities of IFE's experimental facilities for running credible cybersecurity studies.

Three experiments have been planned for 2020 and 2021 where IFE's HAMMLAB and Cybersecurity Centre (facilities and personnel) will be used. The planned experiments are in aviation, power generation and power distribution industries. The scenarios for the experiments are being developed in collaboration with the experts from the three industries. The first experiment planned is

the aviation case, where an air traffic controller will be subjected to credible safety scenarios and cybersecurity scenarios. During the scenario, the controller will be in a situation where he/she is receives wrong air surveillance data and has degraded voice communication capabilities. In the scenario, we will evaluate whether the controller will behave differently when he/she is made aware that the situation is due to an ongoing cybersecurity attack when compared to how he/she behaves if he/she perceives that the situation is due to a systems' reliability event. One aspect of interest here is, to what extent the cybersecurity event could affect the decision-making capabilities of the controller. The second and third experiment are at the early planning phase.

4 Conclusion

Cybersecurity preparedness and training of its workforce is vital for organisations to handle cybersecurity attacks. This paper presents an experiment that has been conducted by researchers and engineers to investigate how the workforce of a power plant - operators and security team - will detect and respond to cyberattack. The experiment utilised laboratory facilities to create a simulated operational environment of a power plant and has introduced a realistic cybersecurity scenario to study the workforce behaviour during the scenario. The main observations from the experiment were that there exist significant gaps in state of practice, including gaps in incident handling procedures, communication between operators and security team, and awareness and training.

ACKNOWLEDGMENTS

We thank Per-Arne Jørgensen, Fabien Sechi, Aleksander Lygren Toppe, Christer Nihlwing, Håkan Svengren, Per Øivind Braarud, Siv Hilde Houmb, and Erlend A. Engum for their support with planning and running the experiment. The study was performed as a part of the CybWin project funded by the Norwegian Research Council.

REFERENCES

- [1] Gyrd Skraaning Jr and Andreas Bye, 2011. The purpose of HAMMLAB and the theoretical basis for experimental research. In Ann Britt Skjerve and Andreas Bye, (Eds.), *Simulator-based human factors studies across 25 years: The history of the Halden man-machine laboratory*. London: Springer-Verlag.
- [2] Vikash Katta, Fabien Sechi, Per-Arne Jørgensen, Stine Strand, Per Axel Wiig, John Eidar Simensen, and Siv Hilde Houmb. 2019. Establishing a Cybersecurity Centre for Industrial Control Systems, In *the proceedings of the 29th European Safety and Reliability Conference (ESREL '19)*.
- [3] George McCullough, 2019. Experiment data collection methodology for application in crew debriefs. 2019 *Conference on nuclear training and education*, Feb. 5-7, 2019. St. Augustine, FL. American Nuclear Society.
- [4] Christopher Poresky, Charalampos Andreades, James Kendrick and Per Peterson, 2017. *Cybersecurity in Nuclear Power Plants: Insights for Advanced Nuclear Technologies*. doi:10.13140/RG.2.2.34430.69449.
- [5] IEC, 2016. *IEC 62859:2016, Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity*. International Electrotechnical Commission.
- [6] IEC, 2019. *IEC 62859:2016+A1:2019. Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity*. International Electrotechnical Commission
- [7] Alexandra van Dine, Michael Assante and Page Stoutland, 2016. *Outpacing cyber threats: Priorities for cybersecurity at nuclear facilities*. Nuclear Threat Initiative.
- [8] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, 2012. *Computer security handling guide. Recommendations of the National Institute of Standards and Technology. Special publication 800-61*. National Institute of Standards and Technology