Cyber-incident Response in Industrial Control Systems: Practices and Challenges in the Petroleum Industry

Vahiny Gnanasekaran
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
vahiny.gnanasekaran@ntnu.no

Maria Bartnes
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
maria.bartnes@ntnu.no

Tor Olav Grøtan
SINTEF Digital
Trondheim, Norway
tor.o.grotan@sintef.no

Poul Einar Heegaard
NTNU - Norwegian University of Science and Technology
Trondheim, Norway
poul.heegaard@ntnu.no

ABSTRACT

The number of significant cyberattacks targeted by national state actors is growing in critical infrastructure. Companies rely on detecting and responding appropriately to such attacks by practicing and developing procedures for the cyber-incident response. This paper presents the findings from seven semi-structured interviews to identify distinct practices, challenges, and roles regarding cyber-incident response in the petroleum industry. The literature has previously addressed specific IT, security, or Operational Technology (OT) teams only, but has not considered the holistic view of cyber-incident response in industrial control systems between internal roles, and external actors, such as Security Operations Centers, Computer Security Incident Response Teams, emergency response teams, and on-site personnel. To address this, a novel framework for empirical inquiry consisting of document analysis, and workshops as preparation for interviews, were conducted. The stakeholder diagram displays the most relevant incident response roles and a list of current challenges extracted from the interviews. Future research should consider extending the sample, and include other, organizational and procedural factors.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; *Distributed systems security*.

KEYWORDS

Incident Response, Cybersecurity, Cyber-incident, Operational Technology, Critical infrastructure

ACM Reference Format:
Vahiny Gnanasekaran, Maria Bartnes, Tor Olav Grøtan, and Poul Einar Heegaard. 2024. Cyber-incident Response in Industrial Control Systems: Practices and Challenges in the Petroleum Industry. In *2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability (EnCyCriS/SVM '24), April 15, 2024, Lisbon, Portugal.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3643662.3643958

EnCyCriS/SVM '24, April 15, 2024, Lisbon, Portugal

ACM ISBN 979-8-4007-0565-6/24/04.
https://doi.org/10.1145/3643662.3643958

1 INTRODUCTION

Major cyberattacks with more significant consequences and greater vigor are increasing in severity within Critical Infrastructure (CI), particularly due to the rising geopolitical tension between Russia and Western countries. Sophisticated state actors are silently targeting CI and even safety systems that can be harmful to fundamental, societal services. SektorCERT in Denmark recently reported a politically motivated cyber-attack on their CI, where 22 companies were subjected to a simultaneous attack, exploiting a critical vulnerability in a widely applied firewall [19]. The exposure granted the adversaries root access without authentication from the firewalls.

Regulations towards cyber-incident response exercises are paramount to increase awareness amongst industries. The advent of the EU's NIS2 directive advocates industrial stakeholders to improve their cyber-incident response. The Norwegian petroleum industry is implementing this to comply with these regulations regarding supply vendor chains, improved maintenance, and security monitoring. The industry performs frequently audits of the safety systems of offshore installations. However, due to the escalated tension in the North Sea, the regulating authorities have also been appointed to inspect the safeguarding of information and information systems enacted by the National Security Act [15] in the petroleum sector, further expanding the sufficient, security level for the industry.

Due to the current conditions, petroleum companies should consider altering their mindset of being affected by a cyberattack from "if" to "when". When zero-day vulnerabilities are exposed and exploited, any CI company is highly dependent on thorough and well-practiced incident response plans with different stakeholders to provide swift reaction, and mitigation to prevent the interruption of the production. Hence, the focus of the paper is an escalated cyber-incident with potentially catastrophic consequences, thereby excluding cyber-incidents from being de-escalated before reaching the emergency response.

The objective of the paper is to investigate all relevant external *actors* and internal company *roles* involved in cyber-incident response and provide a current state-of-the-art of how OT cyber-incident response is practiced in the industrial sector, using a novel framework for empirical inquiry. In this case, an industrial company consists of multiple actors where one actor might have several

Table 1: Alternative types of Security Operation Centre (SOC), from [8, 16]. The paper focuses on the last two alternatives.

Type of SOC	Definition
In-house IT SOC	SOC within the organization that only monitors the office network.
In-house OT SOC	SOC within the organization that only monitors the industrial network.
Outsourced IT SOC	MSSP only monitor the office network as a service.
Outsourced OT SOC	MSSP only monitor the industrial network as a service.
Inhouse integrated (IT and OT) SOC	*SOC within the organization monitoring the office and industrial network*
Outsourced integrated (IT and OT) SOC	*MSSP monitoring the office and the industrial network as a service.*

roles. These stakeholders were identified by attending meetings and further validated through workshops. Seven semi-structured interviews representing distinct roles in the petroleum industry are presented. The findings highlight the most relevant actors and roles involved during the cyber-incident response, and the challenges in the interactions between them, specifically during an OT cyber-incident response. The presented research design aims to explore organizational and human aspects of cybersecurity for the industrial sectors.

2 SECURITY OPERATION CENTERS

The section presents a brief definition and scope of a Security Operations Centre (SOC). A SOC is a service that contributes to incident response, the detection of cyberattacks, and the continuous security monitoring of logs, events, alerts, and incidents [16]. Literature [10, 24] highlights the need to plan sufficient response steps to cyber-incidents, protocols for incident escalation, and prioritizing categories of incidents.

The SOC services could be achieved through software (e.g., Security Information and Event Management (SIEM) [13]), network monitoring [9]), or hardware (e.g., sensors [11]) that enables the data collection of communication between all systems included in the service. Distinct SOC organizational models exist; one individual with various devices and tools, an assigned group in the organization (in-house), or an outsourced security service to a company, established on Service Level Agreements (SLAs) [8] (i.e., Managed Security Service Providers (MSSP)). The SOCs from MSSPs can be distinguished between *cloud and on-premise SOCs*. The cloud-based solutions can be swiftly deployed into the client's system, while on-premise requires more thorough onboarding [16]. This paper only addresses SOCs that involve organizational procedures, roles, and processes to ensure the continuous monitoring of the digital infrastructure, and includes IT and OT security monitoring (see Table 1).

Work on Operational Technology SOCs or both (i.e., *integrated*) is motivated in the literature [4, 5, 18]. Currently, few papers address such SOC operations, where most literature is present in the maritime sector [7, 17]. Integrated SOC analysts should collaborate with the OT operators to understand the threshold values for industrial sensors, process systems, Programmable Logic Controllers (PLC), and potential anomalies. Comprehension contributes to properly analyzing and understanding the log information, based on the OT system behavior, and not single incidents without context. In contrast to IT SOCs [1, 20], additional knowledge and skillsets are required in integrated SOCs, such as the use and control of the process systems, procedures, and planned maintenance [3, 8, 17], without which, the possibility for misinterpretations (e.g., false positives) would be imminent for *false-positives* for the SOC.

3 RELATED WORK

Some work applies qualitative methods to investigate cyber-incident responses with a socio-technical perspective [5, 14, 21]. They assess various cybersecurity standards and guidelines (e.g., IEC/ISO standards, NIST Special Publications, etc.) to assess the usefulness [21] or develop an industry-specific method for incident response [5]. The findings suggest that incident response training is primarily related to safety, whereas cybersecurity is not considered to the same extent. The reduced awareness and collaboration stems from the low frequency of such events in the sector, and the lack of training. However, the work only addresses one team (e.g., control rooms [14] or IT personnel [5]). Staves et al. [21] include incident response, OT, and IT personnel in their interview sample, but do not fully grasp the interactions between critical roles and procedures across multi-disciplinary teams (e.g., SOC, Computer Security Incident Response Teams (CSIRTs), emergency teams). Staves et al. [21] also suggest that no single guideline or standard applies to all aspects of cyber-incident response and recovery, and the lack of tools and frameworks for OT.

Building the cultural bridge between IT and OT workers is essential to improve cyber-incident response times. The communication gap between IT and OT personnel is further discussed in the literature as a significant challenge in environments with ICS systems [4, 5, 25]. In contrast to the IT employees, the OT workers are operating independently, and rely on developing their procedures [25], which might disrupt each other's priorities and tasks. The distinct working style and other differentiating factors (e.g., misunderstandings, unclear responsibility areas) lead to a lack of trust between the IT and OT employees [12]. Fostering collaboration between the different personnel is crucial to enable adequate detection and response to cyber incidents [5].

4 INTERVIEW STUDY DESIGN

This section describes the interview study conducted with different actors in the IT/OT incident response, presenting a possible, methodological approach to delineate stakeholders to grasp their critical procedures, and responsibility areas by applying various qualitative methods.

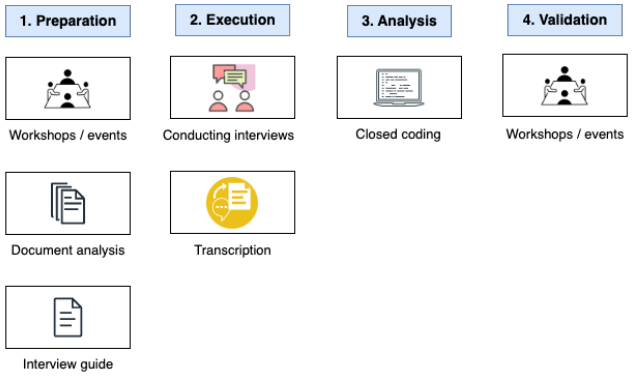

Figure 1: Framework for Research Study Design.

4.1 Data Collection and Analysis

Figure 1 provides a summary of the research design. First, the industry was consulted through meetings, where preparedness scenarios for cybersecurity were developed, document analysis of the revised readiness preparedness scenarios, checklists, contingency plans for cybersecurity, and workshops. The readiness preparedness scenarios were based on potential cyber incidents occurring offshore and onshore (e.g., incidents on the office network). During these sessions, insights about the stakeholders in a cyber-incident response within the petroleum sector were gained, which is the basis for the stakeholder (actors and roles) diagram that will be presented in the next session. Attending the different meetings and workshops was key to building relationships and establishing trust with relevant industrial partners to recruit participants. The increasing amount of sensitive information reinforces the need for security clearances and further affects the trust level of sharing even unrestricted, but still sensitive information. After conducting the interview and analysis, further validation was performed through industry workshops.

Semi-structured interviews were selected as the main qualitative research method, since they contribute to discovering the interactions in the cyber-incident response, including their role description, and procedures. The interview guides using established practices [2] were customized for each role, to cover more of their distinctive knowledge, and experiences, and were approved by other researchers. All interviewees were asked to introduce themselves with their occupations and years of experience and explain their workday and tasks. Furthermore, they were asked to explain their incident response role in detail, such as the difference between normal vs. emergency operations, and how the communication between external and internal roles and actors is during the incident (e.g., IT personnel, incident response teams, CSIRTs, CERTs, etc.)

The interviews were scheduled for approximately one hour and conducted in Norwegian. One researcher conducted the interview, and another researcher aided with questions and notetaking. Interviews were conducted digitally, or in person, using a recorder in both cases. One interview served to test the questions, duration, and format of the interview. All necessary documentation regarding ethical approval, GDPR compliance, and informed consent was obtained before data collection. The national research data collection tools were used to acquire consent, along with questions regarding their position, and years of experience. In total, seven participants were involved in the interview study.

The recordings were transcribed using an institution-approved OpenAI transcription tool, and verified by one researcher listening and correcting the transcription. The interviews were then imported into NVIVO [6], for qualitative data analysis. An open coding approach was opted for, based on the stepwise-deductive inductive procedure [22]. The transcribed interviews were iteratively coded for themes, applying empirically close coding (EC), implying that the coding can not be a priori-defined, and therefore stays close to the actual empirical material. The first iteration resulted in 361 EC codes. The next iteration grouped the relevant EC codes into larger, thematically connected coding groups:

(1) Procedures and roles in an outsourced or in-house SOC service (105 codes).
(2) Procedures and roles in an oil and gas company, both in ordinary and emergency scenarios, and routines and preparations regarding incident response exercises (93).
(3) Interaction between IT and OT personnel, equipment, systems, and infrastructure, both in ordinary and emergency scenarios (45).
(4) Procedures and roles at OT system vendors regarding cyber-incident response (40).
(5) General description of processes and systems in an oil and gas company that do not fit the previous categories (21).

The numbers in parenthesis indicate the number of codes finally placed in each category. One researcher placed all the codes, but they started with one calibration session with another researcher from the same project at each iteration to ensure a common understanding of the coding framework. The last 11 EC-codes were deemed as irrelevant for the study, and placed in the Other/irrelevant category.

4.2 Sample Description

Two petroleum companies participated, where one company employs over 10,000 and the other has 1,500 workers. The installations vary on the age, OT system vendors, and the maturity of the personnel, which creates local differences in cybersecurity knowledge, and awareness. Certain installations are more mature in cybersecurity, due to extensive training from vendors, and company acquisitions, embracing different attitudes, and cybersecurity cultures. For instance, one installation separates the *safety* and the *process* systems in segregated networks.

Two of the participants are from companies applying vendor-independent sensors in the lower Purdue levels (levels 0, 1, and 2) to monitor industrial customers' OT network traffic. The sensors passively read the incoming data, transmit the collection to their premises, and analyze it to investigate and assess anomalies in the customers' infrastructure. The companies seek to provide deep insights into the infrastructure through periodical reports or dedicated platforms. Initially, the service providers grant suggestions to upgrade or configure specific, exposed devices in the infrastructure. If they suspect an ongoing cyber-attack, they offer advisory services with suggested countermeasures to mitigate the attack. However, since they are not obliged to offer 24/7 monitoring

Table 2: Comparison of outsourced, integrated SOC by MSSP, and In-house, integrated SOC.

	In-house	Outsourced
Incident response retainer for multiple companies.		✓
Incident detection, and response for one company.	✓	
Provides digital forensics, root-cause analysis, reverse engineering, etc.	✓	✓
Use one portal for assessing events.	✓	✓
Collecting data from data sources offshore.	✓	✓
Performs threat hunt automation.	✓	✓
Directly contact the installations in case of a cyber incident.	✓	
Specialize in specific installations.	✓	
Manages the alarms within office hours.	✓	✓
Manages the alarms outside office hours.		✓

services, they are not limited to Service Level Agreements (SLA) to their customers, which is the domain of the in-house SOC or MSSP including SOC services.

Figure 2 depicts how an event is escalated to a potential cyber-attack in the outsourced SOC, with four steps. The queue is managed by Tier 1 security analysts, who are students and work part-time. The MSSP's SLA specifies the response time where investigating an event might take up to one hour to determine whether to alter the priority. The Tier 2 analysts are notified if Tier 1 increases the priority (step 1). If Tier 2 analysts cannot conclude, the security event gets escalated to the Tier 3 analysts (step 2). Some level of information gathering occurs at each step and is appended to the security event case. Suppose Tier 3 analysts are uncertain about how to manage the event. In that case, Tier 1 analysts are responsible for collecting the information from all Tiers (step 3), escalating the incident, and notifying the customer PoCs (step 4), since they possess most of the knowledge collected through steps (1) to (3) in Figure 2. The PoC list contains personnel prepared to answer system variations, planned maintenance, or other deviations.

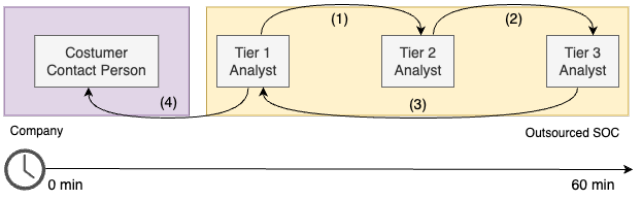

Figure 2: Event Escalation in an Outsourced, Integrated SOC.

5 IDENTIFIED ROLES DURING INCIDENT RESPONSE IN THE PETROLEUM INDUSTRY

This section presents the preliminary results from the meetings and attended workshops with the industry, which are further validated through the interviews. The interview findings reflect the perceptions of offshore and security personnel in the context of the current, geopolitical issues. An overview of all roles during a cyber-incident response is depicted in Figure 3, followed by a description of the roles assumed during a cyber-incident response. Such incident response is only triggered if the company suspects a cyber-attack with physical consequences on the installations. Only specific actors could trigger emergency response and CSIRT,

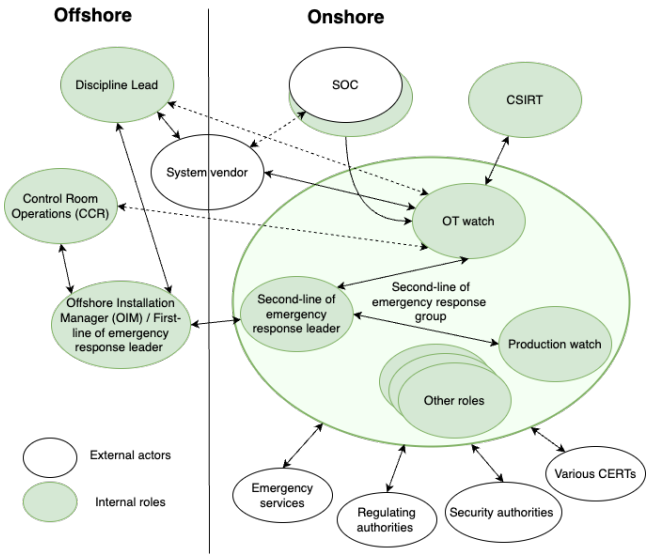

Figure 3: The links between the internal roles and external actors during cyber-incident response.

such as the Chief Cybersecurity Officer (CCSO), other cybersecurity staff members, or OIMs. The incidents could be discovered through the company's IT and OT service providers, offshore, SOC service, CERTs, or regulatory authorities, where the thresholds are pre-determined using contracts, or risk matrices, based on the company's cyber-risk appetite.

Offshore Installation Manager (OIM) / first-line emergency response leader, offshore. OIM is the "captain" of the offshore platform and makes the majority of the decisions throughout the incident response. Considering stopping the production will be due to a perceived malfunction of the control systems or the Safety and Automation Systems (SASs). As a result, it is unsafe to remain on the platform and requires further evaluation of potential shutdown, and/or crew evacuation. In this case, emergency response is alerted, where OIM becomes the leader of the first-line response, along with the second line of the emergency response team. Since they usually do not have in-depth technical knowledge, CCR, and Discipline Lead within various fields, such as electronics, instrumented systems, telecom, etc. serve as OIM's advisors.

The second line of the emergency response team, onshore. The team is mainly responsible for following the emergency response plan regardless of a cyber-induced incident. They consist of one manager, a communication logger, a production watch, an OT watch, and people responsible for establishing contact with relevant third-party actors, inter alia CERTs, regulators, emergency response, the press, social media, and internal communications. Since the OT and production watch are significant during the cyber-incident response, the roles are separated from the rest of the second-line emergency response group onshore.

OT watch & Production watch, onshore. The OT and production watch are two 24/7 watch roles performed by different, alternating OT cybersecurity, and safety personnel. In some cases,

the OT and production watches communicate directly with OIM's technical advisors, or through the leader of the second-line emergency team (depicted with dashed lines in Figure 3). Nevertheless, the OT watch is directly alerted by the SOC if the SOC detects a high or critical incident. The OT and production watch are the most technical employees with sufficient organizational knowledge and network and might provide useful insights to other off- and onshore roles. After a cyberattack, OT watch further contributes to verifying clean system back-ups with the CSIRT team.

The Control Room Operations (CCR), offshore. During an incident detected offshore, CCR verifies the state of the SASs to ensure normal operation. The first physical signs of a cyberattack are unresponsive safety and control systems or system anomalies. Since the anomalies could be the result of other influencing factors, they thoroughly assess Human-Machine Interfaces (HMI), and compressors, to initiate an investigation offshore.

Discipline Lead, offshore. The Discipline Lead possesses the most technical system knowledge offshore on their responsibility (e.g., telecom, safety system, etc.). During the detection phase, OT watch would discuss with the Discipline Lead within instrumented systems to verify the schedule or other, planned activities causing disruptions. They are responsible for revoking any daily work permits issued to prevent sub-contractors, or planned maintenance from tampering with the infrastructure during detection.

Security Operations Centre (SOC), onshore. Regardless of in-house or outsourced service, the SOC aggregates data from the sensors placed on the platform and assesses the criticality of security events in their logs. If any of the pre-defined rules based on several criteria (e.g., location, system, devices) is violated, an incident criticality indicating the severity of the incidents is set. Only the highest criticality (i.e., high, or critical) would be alerted to the SOC's Point of Contact (PoC) (e.g., OT watch, CCSO, security personnel), sufficiently skilled to understand the cyber-incident. In-house SOC contributes to digital forensics and investigation during the recovery phase. This might not be the case for a Managed Security Service Provider (MSSP), in case the customer did not purchase such retainers, but returns during the incident debrief.

Computer Security Incident Response Team (CSIRT). CSIRTs serve as the "task force" of the cyber-incident to provide a swift assessment of the severity and further action. The team is composed of highly competent internal personnel (e.g., OT, IT, security, etc.), vendors (e.g., IT/OT operations), or service providers (e.g., other teams from MSSP, such as incident responders, digital forensics, etc.), depending on the incident scope. They collect information from various sources, limit the damage potential, remove malware, restore clean backup, and follow up on lessons learned. The team is triggered by management or the emergency response team to collaborate and provide accurate information about the incident.

System vendor, on- and offshore. The system vendors are the industrial system providers. If their system(s) is affected, they would assist in investigating the vulnerabilities and the root cause. Usually, independent, industrial vendors with different maintenance routines can be present on one installation. They could stay offshore for a limited time (e.g., two weeks every six weeks). In case they

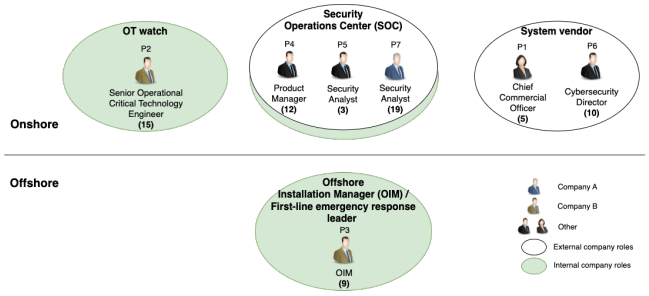

Figure 4: Sample description of the seven participants. The numbers are years of experience in the industrial sector.

are present during an attack, where their system is affected, the installation has another technically skilled person in the industrial system. Otherwise, the rest of the vendor organization resides onshore and provides support during the debugging and sanitation phase of system recovery.

6 INTERVIEW FINDINGS

This section presents the interview findings, where the sample is introduced first. In total, there were seven interviews, consisting of participants involved in the incident response, such as incident response personnel, SOC employees, or workers with in-depth knowledge of OT systems (see Figure 4 for an overview).

6.1 Cybersecurity Knowledge of Offshore Personnel

Participants use forums, the internet, colleagues, customers, and vendors to update their cybersecurity threat picture. The geopolitical issues concerning the Russian/Ukraine war have led to sharpened attentiveness and facilitation from offshore personnel towards cybersecurity personnel: *"They can easily postpone scaffolding so that we can travel to the installation. [...] There is a completely other focus from the management."* (Participant P7). P3 seemed unaware of the potential consequences of a sophisticated, Advanced Persistent Threat (APT) OT-cyber attack. He was concerned about harmful incidents leading to an emergency stop of petroleum production, but less concerned with cyber-attacks compromising the platform's integrity or becoming life-threatening due to the protection from safety barriers. P3 believed that the inherent security and system independence prevented any cyberattack from reaching the SAS systems: *"Emergency generators, completely separated, not connected to anything, [...] There is no way you can hack into those emergency types of equipment because it is not connected to anything."* However, he admitted that the greatest challenge is detecting an ongoing cyber attack, and performing the appropriate actions timely.

The knowledge level among the offshore personnel varies depending on the industrial vendors on each installation, according to P2. The general principle is to detect anomalies in a Human-Machine Interface (HMI) and investigate with the responsible actors in case of software updates or maintenance. He further argued about the capabilities of OIM as the leader managing the first-line response offshore during a cyber attack. Previously, the anomalies were usually suspected to be unintentional faults on servers or

equipment, but due to the increased cyber-situational awareness, they should consider adversaries as a potential motive.

6.2 Interaction between IT and OT Personnel

The IT and OT personnel in one of the petroleum companies meet weekly to classify security incidents that could affect the OT domain in case MSSP is unable to separate OT from IT incidents. Besides the weekly sessions, no further collaborations are initiated with the IT department, because the OT cyber-threats are inherently challenging to mitigate: *"You will never get rid of the threat because the threat itself is the IT-based control system. You use Windows, TCP, IP, firewalls, switches, etc. [...] We should rather protect more against where [the attacks] could come from."*. P7 experienced the same challenges with collaborating with the OT and IT personnel.

P6 and P2 highlighted the language barrier between the OT and IT domains. P2 struggled to feel understood by the IT employees, particularly when he attempted to explain OT system properties, interdependencies, and regulations. OT personnel are more careful of implementing any service that could violate the independence principle in safety systems. In one instance, IT tried to convince P2 to deploy cloud services to the OT infrastructure: *"IT was offended when I explained that we cannot deploy to the cloud, while their opinion is that the cloud is here to stay."* In contrast to the traditional IT personnel, he praised the CCSO and the cybersecurity personnel for their efforts to understand the OT system priorities. Still, they had not yet reached the ideal level of understanding.

Overall, P1 and P4 concur that the relations between IT and OT personnel vary, depending on sector and company. In some cases, they collaborate closely, while in other companies they neglect and disapprove of their differences: IT primarily worries about attack vectors, and patching vulnerabilities, while OT is concerned with production continuity. P1 described OT employees as urgent solving problems, who work autonomously, and become the workers that fix everything on-site: *"They become the MacGyver types that come to the rescue."* They are more critical to anything that might disrupt the production, for instance installing sensors, logs, or other tracking devices. In contrast, IT workers' duty is to enable the OT employees to work efficiently and swiftly. To accommodate the MacGyvers, IT employees reluctantly make exceptions for the OT employees (e.g., by allowing certain connections through the firewall or granting access to ad-hoc WiFi hotspots) to suit their working style. However, IT personnel is still responsible if intruders bypass the security measures, thereby becoming frustrated as the OT personnel keep challenging them to go against their principles.

6.3 OT Incident Response Practices

The petroleum industry has traditionally emphasized safety training and emergency exercises. P1 addressed the increasing focus on cybersecurity incident exercises. Their customers are slowly realizing that they cannot fully prevent security incidents from occurring but learn to manage by training the procedures, and roles in pre-defined scenarios. For instance, P7 contributes to offshore personnel practicing cyber incidents where the connection to the company's enterprise network is interrupted, to prevent the distribution of potential malware. They realize that they cannot stop adversaries from attacking, but practicing incident response reduces the time to return to normal operations.

P1 revealed that their clients (not only in petroleum) in general do not possess an "OT watch"-role in the cyber-incident response. Usually, a few uncredited individual(s) possess, due to seniority and participation in maintenance, or automation, a deeper understanding of the OT systems. They end up becoming the informal OT-watch-role who is always contacted (e.g., middle of the night) if a cyber-attack is suspected. In addition, smaller companies are more often dependent on their system vendor than larger companies, because they frequently purchase the entire industrial system from one vendor.

The need for establishing trust onboard the installations was highlighted by P3 and P7. P3 welcomed all first-time arrivers at the installation and tried learning their names. P7's cybersecurity team frequently visited the installations to *"have a coffee with them and small talk"* with the offshore personnel. As a result, offshore workers gained more cyber security awareness and recognized the cybersecurity personnel during a call. Even though the trust was more easily gained offshore, they were aware that the trust needed to be constantly maintained. P3 expressed worries that the established trust could be compromised by the foreign subcontractors performing system maintenance: *"They have done the security training, but I don't think [company B] requires the subcontractors to perform background checks on their workers."*

Further, P3 believed that his installation trains sufficiently on incident response. As far as he was concerned, his role was only responsible for making timely decisions, regardless of the nature of the event. During the incident response, he will decide to disconnect the communication towards onshore facilities, set the production in a fail-safe mode, and ultimately evacuate the offshore personnel. Even though he consulted with offshore technical employees, he compared the offshore management to a military command line: *"In everyday life, we are playing on the same team [...] but during an emergency [...] when I make the decision, it is going to stay that way."*. However, the dialogue between onshore and offshore personnel is not enough practiced, according to P2.

The scenarios to be practiced are scheduled in an annual schedule for offshore personnel. The tabletops are conducted after an ordinary day offshore and are time-consuming. Usually, the lively discussions result in less time to delve into the technical details of the incident response. Only certain, exercises are initiated to practice cybersecurity, but most are intended to verify safety procedures. The exercises might lead to updating the procedures to the next iteration. Each installation has its safety plan consisting of procedures on how to safely stop the production in case of a critical (cyber-) incident, located in a safe only accessible by security-cleared individuals. When a potential, critical event is detected, the offshore personnel verifies that the relevant scenario is selected, and executes the respective action list. For instance, a potential scenario might be an attack on the office network ashore. The action list indicates that the OIM should consult the Discipline head within Safety Instrumented Systems (SIS), and disconnect communications, activating *Island mode*. Subsequently, the offshore personnel investigates any traces of the adversary on the systems.

6.4 Perceptions of an Outsourced SOC

Most participants concurred that outsourced SOCs need to improve their OT knowledge. P7 had yet to experience an adequate, external OT SOC service: *"It is mostly due to only speaking IT, only they have moved the same IT tool to another level."*. According to him, they only emphasized one level without considering the entire infrastructure, system behavior, and criticality, implying that the majority of reported incidents from external SOCs are false positives. The lack of a holistic system view was further disclosed by P2: *"If you are getting into an OT cyber-incident, you might want to talk to someone that knows OT, and not someone that believes some part of what is going on in there."* Both suggested that insufficient monitoring equipment and unsatisfactory OT knowledge level are two factors contributing to lower SOC performance. An ideal OT SOC provides concise feedback offshore and hand out the appropriate playbooks while the onshore resources are being approached.

From the outsourced SOC, P4 and P5 acknowledged that their OT knowledge is not fully matured yet. Their primary focus is on identifying, detecting, investigating, and responding to IT incidents, which is still relevant since most incidents stem from IT. Nevertheless, the SOC is dependent on clients sharing their OT system knowledge to understand the system behavior and criticality: *"If we approach them with something, wondering what that is, they cannot look at us and say we should know. We are completely dependent on talking with both security and OT guys."*

The dialogue during incidents with the OT team at different clients is currently satisfactory, according to P5. However, this is contradicted by P6 and P7, which credit the limited visibility and understanding of the lower process systems as primary reasons. It remains a challenge to convince OT employees to install agents that passively monitor their infrastructure. They worry that the sensors draw resources from the OT systems. However, if the alerts are not considered critical for the OT employees, OT workers might decide to fully neglect instructions from the MSSP. To further improve the OT knowledge, P4 and P5 encourage the key OT personnel to share their system criticality and to aid the SOC in understanding the OT system reasonably in advance. The awareness could produce earlier detection and response to cyber incidents.

7 DISCUSSION

The proposed research method in Section 4 introduces a novel, qualitative approach to identifying incident response stakeholders. In this paper, the case is from the petroleum industry. By combining document analysis, workshops, and interviews, the method achieves data triangulation, where indications in one source may be elaborated by the other source. The proposed diagram depicts the identified stakeholders and their iterations under a major cyber-attack with potential physical consequences. In addition, the method supplements the existing data in terms of procedures, acquired knowledge, and experience of individuals not yet documented, providing insightful contributions to organizational and operational aspects of OT incident response.

However, the method is time-consuming and requires access to an industrial company willing to share information. Furthermore, the findings only present indications in the industrial sector demanding further qualitative study within a larger sample primarily within the same sector and then include cross-sector studies. Follow-up work should extend the sample size of participants in each role to look deeper into to what extent corporate culture, role descriptions, and other organizational factors affect the OT workers' cybersecurity awareness.

The remaining section provides an overview of the identified challenges in the OT Cyber-Incident Response. In general, few cyber incidents are reported, and a small part of them occur offshore. One of the participating companies had no cyber-incidents, and only five non-cyber-related incidents since 2015, indicating a need for exercises to gain experience. On-site personnel know that the expected system behavior will detect anomalies in the production system, but are less experienced in suspecting the malicious root cause [14]. Despite other sectors and literature [5], the participants had observed an increase in cybersecurity awareness among the operators and engineers, due to the Russia-Ukraine war. However, OT workers still do not "instinctively" seek Indicators of Compromise (IoC), and require more experience and knowledge until they reach full awareness.

The outsourced MSSP does currently not distinguish between IT and OT customers, or between CI companies. This might potentially be crucial when most OT customers demand a swifter response since the physical consequences could further escalate. Nevertheless, guaranteed short response (given in the SLA) is required. Still, they might not receive sufficient information to predict the next course of action and even less if the response time is longer. In case of a sector-specific attack, a strained, outsourced SOC service could restrict the necessary support needed for the customers to manage the cyber incident. In addition, the knowledge among the Tier 1 security analysts is not easily shared for OT events as for IT. The event handling systems are designed for IT security events, and not for OT, making newcomers more dependent on experienced analysts to understand OT security events. Consequently, newcomers are expected to escalate the OT events more frequently, straining the SOC resources further. The CI companies should factor in the limited resources when choosing between outsourced and in-house SOC services.

The interview findings suggest that industrial companies are not sufficiently confident about outsourced SOC services distinguishing the cyber incidents with the correct OT system criticality. Outsourced and in-house SOCs lack the proper equipment and knowledge to classify OT incidents. The emphasis on IT services and vulnerabilities is also reflected in the literature [10, 23]. Monitoring OT systems demands a comprehensive understanding of the OT system behavior, which is generally not known to SOC analysts mostly monitoring IT systems. Since MSSP do not have adequate equipment for monitoring OT services yet, getting familiarized with the installations is crucial to provide sufficient alerts. Dragos [3] suggests that the knowledge gap between the operators and the security analysts is reduced if they spend time learning from each other. Observing and understanding the communication in the facilities contribute to realizing the criticality of their most important assets. Affording physical visits and seeking the OT worker's knowledge might prove as invaluable insights between SOC and OT engineers.

Staves et al. [21] emphasis the need for flexibility during an incident, with an executing practical actor close to the system, and off-site actors who will assist and support with supplementary (cybersecurity) expertise. Such adaptive capacity is a part of cyber resilience, and critical for engaging appropriately in cyber-incident response [4]. Even though such adaptability is not stated in the contingency plans on cybersecurity scenario descriptions during the document analysis, the interview findings indicate that the incident response roles should carry a certain flexibility in such situations (e.g., OT watch acquiring competence in the organizational network to swiftly obtain relevant workers, given the incident).

Even though the differences between IT and OT departments have been discussed in the literature [12, 14, 25], the interviews still suggest few to no signs of change. The fundamentally distinct priorities and challenges each team faces are not properly communicated because they do not have a common language. The CI companies should foster open and comfortable communication between the OT operators and IT cybersecurity departments. Based on the discussion of the literature and interview findings, these are the main challenges within OT security incident handling:

(1) Detecting Security Incidents Sufficiently Early.
(2) Limited Resources at MSSPs.
(3) SOC Triggering at Irrelevant Incidents.
(4) Knowledge Sharing Between SOC Analysts.
(5) Updated List of Personnel and Knowledge in the Organization.
(6) Flexibility In Incident Response Roles.
(7) Cultural Differences between IT and OT Personnel.

8 CONCLUDING REMARKS

This paper presents the current practices, roles, and challenges regarding OT cyber-incident response in the Norwegian petroleum industry. In addition, it introduces a novel framework for empirical inquiry comprising qualitative research methods, that may be applied in similar sectors. A further study expanding the sample with employees off and onshore in other roles (e.g., Discipline head) and multiple participants could contribute to generalizing the key observations discovered in this study.

ACKNOWLEDGMENTS

The authors would like to thank the industrial companies and participants partaking in the document analysis, workshops, and interviews. This research was funded by the Norwegian Research Council through the project *Cybersecurity Barrier Management*, grant number 326717.

REFERENCES

[1] Sathya Chandran Sundaramurthy. 2017. *An Anthropological Study of Security Operations Centers to Improve Operational Efficiency.* Ph. D. Dissertation. University of South Florida. http://scholarcommons.usf.edu/etdhttp://scholarcommons.usf.edu/etd/6958
[2] Juliet Corbin and Anselm Strauss. 2008. *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory.* SAGE Publications, Inc., Thousand Oaks, California. https://doi.org/10.4135/9781452230153
[3] Dragos. 2017. *Insights into Building an Industrial Control System Security Operations Center.* Technical Report. Dragos Inc. 12 pages.
[4] Vahiny Gnanasekaran, Maria Bartnes, Tor Olav Grøtan, and Poul Einar Heegaard. 2024. Rethinking Independence in Safety Systems. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media.* Springer.
[5] Martin Gilje Jaatun, Eirik Albrechtsen, Maria B. Line, Inger Anne Tøndel, and Odd Helge Longva. 2009. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection* 2, 1-2 (2009), 26–37. https://doi.org/10.1016/j.ijcip.2009.02.004
[6] Kristi Jackson. 2019. Qualitative data analysis with NVivo.
[7] Olivier Jacq, Xavier Boudvin, David Brosset, Yvon Kermarrec, and Jacques Simonin. 2018. Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre. In *2018 2nd Cyber Security in Networking Conference (CSNet).* IEEE, 1–9.
[8] Christoph Jansen. 2017. Stabilizing the Industrial System: Managed Security Services' Contribution to Cyber-Peace. *IFAC-PapersOnLine* 50, 1 (2017), 5155–5160. https://doi.org/10.1016/j.ifacol.2017.08.786
[9] Eric D. Knapp and Joel Thomas Langill. 2015. Chapter 12 - Network Monitoring of Industrial Control Systems. In *Industrial Network Security (Second Edition).* Chapter 12, 351–386. https://doi.org/10.1145/3338499.3357354
[10] K Knerler, I Parker, and C Zimmerman. 2022. *11 Strategies of a World-Class Cybersecurity Operations Center.* MITRE. https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center
[11] Daniel L. Marino, Chathurika S. Wickramasinghe, Kasun Amarasinghe, Hari Challa, Philip Richardson, Ananth A. Jillepalli, Brian K. Johnson, Craig Rieger, and Milos Manic. 2019. Cyber and Physical Anomaly Detection in Smart-Grids. *Proceedings - 2019 Resilience Week, RWS 2019* (2019), 187–193. https://doi.org/10.1109/RWS47064.2019.8972003
[12] Ola Michalec, Sveta Milyaeva, and Awais Rashid. 2022. When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures? *Big Data and Society* 9, 1 (2022). https://doi.org/10.1177/20539517221108369
[13] David Nathans. 2015. Chapter 1 - Efficient Operations. In *Designing and Building Security Operations Center.* Syngress, 1–24. https://doi.org/10.1016/B978-0-12-800899-7/00001-X
[14] Espen Nystad, Vikash Katta, and John Eidar Simensen. 2020. What happens in a control room during a cybersecurity attack?: Preliminary observations from a pilot study. In *Proceedings - 2020 IEEE/ACM 42nd International Conference on Software Engineering Workshops, ICSEW 2020.* 270–275. https://doi.org/10.1145/3387940.3391454
[15] The Ministry of Justice and Public Security. 2023. Act relating to national security (Security Act). https://lovdata.no/dokument/NLE/lov/2018-06-01-24. [Accessed 29-11-2023].
[16] Cyril Onwubiko and Karim Ouazzane. 2019. Challenges towards Building an effective Cyber Security Operations Centre. *International Journal on Cyber Situational Awareness* 4, 1 (2019), 11–39. https://doi.org/10.22619/ijcsa.2019.100124
[17] Marco Raimondi, Giacomo Longo, Alessio Merlo, Alessandro Armando, and Enrico Russo. 2022. Training the Maritime Security Operations Centre Teams. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR).* IEEE, 388–393. https://doi.org/10.1109/CSR54599.2022.9850324
[18] Andreas Reisser, Manfred Vielberth, and Sofia Fohringer. 2022. Security Operations Center Roles and Skills: A Comparison of Theory and Practice, Vol. 2. 316–327. https://doi.org/10.1007/978-3-031-10684-2
[19] Anna Ribeiro. 2023. SektorCERT reports cyber attack against Danish critical infrastructure, raises concerns of state involvement - Industrial Cyber. https://industrialcyber.co/reports/sektorcert-reports-cyber-attack-against-danish-critical-infrastructure-raises-concerns-of-state-involvement/. [Accessed 24-11-2023].
[20] Mario Saraiva and Nuno Mateus-Coelho. 2022. CyberSoc Framework a Systematic Review of the State-of-Art. *Procedia Computer Science* 204 (2022), 961–972. https://doi.org/10.1016/j.procs.2022.08.117
[21] Alexander Staves, Tom Anderson, Harry Balderstone, Benjamin Green, Antonios Gouglidis, and David Hutchison. 2022. A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. *International Journal of Critical Infrastructure Protection* 37, March 2021 (2022), 100505. https://doi.org/10.1016/j.ijcip.2021.100505
[22] Aksel Tjora. 2018. *Qualitative research as stepwise-deductive induction.* Routledge.
[23] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul. 2020. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access* 8 (2020), 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514
[24] T Yamada, T Nakano, T Kaji, S Tano, and IEEE. 2020. Security Introduction Framework for Operational Technologies and Applying to Industrial Control System. In *2020 59TH ANNUAL CONFERENCE OF THE SOCIETY OF INSTRUMENT AND CONTROL ENGINEERS OF JAPAN (SICE).* 25–30.
[25] Alberto Zanutto, Ben Shreeve, Karolina Follis, Jerry Busby, and Awais Rashid. 2017. The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems. In *Symposium on Usable Privacy and Security (SOUPS).* USENIX, Santa Clara, CL, 1–6. https://www.usenix.org/system/files/conference/soups2017/wsiw2017-zanutto.pdf