A Comparative Study of Security Operations Center Models for Operational Technology

Vahiny Gnanasekaran[1,2], Thomas Grønbakk Nilsen[2], and Poul Einar Heegaard[2]

[1] Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway
{firstname}.{lastname}@sintef.no
[2] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim, Norway
{firstname}.{lastname}@ntnu.no

Abstract. Operational Technology (OT) systems are facing increasing cybersecurity risks due to IT/OT convergence, legacy systems, and evolving regulatory demands. Security Operations Centers (SOCs) play a central role in monitoring and responding to these threats. However, existing literature predominantly focuses on IT-centric SOCs, leaving OT SOC models underexplored. This study examines the structure and implementation of SOC models designed for OT systems, based on 14 qualitative interviews with security professionals and industry stakeholders. The findings reveal a spectrum of SOC models, including integrated, dedicated, in-house, outsourced, and vendor-operated. Each possesses distinct trade-offs in visibility, contextual awareness, cost, and operational resilience. The study identifies key factors influencing the selection of the SOC model for industrial clients, including organizational size, OT complexity, and regulatory pressures. It also outlines future directions for integrated SOCs, process-aware monitoring, and federated models. By bridging empirical insights with existing literature, this work contributes a comparative framework for evaluating OT SOC models and informs both academic research and industry practices in securing critical OT infrastructures.

Keywords: Security Operations Center · Operational Technology · Cybersecurity · Critical Infrastructure

1 Introduction

Operational Technology (OT) environments are increasingly exposed to cyber threats that can disrupt critical processes, compromise safety, and cause severe economic damage [7]. The convergence of IT and OT networks, combined with regulatory developments (e.g., the NIS2 directive), has increased the need for Security Operations Centers (SOCs) that can monitor and respond to OT-specific threats. A SOC is a centralized team responsible for monitoring, detecting, and responding to cybersecurity incidents within an organization [24]. Current Managed Security Service Providers (MSSP) or in-house teams offer security moni-

toring for distinct parts in the digital infrastructure: only IT systems, only OT systems, or both (i.e., integrated) [10].

Most SOC literature has comprehensively identified and investigated various challenges and elements of a traditional (IT) SOC type, such as alert fatigue among analysts [22,12], false positives [2], and SOC onboarding [11]. Moreover, security monitoring challenges in OT have been increasingly addressed, such as identifying indicators of compromise (IoC) [3] and visibility issues in industrial systems (e.g., PLC, process control systems) [13]. In this paper, we address three types of SOC: IT SOCs, which primarily monitor IT systems, OT SOCs, which monitor OT systems, and an integrated SOC that combines both monitoring capabilities.

While much literature exists on IT SOCs [24], and OT security individually [5], OT SOCs and integrated SOCs remain underexplored. This research addresses that gap by identifying different OT SOC models across and within various organizations. More specifically, the work is guided by the following research questions:

RQ1 What are the current benefits and challenges with existing OT SOC models?
RQ2 Which factors influence the selection of an OT SOC model?
RQ3 What future developments and directions do industry professionals foresee for OT SOC models?

To this end, this study applies an interview study with 14 participants within OT security and stakeholders across multiple industrial sectors in Norway. The study addresses the development of OT SOC models, situational awareness, contextualization of alerts, and process-level monitoring. It also identifies technical and organizational challenges and provides suggestions for increased collaboration, training, and operational integration. Based on empirical insights, primarily from a Norwegian context, this work contributes to the SOC literature and industry efforts to assess and improve current OT SOC capabilities.

2 Background & Related work

SOCs are centralized units responsible for continuously monitoring, detecting, analyzing, and responding to cybersecurity incidents within an organization's IT and/or OT environments. Their overarching goals are to reduce detection and response times, contain threats, and ensure operational continuity by leveraging technologies such as SIEM platforms, threat intelligence feeds, and structured incident response playbooks [24]. Core SOC functions typically include log collection and analysis, real-time alert monitoring, incident triage and escalation, forensic investigation, threat hunting, and compliance reporting [15,20].

In addition to purely IT- or OT-dedicated SOCs, organizations are increasingly adopting integrated SOCs that integrate monitoring across both domains. Integrated SOCs aim to provide integrated visibility and response capabilities, but they must reconcile the different priorities, technologies, and operational practices that characterize IT and OT environments [10]. Figure 2 places the

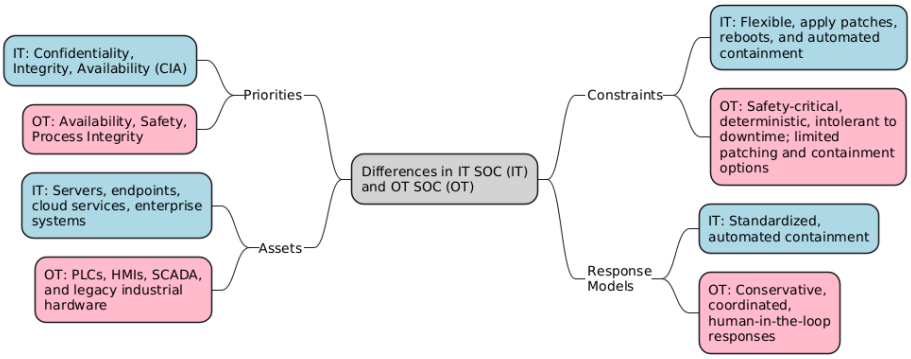

Fig. 1. Key differences between dedicated IT SOC and OT SOC.

monitoring span of the three SOC types (i.e., IT, OT, and integrated SOCs) in the Purdue model. The Purdue model presents a reference architecture of the IT and OT infrastructure in industrial companies.

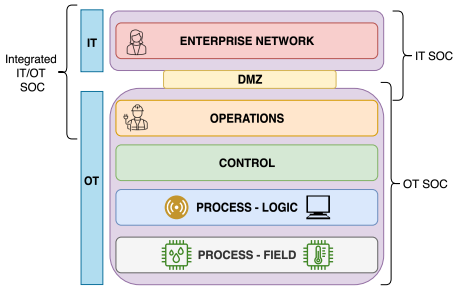

Fig. 2. The monitoring span of each SOC type.

IT and OT SOC share the same fundamental mission of safeguarding critical assets through timely detection and response, but differ in priorities, monitored assets, system constraints, and operational models [8,21]. An overview of the most significant differences between the two SOC types is provided in Figure 1. While IT and OT SOCs share common goals, such as threat detection and incident response, their operational divergences are numerous. Both face challenges such as alert fatigue, skill shortages, and fragmented toolsets [24].

Previous work covers core functions [24], IT/OT convergence [9], and integration of network and security operations [20], but lacks a discussion of a structured categorization tailored to OT. The literature often presents theoretical frameworks, role definitions, or high-level governance models [15], while the industry and vendor documentation offer practical insights into implementation. The lat-

ter, however, often reflect commercial interests and may overstate the benefits of specific solutions. Two broad SOC models for monitoring OT systems emerge in the literature and practice:

1. *Integrated SOCs:* IT and OT assets are monitored within the same SOC, either by the same analyst team or by co-located, specialized sub-teams. Integration promises cross-domain visibility and efficiency, but may dilute the expertise needed in ICS systems.
2. *Dedicated OT SOCs:* Only monitoring for OT environments, with distinct infrastructure and personnel. This supports domain-specific knowledge but risks isolation from enterprise IT operations.

Implementation of OT SOC models can be in-house, offering maximum control and contextual knowledge, or outsourced to MSSPs or vendors, providing scalability and cost savings but often at the expense of context and operational agility [20,1]

2.1 Related Work

Several recent works address specific capability areas relevant to OT SOCs; however, most remain conceptual or technology-focused, without providing empirical analysis of how SOC models are implemented in practice.

Schönig et al. [19] and Novak (2025) [15] propose process-oriented SOC models that align monitoring with business workflows and define SOC roles and decision-making. While valuable as conceptual frameworks, these studies do not assess how such models are applied in operational OT environments.

Perera et al. [17] explore the notion of intelligent SOCs, leveraging automation, threat intelligence, and machine learning to reduce analyst workload. Their work highlights both opportunities and risks, such as alert fatigue and misplaced trust in automation. However, their focus remains mainly on IT SOCs, and they do not examine how automation constraints manifest in the OT environment, which is the primary focus of our study.

The design of human–machine interfaces has also received attention. Reyna et al. [18] and Ofte [16] emphasize that SOC interfaces often fail to support rapid, accurate decision-making in OT contexts. While these works identify usability gaps in SOC, they do not connect interface design to the selection of broader SOC models. Our study highlights that without applying specific OT SOC models, improved interfaces risk being underutilized.

The literature offers valuable insights into specific capabilities, process orientation, and automation interfaces. However, these contributions typically examine isolated aspects of the design of SOC models. They do not provide a comparative analysis grounded in empirical findings from the industrial sector and managed security service providers (MSSP). This gap is addressed in our study by systematically comparing OT SOC models from the literature and practice.

3 Methodology

The primary study objective was to gain in-depth insight into the organization and implementation of OT SOCs within the Norwegian industry. Semi-structured interviews enabled participants to share their experiences, challenges, and best practices that would have otherwise remained unexplored. This section outlines the procedures for data collection, analysis, and sampling.

3.1 Data collection

This section describes the recruitment of participants and the implementation of the interview process.

Recruitment Participants were recruited using convenience and snowball sampling methods. The target group represented a diverse set of roles, including SOC analysts, OT engineers, cybersecurity leads, and managers from critical infrastructure sectors such as energy, manufacturing, and process industries, to gain knowledge and insights from different perspectives. Practical experience with OT SOC initiatives and their familiarity with the challenges of IT/OT convergence for security were also preferred qualifications. Initial participants were contacted through professional networks, industry events, and LinkedIn, with further participants identified through referrals.

Interview Procedure Interviews were conducted through video conferencing or over the phone. All participants were informed about the study objectives, the voluntary nature of their participation, and the data handling procedures, and provided written informed consent that complied with GDPR requirements. Interviews were audio-recorded and subsequently transcribed, and lasted approximately 60 minutes, depending on the participant's availability and engagement. A common interview guide was developed and addressed the following topics:

- Distinctions between OT SOC, and IT SOC
- What is an OT SOC?
- What could look like an ideal OT SOC?
- Factors necessary for advancing OT SOC solutions in Norway
- Advantages and disadvantages of different OT SOC models
- Future development trends for OT SOCs
- Incident handling (or potential neglect) within OT environments
- Current challenges in OT security
- Collaboration (or lack thereof) between IT and OT

Probes and follow-up questions were adapted based on participant responses to encourage elaboration and clarification. Ethical approval for the study was obtained from Norwegian Agency for Shared Services in Education and Research.

3.2 Data Analysis

The interview data were analyzed using an inductive coding approach, well-suited to the exploratory nature of this study and the semi-structured interview format [23]. This method allowed themes to emerge organically from participants' own descriptions, preserving authenticity while accommodating unexpected insights. The analysis process was conducted in NVivo, enabling systematic management of the transcripts, including attribute assignment by participant role and industry to facilitate subgroup comparisons. Coding was performed in English to ensure consistency, with translation of Norwegian statements during transcription to retain original meanings.

Initial codes were developed inductively, guided in part by anticipated themes from the interview guide, and progressively refined into broader thematic categories. The coding structure has a hierarchical form, with parent nodes capturing key areas and child nodes representing more specific subthemes. An iterative approach inspired by the Stepwise Deductive–Inductive (SDI) method [23] was used to validate and adjust codes continuously, ensuring close alignment with the empirical material. Table 1 depicts the number of codes in each identified coding category. In total, 1,141 codes were identified and organized across eleven parent nodes.

Table 1. Coding categories with number of codes, and descriptions.

Coding Category	**# Codes**	**Description**
Current State	487	Perceptions of OT SOC maturity, SOC models in use, and current challenges.
MSSP and Outsourcing	151	Experiences with managed SOC services and scalability issues.
Awareness and Contextualisation	150	The challenge of providing OT context to analysts and maintaining local knowledge.
Future OT SOC	135	Views on how an OT SOC should ideally function, including coverage, analysts, and long-term expectations.
Bridging the Gap	56	The relationship and training needs between IT SOC staff and OT engineers.
External Drivers and Compliance	38	Role of NIS2 and regulation in driving OT SOC adoption.
Vendors and System Integrators	32	Vendor-imposed constraints on security tooling in OT environments.
Monitoring and Sensor Depth	27	Issues with sensor placement and data collection without disrupting operations.
Cooperation	24	Importance of collaboration within and across organizations.
AI in SOCs	21	Perspectives on automation and AI in OT SOCs, including conservatism and trust.

3.3 Sample Description

Table 2 presents the sample description of the 14 interviewees. Two participants had international backgrounds, while the rest worked primarily in the Norwegian industry. Six informants work for one of five distinct industrial companies,

while six work within one of three MSSPs. The remaining two work within OT consultancy, manufacturing, and academia. The informants' working experience varied, with most having worked for over 11 years and five having worked within OT and security for over 20 years.

Table 2. Sample description of the interviewees.

Informant	**Years of Experience**	**Job Title**	**Industry**
P1	11–15	OT Security manager	Consultancy (MSSP1)
P2	16–20	Professor	Academia & Industry
P3	6–10	Security/privacy manager	OT company 5
P4	20+	OT Security Lead	OT company 1
P5	20+	OT Security engineer	OT company 2
P6	20+	OT Lead	OT company 1
P7	1–5	OT SOC analyst	Consultancy (MSSP1)
P8	20+	Sr. OT Security consultant	Consultancy (MSSP3)
P9	1–5	OT SOC analyst	Consultancy (MSSP3)
P10	1–5	OT SOC analyst	Consultancy (MSSP3)
P11	16–20	Strategic SOC advisor	Consultancy 1
P12	1–5	OT SOC analyst	OT company 3
P13	11–15	OT Security manager	Consultancy (MSSP2)
P14	20+	OT Security Architect	OT company 4

4 Empirical Findings

This section highlights the identified SOC models from the interview findings. Tables 3 and 4 provide a brief comparative summary of the SOC models presented in this section. They vary by sector, scale, integration depth, and provider maturity. For instance, an actor operating an integrated IT/OT SOC model can analyze network traffic more thoroughly, provided they have sufficient data sources and other resources. Outsourced SOC models may also provide a suitable operational context through the use of MSSP staff sufficiently understanding the client's perspective.

4.1 Comparing OT SOC models

This section presents the distinct OT SOC models, along with their advantages and disadvantages as reported by different interviewees.

Table 3. The key benefits of each OT SOC model, based on monitoring range.

SOC model	**Benefits**
IT/OT SOC	IT/OT visibility and collaboration
	Fit for smaller organizations
	Hybrid analyst skillset requirement (IT+OT generalists)
	IT-side detection strength for IT→OT attack chains
OT SOC	Cost/overhead of separate SOCs
	OT specialization depth and process-aware IR
	Operational independence from enterprise IT SOC (resilience if IT goes down)

Table 4. Features of each SOC model, based on service provider.

SOC model	**Features**
In-house	Local operational context retained
	Easier tailored monitoring & detections (site/process-specific)
	Requires internal staffing at asset owner
	Offers IT visibility
	Retaining organizational monitoring knowledge
	High cost to maintain service
MSSP-based	Easier 24×7 coverage feasibility
	Higher risk of generic models and false positives
Vendor-operated	Alignment with vendor architecture & support contracts

Integrated SOCs integrate OT monitoring into an existing IT SOC structure, and are valued for their cross-domain visibility and operational efficiency. Participants noted that integrated SOCs can improve collaboration and streamline detection across IT and OT environments, primarily when incidents originate on the IT side. A key advantage mentioned by P2 and P7 is shared situational awareness. Furthermore, maintaining a separate OT SOC is too expensive, particularly considering the organizational size: "*We are too small to maintain a separate OT SOC. It would be too costly and hard to sustain the expertise*" **(P6)**. Integrated SOCs also provide a more complete view of emerging threats, since most OT cyber incidents originate from the IT infrastructure.

Despite these benefits, integrated SOCs come with notable trade-offs. One MSSP analyst emphasized the difficulty of maintaining focus on OT operations when IT incidents dominate: "*People tend to drift toward IT. Phishing and cloud compromises are more exciting. OT issues, like bypassing Windows 7 login, don't seem as cool*" **(P5)**. P6 warned of losing the OT in-depth knowledge when integrating IT and OT monitoring. Moreover, developing interdisciplinary teams covering both domains was deemed resource-intensive by P7.

Looking forward, several participants (P1, P2, P9, P10) believed that most organizations are moving toward some form of integration: "*Most companies try to integrate IT and OT SOC. It's a commonly accepted truth that it should be*

one place" **(P2)**. However, P9 acknowledged that the path to full integration is gradual and constrained by technological and cultural factors. These findings illustrate how integrated SOCs reflect real-world compromises, enabling cross-domain insight and efficiency. Still, they must be carefully structured to avoid losing OT-specific competence and situational awareness.

Dedicated OT SOC offers strong contextual awareness, domain-specific expertise, and operational autonomy. P11 and P3 emphasized that such setups can lead to faster, more informed responses to process-level anomalies and are typically found in larger or high-risk industrial sectors. P12 explained the business continuity benefits for OT systems: "*We established a dedicated OT SOC strategy to ensure it can operate independently. If the enterprise network goes down, OT operations must continue*".

However, participants also reported significant challenges. The IT/OT coordination was considered reduced by P11, limiting the visibility across attack chains: "*you risk missing how an attack moves from IT into OT*". Moreover, implementation can be complex in practice. P5 reflected on an attempt where his company sought dedicated OT monitoring: "*the team that ran it didn't have actual responsibility, and it fell between the cracks. We learned that you need experts with time and mandate to monitor OT properly*". While OT SOCs provide valuable focus and specialization, they require strong governance and deliberate coordination mechanisms to avoid operational silos.

In-house OT SOCs are developed and operated internally by an organization, offering high levels of control, contextual knowledge, and alignment with internal systems and processes. P7, P3, P6, and P10 largely agreed that this model provides the most operationally effective approach for organizations with sufficient resources. According to P3, these setups are particularly valued in domains such as manufacturing and energy, where OT visibility and rapid response are essential. Meanwhile, P2, P6, P8, and P11 emphasized the proximity to facilities and operational staff as a key enabler of meaningful detection and triage.

However, P6 also highlighted that in-house OT SOCs are expensive to build and sustain: "*The main challenge would be having enough capacity to develop high-quality detections*". Staffing and training demands are high, and smaller organizations often struggle to support full-time OT monitoring teams. P10 noted that only major players in an industry tend to pursue in-house SOCs: "*They're big vendors. They have the infrastructure and money. Running a SOC is extremely expensive, so I doubt most companies will do it themselves*". While seen as the most capable model, in-house OT SOCs are viable primarily for large organizations.

Outsourcing OT SOC functions is a common strategy, particularly among small and medium-sized enterprises (SME) lacking the economic and human resources for in-house capabilities. Traditional MSSPs and vendor-operated SOCs emerged as the most common options. MSSPs were often selected for their cost-effectiveness and ability to meet compliance requirements (e.g., NIS2). Five participants

(P1, P2, P4, P6, and P10) noted that MSSPs enable organizations to scale their monitoring capabilities without having to build teams from scratch. However, P8 warned that MSSPs may lack the operational context needed for effective OT monitoring: "*Without integration with the customer, SOC analysts treat alerts like IT issues, which completely misses the mark*". P6 also highlighted the challenge of outsourced services in understanding process-specific, in-depth knowledge at scale: "*In OT, everything is different. Without knowing the context, even normal activities like logging in may trigger unnecessary alerts*".

Vendor-operated SOCs are typically run by the system suppliers delivering large parts of the OT infrastructure. P4 highlighted the benefit of the in-depth system knowledge that the SOCs have access to: "*Since they already know the systems and hold the long-term service contract, they are clearly best positioned to understand what's going on*". However, they might have a too narrow scope and a lack of integration with IT operations: "*We have a control system SOC that sees only its small world. If an attack starts on IT, they may not even notice*" **(P6)**. The findings suggest that success in these models relies on close collaboration and shared understanding between the service provider and the operational environment.

4.2 Future OT SOC models

Seven participants (P1, P2, P3, P4, P6, P7, P10) anticipated that OT SOC models would continue to evolve along two main paths: increased outsourcing to MSSPs and selective investment in in-house capabilities. Regulatory developments are expected to drive more organizations toward outsourcing to achieve compliance: "*Given NIS2 and national legal requirements, I think more Norwegian companies will turn to MSSPs for some form of OT monitoring to meet those demands*" **(P10)**. Nonetheless, P4 suggested that future SOC models will depend heavily on sector-specific needs, risk tolerance, and available resources.

Four participants (P1, P14, P6, and P12) expressed optimism about AI's ability to support, not replace, analysts in OT SOCs. P1 emphasized AI's utility in long-term detection, noting its ability to identify behaviors that are difficult for humans to recognize. P14 shared a similar use case, focused on rare and slow-moving attack activity: "*The actors that come with a little ping every 5 months [...] it is things like that AI can help you with, to create patterns*". Analyst fatigue could be further mitigated by adopting AI. P6 considered AI as a first-line filter or triage system, enabling human analysts to focus on interpretation and response. P12 mentioned AI's potential to enhance detection platforms and reduce manual effort in rule creation. "*Having SIEM tools with out-of-the-box OT detections or AI that understands OT protocols would reduce the amount of manual work*".

Despite optimism about AI's support role, participants also highlighted significant disadvantages. Data privacy and governance concerns involving training AI on sensitive or proprietary information can introduce risks: "*We worry about*

confidentiality [...] if we train AI on confidential attack trees, can others derive them from the model?" **(P3)**. Beyond data concerns, the same participant further stressed that analysts must retain interpretability and control: "*AI and analyst work must go hand in hand. If analysts can't explain what the AI found, that's a problem*" **(P3)**. These concerns reflect a broader reluctance to adopt AI for its own sake, particularly in high-stakes environments.

Although MSSPs will likely play a growing role, in-house SOCs remain a strategic option for organizations with high security requirements, operational complexity, or regulatory exposure. While AI may assist with detection, decision-making in OT must remain under the control of knowledgeable individuals. A mature OT SOC must be purpose-built, context-aware, and collaborative, with capabilities spanning technical, operational, and organizational domains. Table 5 summarizes the key capabilities identified by the participants for the future SOC models monitoring OT systems. While OT SOC should monitor and understand traffic at the process control layers, an IT/OT SOC might not require the same in-depth knowledge. Hence, not all requirements might be a perfect fit for both SOC models.

5 Discussion

Interviews revealed significant diversity in how organizations design and operate OT SOCs. No single SOC model emerged as dominant, since factors such as organizational size, sector, resources, and sectoral or national regulations influenced the selection. Integrated SOCs and OT SOCs were implemented through in-house, MSSP-operated, or vendor-operated models, and occasionally combined in integrated forms. Each model presents trade-offs in detection capability, cost, and operational integration. By comparing OT SOC models, this study provides insights for security leaders, system integrators, and policymakers. The comparative framework highlights trade-offs often implicit in discussions about SOCs, enabling more transparent, criteria-driven decisions.

5.1 Future directions for OT SOC models

Norwegian organizations employ a spectrum of SOC models, ranging from MSSP-based monitoring for SMEs to entirely in-house OT SOCs for large utilities. However, challenges remain consistent across models: difficulties in achieving contextual awareness, a shortage of skilled personnel with dual IT/OT expertise, and limited applicability of IT-centric tools in deterministic, safety-critical OT environments. A recurring theme was the gradual, incremental nature of change in OT environments. Unlike IT, which is accustomed to rapid iteration, OT systems evolve slowly and are often constrained by legacy equipment, long system lifespans, and strict safety and uptime requirements. Participants consistently emphasized that SOC maturity in OT must reflect this reality.

One major direction involves expanding sensor coverage and telemetry depth, in particular for the dedicated OT SOC model. Some participants were asked to

Table 5. Key Capabilities of a Future SOC-models monitoring in OT with the current maturity for each capability. 🟡 indicates moderate, 🟠 low to emerging, while 🔴 is low maturity.

Capability with a brief description		**Current Maturity**
Visibility and Telemetry: Asset inventory, passive network monitoring, and CMDB integration. Limited by legacy systems.	🟡	Site-dependent; legacy systems pose challenges
Interdisciplinary Staffing: Combine IT, OT, and automation skills; promote cross-functional collaboration	🟡	Cultural and domain gaps
Detection Engineering: Tailored detections for OT protocols and weak signals; maintain use-case backlog	🟡	Requires tuning with OT input
Automation: Reduce analyst load via alarm enrichment, baseline checks, and documentation	🟡	Limited automation in most environments
External Collaboration: Coordinate with MSSPs, vendors, and site personnel during detection and response	🟡	Stronger with MSSPs; variable with vendors/sites
Behavioral Baselines and Context Awareness: Understand "normal" operations using traffic patterns and operational context (e.g., maintenance, shifts)	🟠	Baselines are common; contextual integration remains rare
IT-OT Integration: Bridge attack visibility across domains via integrated detection and response	🟠	Technically feasible but organizationally difficult
Continuous Learning and R&D: Support pilots, testbeds, and research initiatives to adapt to evolving threats	🟠	Resource-dependent and inconsistent
Operational Exposure for SOC analysts: Site familiarity through field exposure, lab time, or event simulation	🔴	Rarely practiced systematically
Process Monitoring in SOCs: Monitor real-time control behaviors to detect abnormal process activity	🔴	Aspirational in most organizations

Note: Maturity levels reflect the authors' subjective interpretations from interviewed practitioners and general industry observations. We expect that the ratings may vary significantly by sector, region, and organizational maturity.

envision an "ideal future" where they mentioned endpoint telemetry and network data that are collected across all Purdue levels, especially deeper into the process control systems (Level 1–2). However, this vision is tempered by technical, financial, and safety concerns. While a few organizations are experimenting with deeper visibility, many remain skeptical of its feasibility and value. Schönig et al. [19] caution against assuming that innovation in OT SOCs can mirror IT's pace, emphasizing the need for process-aware and risk-sensitive approaches. At the same time, previous works have proposed a layered SOC architecture specifically designed to enable process-level monitoring using protocol-aware sensors and telemetry pipelines tailored to industrial constraints [9]. Their work underscores the need for enhanced visibility while also highlighting the practical limitations, particularly in brownfield environments where legacy constraints can restrict deployment.

Both the literature and practitioners anticipate a move toward integrated SOCs that combine in-house OT expertise with outsourced 24/7 monitoring.

Integrated SOCs are often presented as improving cross-domain visibility and operational efficiency by integrating IT and OT monitoring [9,6]. However, practitioners in this study stressed that cost and staffing constraints were equally important drivers, particularly for SMEs. Conversely, dedicated OT SOCs are promoted in literature for their depth of domain expertise and process safety focus [14,20], a view echoed by participants. However, the interview findings revealed a trade-off in reduced visibility into IT-originated attack vectors, which is an aspect often overlooked in studies. Federated and sectoral SOC concepts are also seen as promising ways to address skill shortages and cost constraints, though governance and trust questions remain unresolved.

AI and automation also feature heavily in participants' views of the future, but with strong reservations. AI is primarily considered as a supportive tool for triage, pattern recognition, and alert prioritization. Some works [17] concur with the interview findings. However, others [1] emphasize the need for human oversight and rule-based constraints. However, both sides acknowledge the need for human oversight and explainability.

5.2 Recommendations for Selecting a SOC Model

Recommendations for determining the right SOC model are related to organization size, OT complexity (i.e., the degree of asset/vendor heterogeneity, monitoring visibility limits, process criticality and safety constraints, vendor restrictions, and the level of IT/OT coupling and local context required), and regulatory environment. The recommendations reflect trade-offs observed in both the literature [24,4,15,19] and the interviews. For smaller SMEs with limited budgets and staff, an MSSP-based integrated SOC is a pragmatic choice, as it provides baseline monitoring at a lower cost, albeit at the expense of deep OT specialization. Mid-sized manufacturers often operate more diverse OT environments and face stricter compliance demands. For them, an integrated in-house or outsourced SOC with a dedicated OT-focused sub-team enables stronger correlation between IT and OT events while maintaining necessary process insight. In contrast, large multi-site utilities, particularly those subject to NIS2 or sectoral critical infrastructure regulation, require the resilience, availability, and process expertise that aligns with what an in-house OT SOC can provide. This stratification emphasizes that model determination is less about adopting a "optimal" model universally, and more about aligning SOC design with organizational scale, OT complexity, and external regulatory drivers.

5.3 Limitations and Future Work

The findings emphasize that model selection must align with operational priorities and constraints rather than adopting a generic "best practice". SOC model choices will increasingly be shaped not only by internal constraints, but also by the maturity of IT and OT infrastructure, regulations, and tools across industrial sectors. For policy-makers, the results highlight the importance of developing

standards and guidance that distinguish between SOC models, not only technical controls. Future work includes investigating empirical, cross-sector evidence to validate proposed models, particularly metrics that can benchmark the effectiveness of integrated and federated SOCs. The empirical findings and literature highlight several research directions and recommendations for policy-makers for future OT SOC models:

- **Integrated SOC models**: Future research should provide findings on the advantages and challenges of combining in-house OT expertise with MSSP-provided 24/7 monitoring to balance context retention with coverage. This is especially attractive to SMEs that cannot sustain a dedicated OT SOCs on their own.
- **Process-aware monitoring**: Although research is emerging on this topic [13,3], research needs to identify methods of integrating control process data into SOC detection pipelines to identify anomalies beyond network or host events.
- **Selective automation**: Use of SOAR and AI-driven enrichment for triage, while maintaining human oversight in safety-critical decision points, due to the deterministic nature of OT [22].
- **Federated SOC concepts**: For SMEs, sectoral or national SOC models may be a solution for complying with regulations when OT security expertise is scarce. Still, the lack of practical guidance and unresolved governance challenges hinder the development of such SOC models.

This study is limited to the Norwegian context and to a qualitative sample, which might limit generalizability with different regulatory or operational requirements. Rapidly changing regulations, such as NIS2, could shift SOC practices over time. Future work should include conducting similar qualitative studies to facilitate cross-national comparisons, longitudinal studies tracking the evolution of SOC, and quantitative benchmarking of SOC models based on incident response performance, detection coverage, and cost-effectiveness metrics.

6 Concluding Remarks

This study explored the diverse landscape of SOC models in OT environments, addressing a critical gap in the literature and industry practice. Through semi-structured interviews with 14 professionals across industrial sectors, we identified and analyzed the implementation of integrated, dedicated, in-house, outsourced, and vendor-operated SOC models. Each model presents distinct trade-offs in terms of contextual awareness, cost, operational resilience, and IT/OT integration. This is the first step in classifying the emerging SOC models for various critical infrastructures.

The findings emphasize that SOC model selection is not a one-size-fits-all decision but is shaped by organizational size, OT complexity, and regulatory pressures. These insights contribute to a more nuanced understanding of SOC design in OT contexts, offering practical guidance for organizations seeking to align their security operations with operational realities and regulatory demands.

Acknowledgments. This research was conducted as a part of a master's thesis submitted in June 2025 at Norwegian University of Science and Technology (NTNU), and was funded by the Norwegian Research Council through *Cybersecurity Barrier Management*, grant no. 326717, and *Norwegian Center for Cybersecurity in Critical Sectors (NORCICS)*, grant no. 310105. The authors would like to thank the interviewees partaking in the study.

References

1. Al-Dahasi, E., Khan, F.A.: Automating Security Incident Response in SCADA Systems through SIEM-ML Integration. In: 2024 29th International Conference on Automation and Computing (ICAC). pp. 1–10 (Aug 2024). https://doi.org/10.1109/ICAC61394.2024.10718780
2. Alahmadi, B.A., Axon, L., Martinovic, I.: 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms. In: 31st USENIX Security Symposium (USENIX Security 22). pp. 2783–2800 (2022), https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi
3. Asiri, M., Arunasalam, A., Saxena, N., Celik, Z.: Frontline responders: Rethinking indicators of compromise for industrial control system security. Comput. Secur. **154** (Jul 2025). https://doi.org/10.1016/j.cose.2025.104421
4. Cojocar, L., Razavi, K., Bos, H.: Off-the-shelf Embedded Devices as Platforms for Security Research. In: Proceedings of the 10th European Workshop on Systems Security. Association for Computing Machinery, Belgrade, Serbia (2017). https://doi.org/10.1145/3065913.3065919
5. Cotiga, M., Pedersen, J.M., Dushku, E.: Cyber Resilience in OT: Characteristics and Security Challenges. In: 2024 IEEE International Conference on Cyber Security and Resilience (CSR). pp. 750–756 (Sep 2024). https://doi.org/10.1109/CSR61664.2024.10679463
6. Dimitrov, W., Syarova, S.: Analysis of the Functionalities of a Shared ICS Security Operations Center. In: 2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE). pp. 1–6 (Nov 2019). https://doi.org/10.1109/BdKCSE48644.2019.9010607
7. Dragos: Dragos 8th annual year in review 2025. Tech. rep., Dragos (2025)
8. Flå, L.H., Thieme, C.A., Jaatun, M.G., Hanssen, G.K.: Cybersecurity challenges in industrial control systems: An interview study with asset owners in norway. In: Computer Security. ESORICS 2024 International Workshops. pp. 425–438. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-82349-7_27
9. Gaggero, G.B., Caviglia, R., Girdinio, P., Marchese, M.: Toward a Security Operation Center for Operational Technology in Industrial Networks. In: 2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense). pp. 160–164 (Nov 2024). https://doi.org/10.1109/TechDefense63521.2024.10863654
10. Gnanasekaran, V., Bartnes, M., Grotan, T.O., Heegaard, P.E.: Cyber-incident Response in Industrial Control Systems: Practices and Challenges in the Petroleum Industry. In: Proceedings of the 2024 ACM/IEEE 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) and 2024 IEEE/ACM Second International Workshop on Software Vulnerability. pp. 53–60. ACM, Lisbon, Portugal (2024). https://doi.org/10.1145/3643662.3643958

11. Gnanasekaran, V., Grøtan, T.O., Bartnes, M., Heegaard, P.E.: Rethinking Independence in Safety Systems. In: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, pp. 153–166. Springer Nature Singapore, Singapore (2024). https://doi.org/10.1007/978-981-99-6974-6_9
12. Kokulu, F.B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., Ahn, G.J.: Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. p. 1955–1970. ACM, New York, NY, USA (2019). https://doi.org/10.1145/3319535.3354239
13. Kuchar, K., Fujdiak, R.: Analyzing anomalies in industrial networks: A data-driven approach to enhance security in manufacturing processes. Comput. Secur. **153**(C) (Apr 2025). https://doi.org/10.1016/j.cose.2025.104395
14. Lota, S.: Making the Case for a Converged IT & OT Security Operations Center (SOC), https://www.nozominetworks.com/blog/making-the-case-for-an-it-ot-security-operations-center-soc
15. Novak, J., Hueca, A., Rodman, C., Perl, S., Breaux, T., Valdengo, J.: Building a Better SOC: Towards the Ontology for Security Operations Center Assistance and Replication (OSCAR). Digital Threats **6**(1), Article 6 (2025). https://doi.org/10.1145/3722233
16. Ofte, H.J.: The awareness of operators: a goal-directed task analysis in SOCs for critical infrastructure. International Journal of Information Security **23**(5), 3253–3282 (Oct 2024). https://doi.org/10.1007/s10207-024-00872-6
17. Perera, U.N.A., Rathnayaka, S., Perera, N.D., Madushanka, W., Senarathne, A.N.: The Next Gen Security Operation Center. In: 2021 6th International Conference for Convergence in Technology (I2CT). pp. 1–9 (Apr 2021). https://doi.org/10.1109/I2CT51068.2021.9418136
18. Reyna, A., Collins, T., Hossain-McKenzie, S., Blakely, L., Goes, C., Anderson, R., Hubbell, C.: Towards the design of grid cyber-physical integrated security operations center visualizations. In: 2024 IEEE Kansas Power and Energy Conference (KPEC). pp. 1–6 (2024). https://doi.org/10.1109/KPEC61529.2024.10676242
19. Schönig, S., Hornsteiner, M., Stoiber, C.: Towards Process-Oriented IIoT Security Management: Perspectives and Challenges. In: Augusto, A., Gill, A., Bork, D., Nurcan, S., Reinhartz-Berger, I., Schmidt, R. (eds.) International Conference on Business Process Modeling, Development and Support. vol. 450, pp. 18–26 (2022). https://doi.org/10.1007/978-3-031-07475-2_2
20. Shahjee, D., Ware, N.: Integrated Network and Security Operation Center: A Systematic Analysis. IEEE Access **10**, 27881–27898 (2022). https://doi.org/10.1109/ACCESS.2022.3157738
21. Staves, A., Maesschalck, S., Derbyshire, R., Green, B., Hutchison, D.: Learning to walk: Towards assessing the maturity of ot security control standards and guidelines. In: 2023 IFIP Networking Conference (IFIP Networking). pp. 1–6 (2023). https://doi.org/10.23919/IFIPNetworking57963.2023.10186424
22. Tariq, S., Chhetri, M.B., Nepal, S., Paris, C.: Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. ACM Comput. Surv. **57**(9), Article 224 (2025). https://doi.org/10.1145/3723158
23. Tjora, A.: Qualitative research as stepwise-deductive induction. No. 26 in Routledge advances in research methods, Routledge, Abingdon, Oxon New York, NY (2019)
24. Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G.: Security Operations Center: A Systematic Study and Open Challenges. IEEE Access **8**, 227756–227779 (2020). https://doi.org/10.1109/ACCESS.2020.3045514