Influencing Factors of Security Operations Center (SOC) Analysis and Decision-Making for Operational Technology (OT): An Exploratory Study

Vahiny Gnanasekaran[1,2], Ken Stabekk[2], Tobias Dubland Nilsen[2], Thomas Grønbakk Nilsen[3], and Poul Einar Heegaard[2]

[1] SINTEF Digital, Trondheim, Norway
vahiny.gnanasekaran@sintef.no
[2] Norwegian University of Science and Technology, Trondheim, Norway
{firstname}.{lastname}@ntnu.no
[3] mnemonic AS, Oslo, Norway

Abstract. Industrial companies and critical infrastructure are increasingly adopting Security Operations Centers (SOCs) to monitor their Operational Technology (OT) systems. As IT and OT converge, critical infrastructure and operational systems face more complex cybersecurity threats. While SOCs are well-established in IT systems, OT systems differ in priorities, technologies, operational constraints, and real-world consequences. This study investigates the factors that influence analysis and decision-making processes within OT SOCs and explores how IT SOC maturity models can inform OT SOC development. It reports on a qualitative study involving 15 OT security professionals from Norwegian industry. The interviews revealed that OT SOC analysis depends not only on technical telemetry but also on analysts' contextual knowledge, process insight, and exposure to the plant environment. Experience, asset criticality awareness, and alert contextualization emerge as key enablers, while fragmented tooling, limited cross-functional communication, and divergent maturity frameworks constitute persistent barriers. The paper contributes empirically grounded insights for researchers and OT security practitioners seeking to enhance security monitoring in industrial environments.

Keywords: Security Operation Center · Operational Technology · SOC analysis

1 Introduction

Operational Technology (OT) environments are increasingly exposed to cyber threats as Information Technology (IT) and OT networks converge. While this convergence enables remote operations, data-driven monitoring, and improved efficiency, it also expands the attack surface of industrial systems [35].

Several recent incidents demonstrate how Large Language Model (LLM)-based cyberattacks against OT environments can lead to physical consequences. Attacks targeted wind and photovoltaic farms, a private manufacturing company, and a large combined heat and power plant supplying heat to half a million Polish customers [36]. The attack targeted Remote Terminal Units (RTUs), protection relays, serial device servers, and Windows environments. According to Dragos [11], a Mexican municipal water utility was further struck by a cyberattack in which the adversary used LLMs for reconnaissance, environment mapping, tooling development, and intrusion planning. The attack was not autonomous process manipulation, but the reduction in time, expertise, and effort required for IT intruders to identify OT crown jewels and operationalize known attack paths [11] is alarming.

To address these risks, industrial organizations are increasingly adopting OT Security Operations Centers (OT SOCs). An OT SOC is a security function responsible for monitoring, detecting, analyzing, and responding to cyber threats in OT systems and can be classified as outsourced, hybrid, or in-house, depending on the service's origin [19]. Unlike traditional (IT) SOCs, OT SOCs should consider operational, technical, and safety-related characteristics of the industrial environments [12]. These socio-technical needs in OT SOC log analysis show that it depends not only on technical telemetry but also on operational context and collaboration between security and OT personnel.

Although SOCs have been widely studied in IT environments, research specifically addressing the technical and organizational aspects of OT SOCs remains limited [38,19]. Previous work has examined IT SOC analysts' situational awareness in critical infrastructure [30], IT SOC maturity and operation [24], as well as broader challenges for OT security [45]. Because of the complexity of different fields and priorities, other factors may also influence OT SOC analysis and decision-making. To this end, the study addresses the following research questions:

RQ1 How can the maturity development of OT SOCs be informed by insights and practices from IT SOCs?

RQ2 What factors influence the OT SOC analysis process?

This paper presents an exploratory, qualitative interview study with 15 industry professionals involved in OT security and OT SOC operations, and makes three research contributions. First, it advances a conceptual understanding of OT SOC maturity by showing how IT SOC practices can inform OT SOC development. Second, it identifies key factors influencing OT SOC analysis, extending current knowledge of analyst decision-making in OT environments. Third, it provides empirical insights into analyst workflows and information needs that can inform the design of future AI-assisted OT SOC capabilities.

2 Background & Related Work

A SOC is an organizational function responsible for monitoring, identifying, and responding to cybersecurity threats and incidents affecting an organization's

IT and/or OT environments [24]. SOCs typically possess various capabilities, including real-time monitoring, alert triaging, log collection and forensic analysis, as well as proactive activities, such as threat hunting and collecting cyber threat intelligence (CTI) [27,24,10]. Existing literature describes SOCs using a tiered analyst structure, where lower-tiered analysts can escalate unresolved issues to higher-tiered analysts. Higher-tiered analysts typically handle more specialized tasks [23], and experience tends to increase with higher tier levels [24].

The introduction and rapid development of AI may pose additional challenges for organizations already struggling to monitor their current OT networks. Adversaries are increasingly combining conventional IT intrusion techniques with OT-specific knowledge, destructive tooling, and abuse of remote access [13]. OT SOCs are relevant because they provide the operational visibility, contextual analysis, and coordinated response capabilities needed to defend industrial environments amid evolving threat conditions. Defenders need the ability to detect, investigate, and respond to adversary activity before it develops into loss of view, loss of control, or physical process disruption.

2.1 OT SOC Architectures

While IT and OT SOCs share the same core objectives, their operating conditions differ significantly. OT SOCs must consider factors such as legacy technologies, safety-critical environments, real-time operational constraints, and sector-specific regulatory requirements [19,14,24,15]. Figure 1 shows an overview of different SOC architectures. All architectures reflect different structural and operational choices implemented in practice.

A unified SOC could have separate or interdisciplinary analysts managing different alarms based on their areas of expertise [14]. Although the approach enables potential for more seamless response capabilities, it can also lead to a lack of focus on OT monitoring [32]. *Dedicated SOCs* operate exclusively for OT, but can be more costly to operate and maintain than a unified SOC [15,12]. Deployments of OT SOCs can be handled internally or externally: *in-house OT SOCs* can be deployed by companies with sufficient budgets to invest in staffing and other resources. An *outsourced OT SOC* to a Managed Security Service Provider (MSSP) can prove to be more cost-effective for companies [2,19].

2.2 OT Monitoring and Detection

Traditional IT security tools are designed for IT systems, where data confidentiality, user accessibility, and scalability are the main objectives. In contrast, OT environments concern operational continuity, safety, and system availability [9]. These tools are often unsuitable for OT environments because of incompatibility with legacy devices, proprietary protocols, performance constraints, mixing new and legacy technology (brownfield systems), and the risk of disrupting critical processes [9]. While Endpoint Detection and Response (EDR) is widely used in IT, vendor-imposed restrictions or the constrained resources of OT devices can

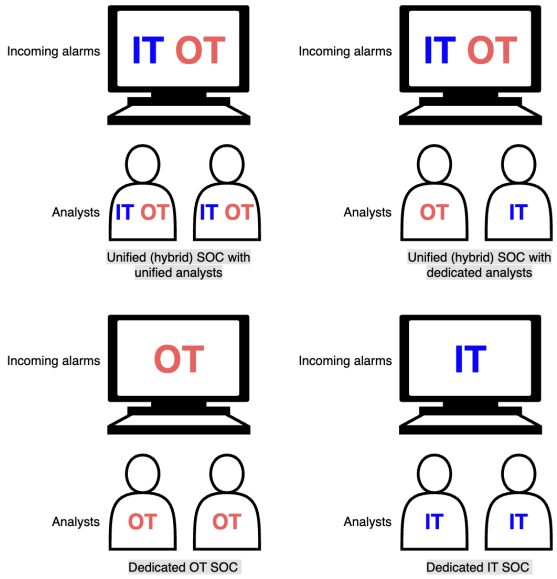

Fig. 1. Different SOC architectures, adapted from Gnanasekaran et al. [19]

limit its adoption in OT environments. When EDR has been used, it has been useful for detecting and mitigating Advanced Persistent Threats (APTs) [22].

Meanwhile, Intrusion Detection Systems (IDSs), grouped into anomaly-based and signature-based detection, vary in their detection accuracy and false-positive rates [21]. Existing work [31] has developed an IDS that continuously learns from industrial network traffic patterns. Previous work, combined with AI capabilities, investigates how to apply domain-specific knowledge to IDS [33]. Network IDSs are also used in OT systems for their passive network monitoring, without modifying or disrupting communications [15]. Because OT systems are often deterministic [9,20], anomaly detection can provide useful packet capture and log correlation for traffic inspection and protocol analysis.

Another key technology utilized in OT SOCs is Security Incident and Event Management (SIEM) platforms. SIEM platforms collect, aggregate, analyze, and correlate logs from different sources to identify patterns, analyze cyber incidents, and prevent attacks with real-time alerting [8,15]. Security Orchestration, Automation, and Response (SOAR) platforms are widely used in IT SOCs but are very limited in the OT context. Although conventional SIEM platforms can provide OT capabilities, additional customization and configuration through Security Operations and Event Management (SOEM) can enable Supervisory control and data acquisition (SCADA) system input for monitoring without constraining the operational environment [6].

2.3 OT SOC Analyst Responsibilities

Since the technical aspects of OT SOCs differ from those of traditional SOCs, this further demands modifications to SOC analysts' tasks in OT SOCs. The tiered SOC model assigns different roles and responsibilities based on the SOC's scope and size [39]. Although certain IT SOC tasks can be addressed by AI tools [44,16], current OT SOC analysts conduct one or more of the following tasks:

1. **Alert prioritization** and triaging are conducted based on severity and availability of safety and security resources [19].
2. **Data collection** from other industrial systems and input from safety-domain experts and customers can enrich alerts.
3. The analysts can also perform **threat hunting** using Cyber Threat Intelligence sources to identify vulnerabilities or malware affecting OT or safety-critical systems.
4. When an incident is escalated, a SOC analyst can participate in **incident response** through the MSSP or a customer-specific Computer Security Incident Response Team (CSIRT).

Previous work on AI tools in SOCs [44] mostly focuses on the first three parts of the NIST CSF 2.0 framework, namely identify, protect, and detect, while respond and recover are underrepresented [16]. This gap suggests that OT SOC analysts are still needed to perform these stages, given the complexity of integrating safety and security processes and knowledge.

2.4 Related Work

SOC research has traditionally centered around IT environments, where tools, processes, and organizational models are more mature [24,2]. Kokulu et al. [23] identify the technical and organizational challenges in SOC environments, such as limited visibility across networks and endpoints, and differences in expectations between management and SOC personnel.

Studies also highlight that effective SOC analysis depends on more than automated data collection. Ofte [30] focused on how SOC analysts develop and use situational awareness in their work (e.g., information gathering, interpretation, and transitioning to operational measures). Effective OT incident response across multiple internal and external roles (e.g., SOCs, CSIRTs, emergency response teams, OT personnel, and on-site staff) depends on technical detection, coordination, role clarity, and collaboration between cyber and operational stakeholders [18]. Technical detection of Indicators of Compromise (IoC) in OT systems shows that anomaly detection in OT environments requires analysts to understand and interpret the operational context and distinguish abnormal activity from normal process behavior [4]. Socio-technical challenges, such as communication silos and pressure to maintain continuous production, may delay anomaly escalation and increase the risk of overlooking early signs of faults or cyber incidents.

Previous work [19] examines the current state of OT SOCs in Norway by exploring trends, challenges, and opportunities for improvement. It offers a highly relevant basis for the work by showcasing the operational and organizational conditions that shape OT SOC capabilities. While the study provides a solid foundation for understanding OT SOC models and their current status in Norway, it does not examine in detail the data sources and influencing factors required for OT SOC analysis and decision-making.

Overall, the literature shows that SOC effectiveness depends on different factors such as visibility, contextual awareness, correct tooling, and organizational alignment. However, SOC literature still remains centered on IT, while the emerging OT SOC literature tends to focus on SOC models and general organizational challenges. Less attention has been given to factors that shape OT SOC analysis and decision-making, including how information is identified, accessed, and used; what influences OT SOC analysis; and current analytical workflows. There is also limited literature on how practices from IT SOC maturity development have informed or supported OT SOCs. Understanding the factors influencing OT SOC analysis helps clarify how the process should be addressed.

3 Study Set-up

The study objective was to gain insights into factors in OT SOC analysis and potential areas for improvement in OT SOCs. Figure 2 depicts how the study was achieved through a literature review and two iterations of interviews. The semi-structured interviews allowed participants to share experiences, challenges, and other insights that would otherwise have remained unexplored. This section outlines the procedures for the literature review, data collection, analysis, and sampling.

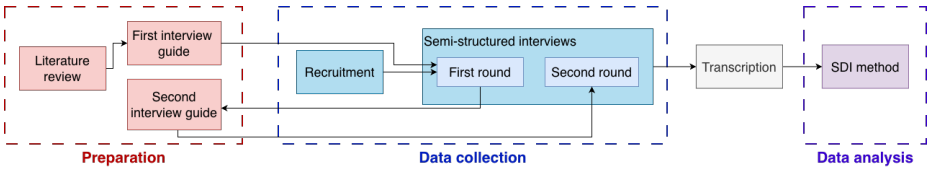

Fig. 2. The full study set-up.

3.1 Literature Review

A literature review was conducted to identify, screen, and synthesize relevant academic and industry sources as a preparation for the interview study, complying with the PRISMA (Preferred Reporting Items for Systematic Reviews

and Meta-Analyses) guidelines [34]. The search strings were used to search for relevant papers in six academic databases: *Scopus*, *ACM*, *Springer*, *IEEE*, *Web of Science*, and *ScienceDirect*.

The results from the databases were managed in *Zotero*, and later transferred to *ASReview*, an open-source tool that uses AI to assist with the screening process [5]. The screening process was conducted using a data-driven approach [37], with a threshold of 40 consecutive irrelevant articles for searches related to RQ1 and 80 for RQ2. A total of 3388 results were found, and the final corpus after screening and review was reduced to 15, based on the exclusion and inclusion criteria depicted in Table 1.

Table 1. Inclusion and exclusion criteria for the literature selection.

Inclusion criteria	**Exclusion criteria**
Addresses OT, ICS, SCADA, or critical infrastructure security, or SOCs.	Published before 2015.
Discusses SOCs, their evolution, development, best practices, and challenges.	Non-English publications
Addresses OT SOC-related monitoring, analysis, incident response.	Non-Access to full-text.

3.2 Interviews

Recruitment Participants were recruited using convenience and snowball sampling. They were selected based on their experience and direct relation to OT security and OT SOC-related operations. The target sample included OT security engineers, IT/OT SOC analysts, OT security consultants, managers, C-level executives, and researchers specializing in OT security. Initial participants were recruited through industry forums, *LinkedIn*, and email.

Interview Procedure Interviews were conducted through video conferencing using *Teams*. All participants were informed about the purpose of the study, the data collection procedures, and how the data would be stored, processed, and used. They were also made clear that participation was voluntary, and written consent was obtained. Interviews were audio-recorded and later transcribed. The interviews lasted approximately 60 minutes, depending on the participant's engagement and availability. The first interview guide was developed and addressed the following topics:

- The overall OT SOC workflow, including detection, analysis, event escalation, and decision-making
- How information and data sources are identified, accessed, and used during OT incident analysis

- Alert management for analysts with insufficient technical or operational context
- Factors currently influencing analytical and decision-making in OT SOCs
- Bottlenecks and challenges
- Potential knowledge transfers between IT SOC and OT SOC practices
- Future development of OT SOC capabilities

Follow-up questions were based on participants' responses to encourage elaboration and clarification. The interview guide was revised based on feedback and responses from the first six participants (P1-P6 in Table 3) to ensure the questions remained relevant to technological developments. The revised interview guide for the remainder of the sample was extended with the following topics:

- Identifying information and data sources for OT SOC analysis.
- Operational constraints affecting incident response.
- Differences across organizational sizes, greenfield vs. brownfield, and industrial sectors.

All interview recordings were transcribed using a transcription tool for the Norwegian research sector, based on Whisper and hosted and used only by the Norwegian research sector. The transcripts were anonymized and given aliases to remove company names and specific technologies, and all Personally Identifiable Information was removed before data analysis.

Data management and Ethics Prior to participation, the interviewees received a consent form describing the study purpose, data collection procedures, data processing, data access, and consent withdrawal. Written consent was then obtained via *Nettskjema*, which required a Digital ID or an equivalent for secure identification. Verbal consent was also given at the beginning of the interview. All data processing was conducted in accordance with the General Data Protection Regulation. The study was approved by the Norwegian Agency for Shared Services in Education and Research. Interview recordings and transcriptions were stored on an institutionally approved infrastructure that was encrypted and access-controlled.

3.3 Data Analysis

An inductive coding approach was used to analyze the interview data, which is well-suited to the semi-structured interview format and the exploratory nature of this study [46]. The approach allowed the natural development of themes from participants' own words, rather than being constrained by predefined categories. The analysis and coding process was conducted in *NVivo 15*, a qualitative data analysis software. Coding was performed in English to ensure consistency, with statements coded in both English and Norwegian to retain their original connotation.

Initial codes were developed inductively, guided by themes from the interview guide and general impressions from interviews conducted. The analysis

followed the Stepwise Deductive-Inductive (SDI) method [46], emphasizing iterative movement between empirical data and analytical movement. The interview transcripts were systematically coded and organized into eleven parent nodes. Each of them represented a broader thematic area, and its child nodes contained sub-themes. Table 2 outlines the broader coding categories and the number of codes within each. Although 647 codes were identified in the initial iteration, only 546 codes across seven parent nodes were deemed relevant for this study.

Table 2. Parent codes with the number of codes and descriptions in descending order.

Parent Code	**Relation to RQ**	**# Codes**	**Description**
Current State of OT SOCs	RQ2	157	Views on the current state of OT SOCs and OT security, and how they affect OT SOC analysis.
OT SOC Analyst Workflow	RQ1, RQ2	143	The general workflow of analysts, including alarm analysis and escalation, and other tasks.
Importance of contextual knowledge	RQ2	101	Views on contextual knowledge, its value, and factors affecting analysts.
OT SOC Analyst	RQ1, RQ2	54	Derives perspectives on what analysts experience, their challenges, and other themes related to them.
Practices from IT SOC to OT SOC	RQ1	45	Views on practices transferable from IT to OT SOCs.
Industrial customers	RQ2	24	Perspectives on how customer capabilities affect OT SOC analysis capabilities.
Future State of OT SOCs	RQ1, RQ2	11	Views on how OT SOC capabilities can evolve.
Greenfield vs. Brownfield	RQ2	11	Discusses the difference in analyzing events between new and older sites.

To maintain a consistent coding approach and ensure intercoder reliability (ICR), rigor and transparency in the coding process are necessary [29]. The study followed established ICR measures [7]. Two additional researchers were also included when disagreements arose or to assess the final coding scheme. In addition, regular communication and alignment discussions between the researchers were essential.

Data saturation from the interviews was treated in relation to the study's relevance and purpose, and discussed with other researchers involved in the study [41]. Since the second interview round generated few new codes and no parent codes, data saturation was deemed established.

3.4 Sample Description

Table 3 presents the sample description of the 15 interviewees. One participant had an international background, while the rest worked primarily in the Norwegian industry. Eight participants represented four MSSPs, five represented four industrial companies in the energy sector, two were OT security vendors, and two were from academia. The informants' experiences varied, with most having worked for 11+ years and six having worked in OT and security for over 20 years.

Table 3. Sample description of the interviewees. YoE stands for Years of Experience.

Informant	YoE	Position	Industry
P1	20+	OT Security Coordinator	OT Company 1
P2	20+	Manager OT Cybersecurity	MSSP1 & Industry
P3	0-4	OT Security Consultant	MSSP2
P4	20+	Head of OT Security	MSSP3
P5	20+	Head of OT Security	OT Company 2
P6	20+	Chief Technology Officer	OT Security Vendor 1
P7	5-10	OT SOC Analyst	OT Company 1
P8	5-10	OT SOC Manager	MSSP2 & OT Company 3
P9	0-4	IT/OT SOC Analyst	MSSP3
P10	5-10	IT/OT SOC Analyst	MSSP3
P11	20+	Senior Scientist OT	Academia
P12	11-20	CISSP	OT Company 4
P13	0-4	OT SOC Analyst	MSSP2
P14	5-10	Researcher	MSSP4 & Academia
P15	0-4	Security Consultant	OT Security Vendor 2

4 Results from the Systematic Literature Review (SLR) study

The SLR identified current knowledge, practices, and challenges discussed in the literature related to the RQs and informed the development of the interview guides. A total of 12 papers discussed SOCs explicitly, ranging from papers suggesting new technology to broader reviews of SOCs. Several papers were considered indirectly relevant through related focus areas, such as IoC [4] and digital twins [3]. Each paper was mapped to one or more RQs, along with its relevance and other contributions. The SLR identified 14 relevant papers, as shown in Table 4.

The SLR findings were used to refine the interview instrument by operationalizing research gaps, limitations, and future work suggestions identified in the literature. In particular, the revised interview guide expanded its focus on

Table 4. Classification of Papers by Relevance to RQs.

Paper	RQ1	RQ2	Relevance to RQs
Asiri et al. [4]		✓	Analyzes technical, human, and organizational factors affecting analysis.
Caviglia et al. [6]		✓	Evaluates IT SOC tools for use in OT environments.
Dimitrov & Syarova [12]		✓	Describes OT SOC functions and processes.
Gaggero et al. [15]		✓	Presents an OT SOC platform for monitoring and alert correlation.
Gnanasekaran et al. [18]		✓	Examines information aggregation and analysis in OT SOC.
Jacq et al. [28]		✓	Addresses shared situational awareness between SOC and operators.
Lohfink et al. [1]		✓	Proposes visualization support for anomaly detection and triage.
Nasr et al. [25]	✓	✓	Examines SOC efficiency and challenges in maritime OT.
Nganga et al. [26]		✓	Describes SOC monitoring and incident handling in maritime OT.
Ofte [30]		✓	Examines SOC operator awareness, decisions, and training needs.
Reyna et al. [40]	✓	✓	Addresses integrated visibility across IT, OT, and physical systems.
Sen et al. [42]		✓	Explores multi-source intelligence correlation for smart-grid cyberattack detection
Simola et al. [43]	✓		Examines IT/OT sensor correlation for OT threat detection.
Vielberth et al. [24]		✓	Summarizes IT SOC functions, workflows, and challenges.

contextual information needs, situational awareness, analyst expertise, visibility limitations, collaboration with operational personnel, and the transferability of IT SOC practices to OT environments. These additions enabled deeper exploration of areas that were identified in the literature but insufficiently studied in OT SOC settings. Appendix A provides more details on the selection of topics for the second round of interviews.

5 Interview Findings

This section reports the results of the qualitative data analysis, supplemented with quotes from the transcripts. PX (X=1-15) indicates the anonymized interview participant. The findings include participant quotes, with more descriptive text highlighted in grey boxes.

5.1 Practices From IT SOCs to OT SOCs

Most participants described IT SOC practices as a useful starting point for OT SOC development. Five participants (P1, P5, P9, P10, P13) were involved in designing and implementing their companies' OT SOCs. All five explained that they took inspiration from their IT SOCs. Two (P9, P10) began their careers as IT SOC analysts before working in OT at an MSSP. With their IT insights, both agreed that IT SOC maturity has already been achieved. P13, who started as an OT SOC analyst, further concurred with the maturity development from IT SOC.

OT SOCs differ from IT SOCs in alert management and decision-making during incident response. Even when similar detections or technologies are used, the response differs because of the potential for physical consequences: *"in IT, it is often shoot first, ask questions later. In OT, you can get fired for that"* (P3). OT SOC analysts adopt a cautionary approach when recommending countermeasures to alerts or incidents. While isolating devices, revoking sessions, or resetting passwords may be common in IT, participants (P3, P9, P13, P15) emphasized that such actions require further consideration in OT systems because they may affect production or safety. As a result, OT SOC analysts often have less autonomy than IT SOC analysts, and critical response decisions are typically escalated to OT personnel or operators with responsibility for the physical processes.

OT SOC analysts require different competencies and a mindset than IT SOC analysts. OT SOC analysts need to understand not only alerts and network activity but also the criticality and how OT components are embedded in physical processes: *"Where OT and IT differ is in understanding the context and the criticality."* (P8). P5 claimed that IT SOC analysts cannot simply be transferred into OT SOC roles without additional OT-specific knowledge and exposure. However, IT competence remains relevant because OT environments contain IT equipment and share a common networking infrastructure (P7, P12).

At the same time, participants emphasized that OT SOC maturity cannot be developed by simply copying IT SOC practices. As monitoring moves further into OT environments, the need for OT-specific context, process understanding, and operational awareness increases. P2 described maturity as a staircase, in which organizations may begin by monitoring IT components, network infrastructure, and the IT/OT boundary layers before gradually addressing more process-oriented networks. Future OT SOC practices were connected to the modernization of industrial environments. Greenfield facilities were described as important, since they can implement cybersecurity from the design phase. P10, P7 and P15 agreed that greenfield development enables security-by-design OT systems: *"if you go back 10 years, security was not that much important. Now we have solutions with security built into them"* (P7).

5.2 Influencing factors of OT SOC analysis processes

Three factors were mainly discussed by the interviewees, namely, site familiarity and OT system exposure, analyst experience, and process knowledge

Site Familiarity and Exposure to OT Environments Participants highlighted how site familiarity and OT exposure, including physical visits to sites and facilities, make a key contribution to gathering contextual knowledge. P4 explained how, in their view, critical it is to expose their SOC analysts to OT environments: *"They need to put on a suit and boots and spend time [...] in the environment."*. P4 further highlighted exposure as an important aspect of familiarizing themselves with the site and its infrastructure. One SOC analyst from the study, P7, explained how the site became less abstract during physical visits: *"When you see the systems in place, you understand why things are the way they are, and that knowledge gives you perspective when handling alerts"*.

Nevertheless, logistical challenges make such activities difficult to plan and execute, as specific sites also require entry certifications and permissions. Another issue, raised by P10, especially relevant for MSSPs, concerns scalability: *"it's neither sustainable nor scalable to send everyone [...] knowledge has to be transferred through documentation, training, and team experience"*.

Analyst Experience Eleven participants described analysts' accumulated experience and competence as an important factor in analyzing alerts in an OT SOC. P9 described how tacit knowledge enables swift interpretation of large amounts of information: *"Over time, experience will generate a gut feeling, which is something you quickly come to rely on as an analyst. You skim through a lot of information and quickly form an impression of whether this is normal or not based on the alert presented to you"* (P9). Analyst maturity is highly demanded in OT environments, where less experienced analysts may struggle to grasp the criticality of their work. P8 and P13 highlighted how escalation decisions of alerts are also linked to experience: *"You look for typical signs of malicious activity, and the analysis is largely experience-based"*.

Process knowledge Participants varied in the importance of depth of process knowledge. P11 expressed that too extensive process knowledge is unnecessary: *"You need to know what you are looking at, but needing deep knowledge is another question. At that point, you are moving into a different engineering field"* (P11). P1 and P4 viewed hands-on experience as relevant and needed: *"Operational understanding should not be necessary, as alert prioritization should cover it. However, it is important to understand how the facility uses its tools and machines, the relevant time horizons, and what it would take to carry out an attack"* (P1). On the other side, P8 and P7 emphasized familiarizing oneself with the organizational network as more paramount: *"It is not important for me to know what the process does, [...] I rely on those with the expertise to tell me that. My job is to monitor security. The more knowledge I have, the better, but it is not essential"* (P8).

6 Discussion

The study explores factors perceived to influence OT SOC analysis processes and discusses how insights and practices from IT SOCs may inform OT SOC maturity development. Rather than treating OT SOCs as a direct extension of traditional IT SOCs, the findings suggest that OT SOC development is shaped by interactions among security capabilities, industrial processes, and operational constraints. The findings provide exploratory guidance for practitioners and a basis for future empirical and technical investigations into OT SOC maturity.

6.1 Adoption of Practices from IT SOCs to OT SOCs (RQ1)

Previous research describes OT security as relying on IT security tools and practices [43,25]. IT SOC practices can provide a useful starting point for OT SOC development, particularly regarding structure, workflows, tooling, and overarching analysis principles. However, as monitoring moves deeper into domain-specific process control environments, maturity increasingly depends on OT-specific visibility, process knowledge, contextual understanding, safety considerations, vendors, and decision-making routines. OT SOC visibility depends on the condition of the monitored OT environments, particularly for outsourced OT SOCs, where the SOC may have limited influence over the security posture of customer sites. Legacy systems, limited logging, and concerns about disrupting production can restrict what the SOC can monitor, detect, and respond to. The interviews emphasized that organizations and OT personnel often prioritize operational continuity and personnel safety, which may limit the deployment of new monitoring capabilities. Greenfield environments provide better opportunities to include cybersecurity, logging, visibility, and monitoring capabilities from the design phase. OT SOC maturity develops through modernization of the industrial environments being monitored. Future research could investigate whether greenfield sites enable more efficient detection and monitoring than brownfield sites, thereby facilitating easier analysis for OT SOC analysts (e.g., by reducing false positives that affect detection and monitoring capabilities).

Participants regarded hybrid SOCs as beneficial because cross-domain visibility can help analysts understand the entire attack path. Although integrated SOC environments can improve threat visualization, collaboration, and cross-domain visibility [19,40], concerns were also raised about whether hybrid SOCs provide sufficient OT-specific expertise. IT SOC structure, workflows, tooling, triage practices, and analytical routines can help establish initial OT SOC capabilities. However, mature OT SOC capabilities require adaptation to OT-specific constraints. OT SOC maturity is shaped by the monitored environment, available expertise, organizational model, and the ability to combine IT security practices with OT-specific contextual understanding.

6.2 Factors that influence OT SOC analysis processes (RQ2)

The interview findings indicate that OT SOC analysis is shaped by technical, organizational, and human factors. In OT environments, analysts should deter-

mine what an alert concerns, which assets or processes are involved, whether the activity is expected, who can verify it, and what consequences may follow from (in)action. This does not only reduces analysis time but also enables analysts to make sufficiently informed and safe decisions under uncertainty.

Technical telemetry is often insufficient unless OT SOC analysts can relate alerts to the relevant OT environment, affected assets, normal process behavior, and possible operational consequences, emphasizing the importance of contextual understanding, human interpretation, and domain knowledge in OT security analysis [26,4,18]. The interview findings emphasized that visiting industrial sites could help analysts understand component deployment, process dependencies, and the practical consequences of cyber incidents. Quantifying their impact on operational performance could further evaluate whether these factors influence measurable outcomes such as false-positive rates, escalation accuracy, analyst workload, investigation quality, or Mean Time To Resolution (MTTR) across different OT SOC settings.

Experienced OT SOC analysts are better able to recognize patterns, interpret alerts, and process large amounts of information, which is consistent with prior research [30,4]. While IT SOC literature often links experience to greater responsibility and more advanced tasks [24,23], our findings suggest that OT SOC analysis may be unsuitable for inexperienced analysts because misinterpretations can extend into physical operations. Experienced analysts can work more efficiently because they understand the constraints and consequences of OT environments and can rely on developed intuition. This raises the issue of increasing the experience for OT SOC analyst novices without risking unnecessary escalation. In this regard, IT SOC research has demonstrated CRX programs for SOC analysts [17] and implemented additional verification mechanisms by engaging colleagues and using AI for decision support [2]. Further work should incorporate the complex needs and domain-specific knowledge of OT systems to create meaningful training programs for future OT SOC analysts.

Process knowledge helps analysts understand OT system behavior, normal traffic patterns, and anomalies [18,4,25]. Our study further extends the literature by identifying how it is made available and used during investigations. OT SOC analysts do not require detailed engineering knowledge of the process systems, but they need access to relevant operational information through documentation, escalation routines, and collaboration with OT personnel. AI-assisted tools for OT SOCs should be grounded in an accurate model of how analysts interpret heterogeneous technical anomalies [4], integrate process- aware knowledge [38], and balance safety-critical constraints. By identifying the key OT SOC analysis factors and clarifying which IT SOC practices can be meaningfully adapted to industrial environments, the study provides essential design inputs and domain-specific knowledge [33] for next-generation AI-enabled OT SOC systems. These insights help ensure that automation aligns with real analyst workflows, ultimately supporting AI tools that enhance rather than disrupt human decision-making in complex OT settings.

Limitations

Since the study targeted Norwegian organizations with OT SOCs, the results may reflect country-specific conditions such as industrial structure, cultural factors, and OT SOC maturity. Furthermore, the study relied on 15 interviews and was designed as an exploratory qualitative study. While the exploratory nature of the study is appropriate for examining OT SOC analysis and decision-making in practice, the results reflect subjective perspectives shaped by participants' roles, organizations, and SOC models. Due to the nature of the study, the findings should not be interpreted as representative of all OT SOCs or broadly generalizable to other sectors or geographical contexts. The target group consisting of participants with OT SOC experience may also have constrained the range of viewpoints represented in the study.

The qualitative coding might be subject to interpretative bias. To mitigate this, participants received the first draft of the results section to assess their interpretations of the transcripts and to ensure that their meaning and the researcher's interpretation were aligned.

7 Concluding Remarks

This paper investigated factors influencing OT SOC analysis processes and how OT SOC maturity development can be informed by insights and practices from IT SOCs. Based on semi-structured interviews with 15 experts involved in OT security and OT SOC work, the findings show that OT SOC analysis depends on more than technical telemetry and tooling. Experience, contextual and process knowledge, and analysts' site exposure were identified as key factors influencing OT SOC analysis. Structures, workflows, tooling, and analysis processes from IT SOCs can help establish OT SOC capabilities, but these must be adapted to OT-specific constraints such as safety, availability, legacy systems, and limited visibility. These findings should be regarded as exploratory insights derived from a Norwegian sample and would benefit from validation across additional industrial sectors, countries, and OT SOC models.

As SOCs increasingly integrate AI-enabled monitoring tools, it is important to align such technologies with real analyst workflows. The identified OT SOC analysis factors offer input for designing AI systems that can incorporate operational context, process-aware reasoning, and the constraints of industrial environments. By clarifying which IT SOC practices transfer meaningfully to OT settings, the results can help guide the development of AI tools that enhance analyst decision-making.

References

1. A. -P. Lohfink, S. D. D. Anton, H. D. Schotten, H. Leitte, C. Garth: Security in Process: Visually Supported Triage Analysis in Industrial Process Data. IEEE Transactions on Visualization and Computer Graphics **26**(4), 1638–1649 (Apr 2020). https://doi.org/10.1109/TVCG.2020.2969007

2. Alahmadi, B.A., Axon, L., Martinovic, I.: 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms. pp. 2783–2800 (2022), https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi
3. Allison, D., Smith, P., Mclaughlin, K.: Digital Twin-Enhanced Incident Response for Cyber-Physical Systems. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. pp. 1–10. ARES '23, Association for Computing Machinery, New York, NY, USA (Aug 2023). https://doi.org/10.1145/3600160.3600195
4. Asiri, M., Arunasalam, A., Saxena, N., Celik, Z.B.: Frontline responders: Rethinking indicators of compromise for industrial control system security. Computers and Security **154**(January), 104421 (2025). https://doi.org/10.1016/j.cose.2025.104421
5. ASReview: ASReview - Active learning for Systematic Reviews, https://asreview.nl/
6. Caviglia, R., Aliaskharov, D., Aceti, A., Dalla Preda, M., Girdinio, P., Gaggero, G.: A Security Operation and Event Management (SOEM) Platform for Critical Infrastructures Protection. Computers, Materials & Continua (2025). https://doi.org/10.32604/cmc.2025.068509
7. Cofie, N., Braund, H., Dalgarno, N.: Eight ways to get a grip on intercoder reliability using qualitative-based measures. Canadian Medical Education Journal **13**(2), 73 (mar 2022). https://doi.org/10.36834/cmej.72504
8. Coletta, A., Armando, A.: Security Monitoring for Industrial Control Systems. In: Bécue, A., Cuppens-Boulahia, N., Cuppens, F., Katsikas, S., Lambrinoudakis, C. (eds.) Security of Industrial Control Systems and Cyber Physical Systems. pp. 48–62. Springer International Publishing, Cham (2016)
9. 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
10. D. Shahjee, N. Ware: Integrated Network and Security Operation Center: A Systematic Analysis. IEEE Access **10**, 27881–27898 (2022). https://doi.org/10.1109/ACCESS.2022.3157738
11. Deen, J.: AI-Assisted Compromise of Mexican Water Utility with OT Implications. Tech. rep., Dragos, Inc. (May 2026), https://5943619.hs-sites.com/hubfs/116-Whitepapers/dragos-2026-ai-mexico-water-attack-intel-brief.pdf?hsCtaAttrib=212227055633, threat Intelligence Brief, updated May 2026
12. Dimitrov, W., Syarova, S.: Analysis of the Functionalities of a Shared ICS Security Operations Center. In: Proceedings of the 2019 IEEE Conference on Big Data, Knowledge and Control Systems Engineering (BdKCSE) Analysis. pp. 1–6. IEEE (2019). https://doi.org/10.1109/BdKCSE48644.2019.9010607
13. Dragos: 2026 OT Cybersecurity Year in Review. Tech. rep., Dragos (2026), https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsCtaAttrib=205683189348
14. Fink, G.A., Shulga, Y.: Helping IT and OT Defenders Collaborate. In: 2018 IEEE International Conference on Industrial Internet (ICII). pp. 188–194 (Oct 2018). https://doi.org/10.1109/ICII.2018.00036
15. G. B. Gaggero, R. Caviglia, P. Girdinio, M. Marchese: 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

16. Giarimpampa, D., Meier, R., Bissyande, T.F., Lenders, V., Klein, J.: Exploring the role of artificial intelligence in enhancing security operations: A systematic review. ACM Comput. Surv. **58**(3) (Sep 2025). https://doi.org/10.1145/3747587, https://doi.org/10.1145/3747587
17. Glas, M., Kersten, L., Mulders, T., Pernul, G., Allodi, L.: T1ger: An instructional re-design of a cyber range exercise in a commercial security operations center. In: Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems. CHI '26, Association for Computing Machinery, New York, NY, USA (2026). https://doi.org/10.1145/3772318.3791226, https://doi.org/10.1145/3772318.3791226
18. Gnanasekaran, V., Bartnes, M., Heegaard, P.E.: A Framework for Onboarding Security Operations Centers in Industrial Environments. Information and Computer Security (2026). https://doi.org/10.1108/ICS-03-2026-0145
19. Gnanasekaran, V., Nilsen, T.G., Heegaard, P.E.: A Comparative Study of Security Operations Center Models for Operational Technology. Norsk IKT-konferanse for forskning og utdanning **37**(3) (Nov 2025). https://doi.org/10.5324/yd7t8t20
20. Hollerer, S., Brenner, B., Bhosale, P.R., Fischer, C., Hosseini, A.M., Maragkou, S., Papa, M., Schlund, S., Sauter, T., Kastner, W.: Challenges in OT Security and Their Impacts on Safety-Related Cyber-Physical Production Systems. In: Vogel-Heuser, B., Wimmer, M. (eds.) Digital Transformation: Core Technologies and Emerging Topics from a Computer Science Perspective, pp. 171–202. Springer Berlin Heidelberg, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-662-65004-2_7
21. Kaouk, M., Flaus, J.M., Potet, M.L., Groz, R.: A Review of Intrusion Detection Systems for Industrial Control Systems. In: 2019 6th International Conference on Control, Decision and Information Technologies (CoDIT). pp. 1699–1704 (Apr 2019). https://doi.org/10.1109/CoDIT.2019.8820602, iSSN: 2576-3555
22. Karantzas, G., Patsakis, C.: An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. Journal of Cybersecurity and Privacy **1**(3), 387–421 (2021). https://doi.org/10.3390/jcp1030021
23. 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. pp. 1955–1970. CCS '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3319535.3354239
24. M. Vielberth, F. Böhm, I. Fichtinger, G. Pernul: Security Operations Center: A Systematic Study and Open Challenges. IEEE Access **8**, 227756–227779 (2020). https://doi.org/10.1109/ACCESS.2020.3045514
25. Nasr, A.N., Vaarandi, R., Zaitseva-Parnaste, I., Kujala, P.: Maritime Security Operations Center (M-SOC): Systematic Literature Review, Research Gaps and Future Areas to Investigate. Transnav-International Journal on Marine Navigation and Safety of Sea Transportation **19**(4), 1141–1155 (Dec 2025). https://doi.org/10.12716/1001.19.04.11
26. Nganga, A., Scanlan, J., Lützhöft, M., Mallam, S.: Enabling cyber resilient shipping through maritime security operation center adoption: A human factors perspective. Applied Ergonomics **119**(May) (2024). https://doi.org/10.1016/j.apergo.2024.104312

27. 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), 6:1–6:22 (Mar 2025). https://doi.org/10.1145/3722233
28. O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, J. Simonin: 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). pp. 1–8 (Oct 2018). https://doi.org/10.1109/CSNET.2018.8602669
29. O'Connor, C., Joffe, H.: Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines (Jan 2020). https://doi.org/10.1177/1609406919899220
30. 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 (2024). https://doi.org/10.1007/s10207-024-00872-6
31. de Oliveira, P.R., Santin, A.O., Horchulhack, P., Viegas, E.K., de Matos, E.: A Dynamic Network-based Intrusion Detection Model for Industrial Control Systems. In: 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 1496–1501 (Nov 2023). https://doi.org/10.1109/TrustCom60117.2023.00204, iSSN: 2324-9013
32. Optiv: Practical Approaches to OT SOC Monitoring (May 2024), https://www.optiv.com/insights/discover/blog/practical-approaches-ot-soc-monitoring
33. Padín-Torrente, H., Carneiro-Diaz, V., Ortega-Fernandez, I.: Toward human-centered explainability: Natural language explanations for anomaly detection. Information Systems Frontiers pp. 1–17 (2026). https://doi.org/10.1007/s10796-026-10717-3
34. Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., Moher, D.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ **372**, n71 (Mar 2021). https://doi.org/10.1136/bmj.n71
35. Pliatsios, D., Sarigiannidis, P., Lagkas, T., Sarigiannidis, A.G.: A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. IEEE Communications Surveys & Tutorials **22**(3), 1942–1976 (2020). https://doi.org/10.1109/COMST.2020.2987688
36. Polska, C.: Energy Sector Incident Report - 29 December 2025 (2026), https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
37. Quan, Y., Tytko, T., Hui, B.: Utilizing ASReview in screening primary studies for meta-research in SLA: A step-by-step tutorial. Research Methods in Applied Linguistics **3**(1), 100101 (Apr 2024). https://doi.org/10.1016/j.rmal.2024.100101
38. Rehman, M.U., Bahşi, H.: Process-aware security monitoring in industrial control systems: A systematic review and future directions. International Journal of Critical Infrastructure Protection **47**, 100719 (Dec 2024). https://doi.org/10.1016/j.ijcip.2024.100719
39. Reisser, A., Vielberth, M., Fohringer, S.: Security Operations Center Roles and Skills: A Comparison of Theory and Practice. In: Data and Applications Security and Privacy XXXVI. DBSec 2022. vol. 2, pp. 316–327 (2022). https://doi.org/10.1007/978-3-031-10684-2

40. 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 2024. pp. 1–6. IEEE (2024). https://doi.org/10.1109/KPEC61529.2024.10676242
41. Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., Jinks, C.: Saturation in qualitative research: exploring its conceptualization and operationalization. Quality & Quantity **52**(4), 1893–1907 (2018). https://doi.org/10.1007/s11135-017-0574-8
42. Sen, Ömer and van der Velde, Dennis and Wehrmeister, Katharina A. and Hacker, Immanuel and Henze, Martin and Andres, Michael: On using contextual correlation to detect multi-stage cyber attacks in smart grids. Sustainable Energy, Grids and Networks **32**, 100821 (Dec 2022). https://doi.org/10.1016/j.segan.2022.100821
43. Simola, J., Takala, A., Lehkonen, R., Frantti, T., Savola, R.: Improving Detection Capabilities in OT Environments Through Multisource Data Sensors. In: Lehto, M. (ed.) Proceedings of the 23rd European Conference on Cyber Warfare and Security. Curran Associates Inc. (2024). https://doi.org/10.34190/eccws.23.1.2339
44. Srinivas, S., Kirk, B., Zendejas, J., Espino, M., Boskovich, M., Bari, A., Dajani, K., Alzahrani, N.: Ai-augmented soc: A survey of llms and agents for security automation. Journal of Cybersecurity and Privacy **5**(4), 95 (2025). https://doi.org/10.3390/jcp5040095
45. Timpson, D., Moradian, E.: A Methodology to Enhance Industrial Control System Security. Procedia Computer Science **126**, 2117–2126 (Jan 2018). https://doi.org/10.1016/j.procs.2018.07.240
46. Tjora, A.H.: Qualitative research as stepwise-deductive induction. Routledge advances in research methods 26, Routledge, Abingdon, Oxon (2019)

A SLR findings to interview guide topics

Table 5. Traceability from SLR findings into topics included in the interview guide of the second round of interviews.

New/Expanded Topics	Relevant Paper(s)	Relevance
Distinction between technical and operational context	[18,28,4]	Information aggregation, situational awareness, and human factors are discussed, but leave open how analysts compensate for missing context during real-world investigations.
Log sources, visibility gaps, and awareness of missing telemetry	[15,42,26]	Monitoring, alert correlation, and multi-source data analysis are addressed, but they offer limited insight into practical telemetry limitations.
Impact of site visits and exposure to OT environments	[30,28]	The literature discusses awareness, training, and collaboration with operators, but provides limited evidence regarding the value of physical operational exposure for analysts.
Difference between experienced and novice OT SOC analysts	[30,4]	Human expertise, decision-making, and training needs are acknowledged, but the characteristics of effective OT analysts remain underexplored.
Impact of asset inventory quality on analysis	[40,25]	Integrated visibility is identified as important, yet little is known regarding the operational consequences of incomplete asset inventories.
Communication with OT personnel	[28,4]	Shared situational awareness and organizational coordination are needed, but there is little understanding of how collaboration affects analysis outcomes.
Influence of production constraints on incident response	[4,25]	Operational constraints are identified as important factors, but their effect on real-world response decisions remains insufficiently explored.