International Journal of Information Security (2025) 24:229
https://doi.org/10.1007/s10207-025-01147-4

REGULAR CONTRIBUTION

A Model-Based Framework for Developing Security-Safety Incident Response Plans

Vahiny Gnanasekaran[1] · Urooj Fatima[1] · Magdalena Glas[2] · Poul Einar Heegaard[1]

Received: 17 July 2025 / Accepted: 20 October 2025 / Published online: 3 November 2025

Abstract
Cyberattacks are increasingly affecting the safe operation of critical infrastructure (e.g., energy, manufacturing) and potentially endangering production, people, equipment, and the environment. A cyber-incident with physical consequences requires personnel responsible for aggregating log information, analyzing root cause (i.e., cybersecurity), and ensuring the production and safe operation of safety-critical systems (i.e., safety) to collaborate. For this, they must understand their own and each other's roles in the incident response process, as well as when and how to interact with different roles. To address this problem, this paper proposes a framework that utilizes a model-based approach to illustrate the critical roles and their interactions within a security-safety incident response plan. To demonstrate its applicability, the framework was applied in a qualitative study within the Norwegian oil and gas industry, involving two companies. This research sheds light on the relevance of applying a model-based approach to developing security and safety incident response plans for organizations. It investigates the relevance of using two modeling languages: a general-purpose software systems modeling language, the Unified Modeling Language (UML), and an enterprise process workflow modeling language, the Business Process Modeling Notation (BPMN), for visualizing the security-safety incident response plan. The findings indicate that the modeling languages are suitable and relevant for understanding and discussing the collaboration and coordination of different personnel's roles during security-safety incident response. The distinct diagrams highlight various aspects, including roles, transmitted information, tasks, and the sequence of tasks. Future work should consider how the diagrams can be applied during the training and learning of the incident response plans.

Keywords Modeling language · Incident response · Critical infrastructure · Roles · Cyber security · Safety

1 Introduction

Attacks on IT systems can lead to severe consequences, including data loss, financial damage, and reputational harm for organizations. These consequences become even more critical when cyberattacks target cyber-physical systems, which integrate information technology (IT) with operational technology (OT). In such environments, the impact of an attack is not limited to digital assets but can extend to the physical world, potentially endangering human life and the environment [1]. A notable example is the Industroyer malware [2], which targeted critical infrastructure and disrupted electricity supply.

These risks are particularly pronounced in the industrial sector, e.g., the oil and gas industry. Here, cyberattacks can lead to catastrophic oil or gas leaks, resulting in environmental contamination, explosions, or loss of life. Moreover, such incidents can severely disrupt supply chains, affecting downstream operations and causing regional or even global ripple effects.

While cybersecurity risk management strategies help reduce the likelihood of attacks, a residual risk always remains – particularly due to unpredictable events such as

✉ Vahiny Gnanasekaran
vahiny.gnanasekaran@ntnu.no

Urooj Fatima
urooj@ntnu.no

Magdalena Glas
magdalena.glas@ur.no

Poul Einar Heegaard
poul.heegaard@ntnu.no

[1] Norwegian University of Science and Technology, O. S. Bragstad Plass 2A, 7491 Trondheim, Norway

[2] University of Regensburg, Universitätstr. 31, 93053 Regensburg, Germany

zero-day vulnerabilities. Organizations must address these residual risks through incident response plans, structured approaches that outline roles, responsibilities, procedures, and communication channels during and after a security incident to contain damage and ensure recovery. In cyber-physical environments, which blend IT and OT systems, these plans must address not only security concerns (e.g., malware removal, data integrity) but also safety concerns (e.g., hydrocarbon leakage, explosion prevention, evacuation). Thus, they converge the two previously separated domains. In the oil and gas sector, an incident response plan may define the coordination between IT and OT security teams and field engineers during a leak caused by a cyber intrusion into pipeline control systems.

To this end, responding effectively to such incidents requires cross-functional collaboration. Security and safety professionals must jointly understand and mitigate the effects of attacks [3]. This integrated approach is referred to as security-safety incident response (in short: *joint incident response*), the coordinated action of emergency response and cybersecurity teams when dealing with incidents that affect both digital and physical dimensions [4]. For instance, in an oil and gas facility, a control room operator might work alongside a cybersecurity analyst and an automation engineer to shut down process-critical systems and initiate evacuation protocols in the event of a cyber-induced pressure anomaly.

When such joint security-safety incident response plans, defined here as coordinated procedures bridging IT and OT responses, are poorly defined or absent, organizations risk responding too slowly or ineffectively, thereby exacerbating harm to people, infrastructure, and the environment.

Despite this urgency, little attention has been paid to the non-technical aspects of joint security-safety collaboration, and there is a lack of empirically grounded research on cyber incidents with physical consequences [5–7]. Existing standards and guidelines (e.g., NIST SP 800-61, the ISA/ISO 27000-series) typically focus on IT-centric procedures [5, 8], emphasizing information over functions, an approach that is often inadequate for OT systems. While some IT standards can be adapted to industrial control systems (ICS), they rarely account for the complexity of OT processes, reducing their effectiveness and adoption. To develop effective joint incident response plans, organizations must understand how to model and coordinate roles and processes across domains during detection, response, and recovery phases. This leads to our first research question:

RQ1: How can an organization define a joint incident response plan?

Contribution 1. To address this research question, we propose a framework based on system modeling, a methodology commonly used to describe, analyze, and communicate the structure and behavior of systems. System modeling uses modeling languages, such as UML or BPMN, to visually represent system processes, components, use cases, and interactions. Traditionally rooted in software engineering [9], using modelling languages gained traction in the field of cybersecurity, e.g., to represent misuse cases [10], attack scenarios [11], and incident response playbooks [12]. The purpose of modeling languages is to provide a system overview. Any interaction described can be represented by explaining behavior only, without considering the details of the system underneath. Given the availability of various modeling languages, each with specific strengths and weaknesses, we raise a second research question:

RQ2: What are the strengths and weaknesses of different types of modelling languages in joint incident response plans?

Contribution 2. To address this question, we conduct a comparative analysis of modeling languages commonly used in system modeling, focusing on UML and BPMN. We consider the UML diagram types (1) sequence diagram, (2) activity diagram, (3) class diagram, and (4) collaboration diagram, as well as (5) BPMN notation diagrams. These diagrams were assessed based on their ability to express key aspects of joint incident response processes.

Contribution 3. To move beyond a purely theoretical description of our framework, we applied it in a case study involving two oil and gas companies. Following the proposed framework, we analyzed existing incident response documentation, conducted expert interviews with key stakeholders, and organized workshops to evaluate and refine the modeled processes. We then represented the resulting joint incident response plans using the diagram types examined in the context of RQ2, including both UML and BPMN. In the study, the diagrams illustrate how different modeling languages can help organizations clearly define responsibilities, escalation paths, and coordination points, ultimately fostering a shared understanding of joint incident response.

2 Joint Incident Response

Managing a cyber incident with physical consequences demands collaboration between the safety and security domains. Due to the lack of incident response standards that combine cybersecurity and safety [5], this section addresses the security and safety incident response separately before moving to joint incident response.

2.1 Cybersecurity Incident Response

A security incident response plan defines the organizational procedures for detecting, responding to, and recovering from a cyber incident [13]. They may consist of multiple playbooks for mitigating specific scenarios (e.g., ransomware, Denial of Service attacks, etc.). For security incident response, NIST SP-800-82 [14], NIST SP-800-61 [15], and IEC 27035 "Information Security Incident Management" [16] provide five phases before, during, and after a security incident:

CS1 **Plan and prepare** security management policies and schemes, establish an incident response Team (IRT), and develop an awareness program, among other tasks.
CS2 **Detection, reporting, and analysis** includes receiving alerts from Intrusion Detection Systems (IDS), firewalls, log information systems, antivirus, and other monitoring software.
CS3 **Assessment and decision/containment and eradication** phase appoints a Point of Contact (PoC), which assesses whether the occurred security incident is an incident or not (e.g., false positives). Subsequently, PoC alerts the necessary personnel and resources to distribute responsibility and ensure documentation.
CS4 **Responses/recovery** involves validating whether the incident is under control, performing forensic analysis, and communicating the results internally and externally.
CS5 **Lessons learned/post-incident activity** identifies feedback and suggestions from the incidents and initiates a review and, if necessary, an update of the security controls. This includes sharing results with a trusted community.

2.2 Safety Emergency Response

ISO 27035 emphasizes incident response in cybersecurity, whereas ISO 22320 describes the safety emergency response. In safety emergency response, ISO 22320 [17] is regarded as a standard for emergency response in specific sectors within the safety domain. The Norwegian oil and gas industry also leverages industry-specific standards to develop emergency response assessments, such as NORSOK-Z-013 [18]. ISO 22320 operates with four phases during safety emergency response:

S1 **Planning** involves alerting and warning key personnel and initiating important safety-critical procedures.
S2 **Information gathering and sharing** highlights the continuous flow of information between offshore and onshore personnel, enabling proactive measures for possible remedial actions and preparing for the next course of action or decision.
S3 **Decision-making and sharing** defines how planned actions should be executed from the last step, such as search and rescue, evacuation, and environmental protection.
S4 **Assessment of situation and forecast** includes debriefing, sharing experiences, and evaluating response activities according to best practices.

Joint incident response [1, 4, 6] denotes the unified response of security incident response and safety emergency response during a cyber incident with physical consequences (e.g., power outage, gas leakage). The literature emphasizes the need to develop a holistic security-safety incident response framework [5, 8]. Staves et al. [8] comprehensively compare the most common ICS incident response and recovery phases, described later in this section. They suggest that no single guideline or standard applies to all aspects of IR, and there is a lack of tools and frameworks tailored explicitly for OT systems. Although the overlap between phases is identified among the standards discussed in this section, more emphasis is needed on criticality assessment and resource availability to provide a comprehensive and efficient ICS response and recovery [8]. Plans for organizational backup should be prepared. There might be deadlocks or single points of failure that could pose a risk during critical incidents. Figure 1 links the procedures to provide an overview of the joint incident response. The joint incident response plan (see Section 6.1) primarily considers the steps *during* the IR, which encompasses all emergency response phases and three cybersecurity phases, due to the role changes between normal and emergency procedures (i.e., after entering the incident).

2.3 Interactions Between Roles in Joint Incident Response

Role interactions are not described in the literature in detail, neither in cyber incidents nor in safety emergency response. NIST SP-800-82 [14] is one of the few standards that provide a list of critical personnel needed during OT incident response, including a designated incident commander, on-call OT system personnel, on-call ICT personnel, and physical safety personnel, among others. Still, specific internal roles and external resources are missing, such as more detailed information about emergency response tasks and roles (e.g., tactical, operational, and strategic), sector-specific Computer Emergency Response Teams (CERTs), relevant authorities, and cyber insurance. Gnanasekaran et al. [4] proposed a role taxonomy based on joint incident response using seven cybersecurity and five safety standards. The taxonomy is two-layered and primarily focuses on the internal roles and responsibilities. They include NIST SP-800-82 as part

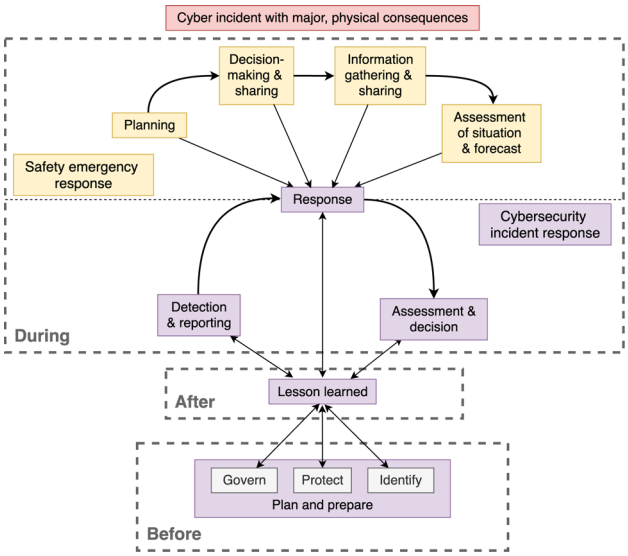

Fig. 1 Theoretical framework used for the joint incident response plan, adapted from [15–17]

of their corpus for the role taxonomy and identify distinct types of expertise needed for the technical roles (e.g., OT security, IT security, safety personnel, etc.).

According to ISO 22320 [17], organizations should establish roles, responsibilities, and procedures for emergency response during safety incidents. However, they only include examples of incident management tasks (e.g., incident command, operations, public communication, logistics) without providing input on the tasks that should be linked to one/multiple role(s) and when and how the roles collaborate. The interaction between roles and the order in which they occur are less clearly explained in security and safety standards and literature. Due to the lack of input on role interactions, empirical insights are needed to understand how collaborations occur during joint incident response.

3 Leveraging a Model-based Approach for Joint Incident Response

Effective communication among users, owners, and stakeholders requires a shared understanding of system concepts [19]. Modeling languages help bridge these conceptual gaps by offering standardized, visual representations of roles, responsibilities, and interactions. This section introduces a model-based framework for joint incident response, providing both the rationale for its adoption and a detailed outline of its structure. The joint incident response system is a complex, distributed, communicating system due to the number of actors involved, and their distribution (i.e., offshore versus onshore), the number of interleaving interactions ongoing between the actors themselves, and between them and their environment.

Due to these characteristics, understanding the system's interactions with the actors that derive their roles and responsibilities is a complex and error-prone process. Models are the key to decomposing this complexity [20]. They help to build a conceptual understanding of a complex system visually by decomposing its complexity at different levels of abstraction or from various perspectives. In model-based approaches, modeling serves as a central technique for understanding and analyzing the system.

Figure 2 presents the framework based on a model-based approach for joint incident response. **Step 1** includes discerning the safety emergency response and cybersecurity incident response in the specific sector or company. The procedures differ based on the industrial sector and need to be adapted to each other. The objective is to elicit critical requirements (e.g., involved roles, the event order, procedures, etc.). Building on the elicited requirements, **Step 2** analyzes how roles and responsibilities align with the sequence of events. The purpose is to provide models of the joint incident response for further evaluation. The models can be presented in either textual or graphical representation. We opted for UML and BPMN diagrams because they clearly capture both role responsibilities of joint incident response by providing helpful constructs for representing the interacting roles [21].

Step 3 indicates evaluating the models, which should be conducted with cross-domain experts and between IT and OT, security and safety, and the internal staff. The evaluation can be performed using qualitative methods (e.g., surveys, focus groups, etc.). The aim is to validate whether the modeled interactions and responsibilities accurately reflect real-world practices and expectations. The feedback from the evaluation is applied to improve the models, resulting in a final representation of the joint incident response in **Step 4**. After presenting the final representations, they can be subjected to change post-incident, scheduled audits, or the onboarding of new services and regularly as part of table-top exercises. Such updates can be guided and enforced through maturity models [22, 23], which enable organizations to regularly assess and ensure the level of maturity of their incident response capabilities. Depending on the change, it may require a new synthesis of joint incident response requirements or revising existing models.

3.1 Modeling languages

Models are described using modeling languages. Modeling languages provide underlying concepts and symbolic representations of the subject matter. Due to the numerous existing modeling languages, it is challenging to determine which to use. For this, authors in [19] provide the respective guidelines for the concepts provided by the modeling languages: They

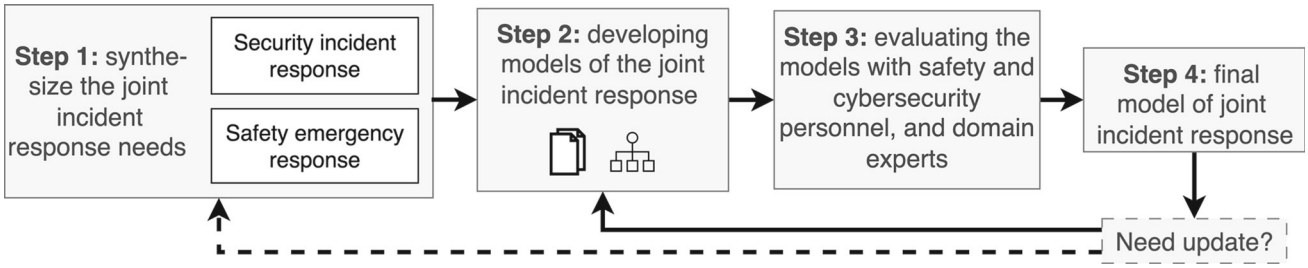

Fig. 2 The framework based on a model-based approach applied for joint incident response. The need for an update could come from recent incidents, periodic changes due to company policies, onboarding new services, etc

"must fit the concepts one wants to describe and must be convenient concerning: ease of making; ease of interpretation, and ease of reasoning" [19]. We seek a similar objective for the personnel involved in the joint incident response, i.e., unambiguity in understanding their roles and responsibilities.

3.1.1 Structural Diagrams

To model joint incident response effectively, we use UML and BPMN, as they are considered the most famous modeling languages when it comes to factors like universality, user-friendliness, expressiveness, ease of learning, and tool support both for business users and technology experts [24]. UML diagrams are broadly categorized into structural diagrams, which show system components and their relationships, and behavioral diagrams, which illustrate how these components interact over time [25]. The UML 2.x specification includes collaboration and class diagrams among its structural diagram types. Structural diagrams represent a system in terms of its components (actors) and their interconnections.

The UML Collaboration Diagrams (ColD) was chosen due to its effectiveness in visualizing role responsibilities during joint incident response. UML ColDs are used during the analysis and early design phases to visualize the relationships between roles. Figure 3 represents a simple notation of UML ColDs. Two actors are connected through a collaboration (smaller dashed ellipse) in which they participate by playing their respective roles in the specific collaboration.

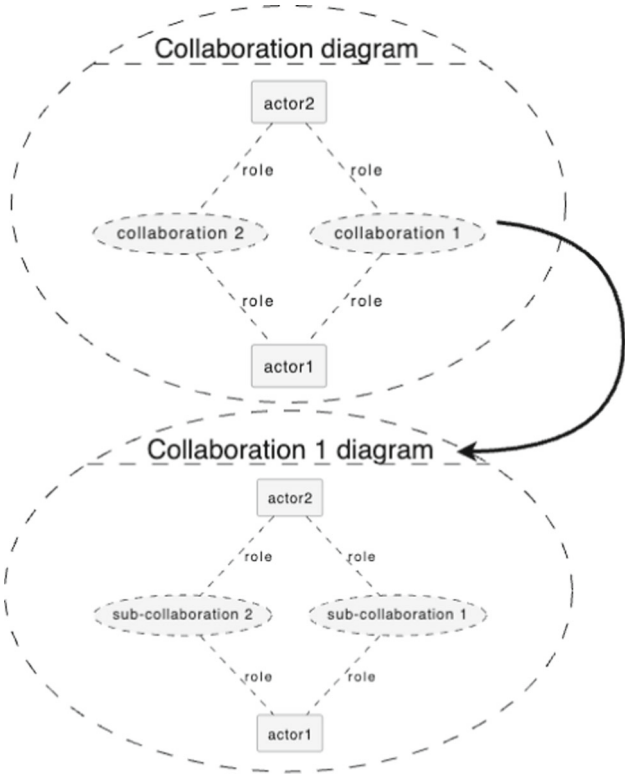

Fig. 3 UML collaboration diagram notation

Collaborations can be composed of smaller sub-collaborations. The sub-collaborations have limited complexity and, therefore, can help describe a system in a more organized manner. The composition of sub-collaborations describes their interrelationships. Although the ColDs are powerful tools for representing actors, their roles, and the interactions (collaborations) they participate in, they do not explicitly show how smaller sub-collaborations work together. For example, whether a sub-collaboration representing *task x* occurs before the sub-collaboration representing *task y* or after, or do these collaborations coincide? Nevertheless, collaborations can have associated behavior and are, therefore, both structured and behavior classifiers [25]. These behaviors – representing the steps involved in constructing a composite collaboration – can be associated with the collaboration through the use of other UML behavioral diagrams, such as sequence and activity diagrams.

The UML Class Diagrams (ClaD) explain the static system structure. The purpose of a class is to represent the classification of objects and the features that characterize those objects. Figure 4 illustrates this paper's most relevant ClaD notation. Each class represents an actor and has two compartments: actor attributes and participating tasks (i.e., "operations" as per UML term). The actor has distinct links with other actors to display their relationship [25].

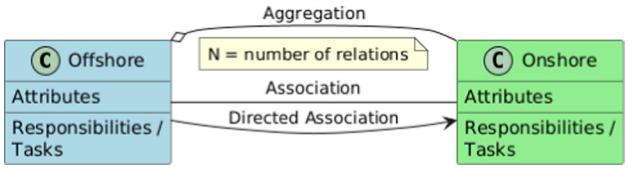

Fig. 4 UML class diagram notation

ColDs and ClaDs represent actors and their relationships from different perspectives. In ClaD, the relationship depicts the connection between two actors in terms of their association with each other. In contrast, ColD focuses on the relationship between actors, specifically how they collaborate to accomplish a joint task. Hence, both diagrams contribute towards achieving the goal of clear and precise structural modeling of the actor-role relationship within a given incident response.

3.1.2 Behavioral Diagrams

While structural diagrams present system components and how they are connected, behavioral diagrams generally describe the overall coordination of these interacting components or actors in terms of their possible execution order.

The UML Sequence Diagrams (SD) can be used for any system where entities interact with each other. These may be the first diagrams that stakeholders use to gain an initial understanding of a system's behavior. Figure 5 presents the notation for SDs and some of its structuring mechanisms: *opt, break, loop*. The drawback of SD is that as the system becomes larger in terms of interactions between actors or components, it becomes more complex and prone to errors. Hence, they are useful when describing specific system behavioral scenarios, rather than complete behaviors.

The UML Activity Diagrams (AD) have constructs that enable the representation of complete complex behaviors while keeping the diagrams readable. One AD construct is an activity partition, which represents an actor's participation or responsibility in a specific task (i.e., an activity node). Figure 6 illustrates the UML AD notation we use in this paper. We opted for this notation, originally proposed in [26, 27], because of its clarity and suitability to our modeling needs of illustrating role responsibilities, i.e.: (1) these activity nodes represents the participating actors and the task (activity) in which they participate during an incident as one joint activity node; (2) This partition notation indicates which actors are involved in each interaction. (3) We can specify which actor initiates a specific activity (i.e., sends the first message), thereby making the representation of responsibilities assigned to personnel during joint incident response more explicit. For simplicity's sake, the initiating actors are on the left, and the receiving actors are on the right of the activity node, as depicted by *initiator* and *receiver* names in Figure

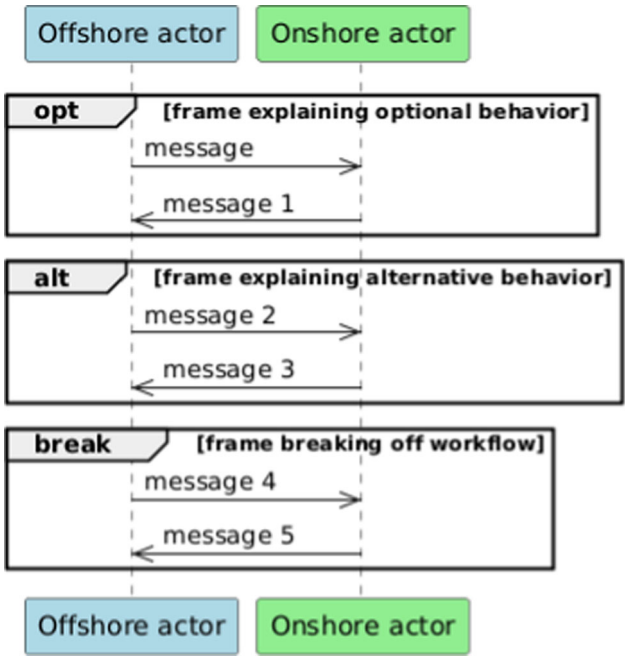

Fig. 5 UML sequence diagram notation

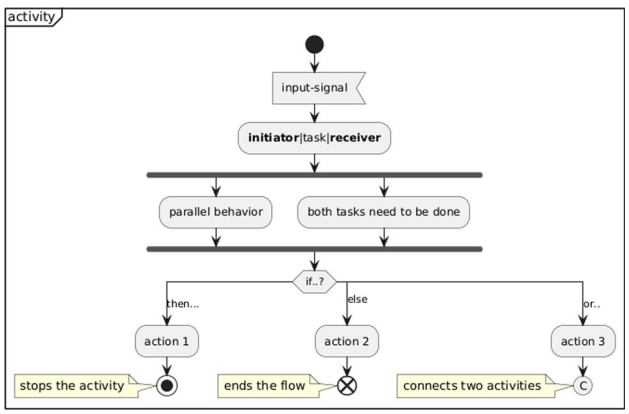

Fig. 6 UML activity diagram notation

6. We have also followed the software systems specification methods presented in [26, 27] to describe a system's behavior regarding the orderings of sub-collaborations described in the ColDs.

BPMN is used in business processes towards a non-technical audience [28]. Major incident response playbook formats leverage BPMN to model the incident response workflow [12]. Figure 7 presents the notation used for BPMN diagrams. The swimlanes represent distinct roles in collaboration during an incident. Diamonds indicate a choice, diamonds with a plus indicate parallel execution, and a circle suggests optional behavior.

Regarding the reliability and ease of comprehension, BPMN and ADs are proven to be equally readable by business users [29]. UML is the de facto standard in object-

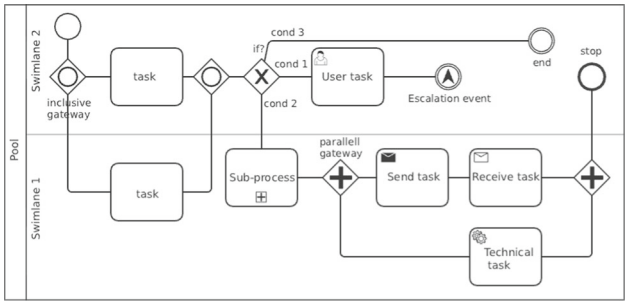

Fig. 7 BPMN diagram notation

oriented modeling, and we have also utilized BPMN due to its popularity among business users and incident response playbooks. SDs, ADs, and BPMN modeling concepts are well-equipped to capture the intricacies of coordination among personnel involved in the joint incident response. Although we do not explicitly model or propose any technical requirements for the joint incident response system's functionality, the models we develop to analyze actions and communication among joint incident response actors can offer guidance on considerations for designing functional system models.

3.1.3 Modeling Perspectives

Models can be developed to present distinct perspectives or design views based on specific questions. Curtis et al. [30] proposed a set of criteria for processing information to highlight perspectives in various modeling languages. The requirements have previously been applied to compare UML, BPMN, and Decision Modeling and Notation (DMN) [31]. Another approach proposed by Van der Aalst [32] has similar perspectives to process mining. An overview of the diagrams used in the paper is presented in Table1, highlighting which perspectives or views they represent. The presented diagrams may display multiple perspectives, but no diagram highlights all perspectives simultaneously.

These perspectives provide an understanding of the focus while modeling joint incident response. While each perspective offers unique insights, they are interrelated and collectively contribute to a holistic understanding of the process. For instance, the functional perspective might reveal a bottleneck, the organizational perspective could identify resource constraints causing it, the time perspective would quantify the impact of the delay, and the informational perspective would provide insights on how the data (e.g., logs, system files) is utilized. Together, these perspectives enable organizations to achieve process transparency and continuous improvement.

Although model-based approaches (e.g., in [27, 33, 34]) prescribe certain combinations of diagrams and guidelines in addition to the language itself, we do not confine our approach to any specific modeling method. We encourage organizations to select and combine any of the five diagram types based on their unique needs, size, and structure. For example, an incident responder may require detailed communication flows, whereas management might only need a high-level overview of their role. During tabletop exercises (TTX), understanding the task order and role interactions becomes especially important. Each diagram type offers distinct strengths, and no single approach fits all scenarios. Therefore, we recommend combining structural and behavioral views–using static diagrams to map roles and responsibilities, and dynamic diagrams to capture critical interactions and message flows.

4 Comparative Analysis of Modeling Languages in Joint Incident Response

This section presents a comparative analysis of using different diagrams for joint incident response. The strength of using UML and BPMN modeling languages lies in their expressive power, which can capture a rich set of alternative behaviors and structures, and the standardized notation, which enables the comparison of different plans. Additionally, a formal model checker can be applied to identify potential problems in the plan, such as deadlocks and livelocks. Multiple application areas exist for modeling languages in incident response:

- **Model Checking.** Modeling incident response plans can be used to model previous incidents and mathematically compute simulations using formal methods. The methods could provide input on the ideal course of action, resource usage, and awareness training.
- **Requirements Engineering.** The modeling diagrams could contribute to eliciting requirements for incident response in each industrial company based on their internal organizational structure and include the relevant IT, OT, and security service providers. This way, a greater understanding of their response times could be considered. The diagrams could further provide feedback on regulatory compliance.
- **Impact Analysis.** The modeling representations could be analyzed for the impact of previous security incidents in multiple dimensions (e.g., reputational, business, organizational, technical).
- **Visualization.** The joint incident response plans may improve human comprehension of the joint incident response. The diagram could promote fruitful discussions among employees on the sharp and blunt ends, as they may possess different viewpoints on their incident response roles.

Table 1 Classification of different diagram types used in this paper, and which perspectives from [30, 32] they represent.

Perspective	Description	Behavioral			Structural	
		SD	AD	BPMN	ClaD	ColD
Organizational	*where* and *by whom* the activities are executed					✓
Behavioral	*when* the activities are performed and *how* they are performed (e.g., feedback loops, iterations) to identify bottlenecks in the process.		✓		✓	✓
Functional	*what* kind of activities, and the process decomposition or task order		✓	✓		✓
Informational	*data* constructed or influenced by a process (e.g., messages, artifacts, files).	✓				

- **Model Refinement.** The diagrams can be used to remove deadlocks, investigate resource usage, or refactor the used models (e.g., changing organizational structure), improving the organizational posture towards security incidents.

Table 2 summarizes the comparative analysis between the modeling diagrams. ClaD and ColDs explain the system structure and architecture by defining entity relationships. The primary emphasis is on a static model representation. The diagram is ideal for modeling the incident response structure of the organization by depicting the roles and actors as classes and the relationships between them. However, some disadvantages are present. Concurrent behavior cannot be modeled with these diagram types because the order of the interactions is not visible in the diagrams. Hence, structural diagrams can be supplemented with behavioral diagrams to further describe their procedures, as proposed by the model-based method in [26, 27]. Still, the structural diagrams provide a useful overview, e.g., for management, third-line emergency teams, and other roles not directly affected by the incident, to understand how the incident is handled (e.g., who should be involved).

SDs and ADs are suitable for describing the dynamic details in the joint incident response plans. They leverage different artifacts – SD employs message exchange between actors and roles, while the AD centers around decomposed tasks. On the one hand, SDs explain detailed message interactions between the entities to demonstrate a simple, top-down message flow. However, due to the inherent concurrency and number of possible orderings of interactions (and exceptions, loops, exits) involved in the joint incident response, SDs become complex, i.e., hard to read[1]. On the other hand, AD is ideal for demonstrating concurrent and interleaving interactions between the joint incident response plan and decision points. AD further enables the representation of participating roles in a more straightforward and more readable manner. On the contrary, multiple roles complicate and enlarge the SD and BPMN diagrams. These AD features have been shown to represent complete behaviors, modeling all desired behaviors expected of a system [35]. The detail level of behavioral diagrams may be too extensive for roles demanding an overview. However, it may serve central roles in in-depth information about the joint incident response (e.g., incident responder, OIM).

BPMN focuses on business processes, while UML is primarily designed for software engineering and development. BPMN decomposes the system behavior into sub-processes and demonstrates concurrent behavior at the same level as AD. However, they exhibit their specific strengths. The BPMN specifies the internal operations performed locally by an individual role, while the ADs model joint tasks at the interface of two roles. Nevertheless, the ADs can be used to model internal operations (core functionality) regarding local role behaviors [35]. However, this is not demonstrated in this paper. The BPMN diagram is well-suited to express details in incident response processes, high-level decisions, and workflows (partly used by company A). Since OT emphasizes safety, a larger pool of internal roles and external actors is relevant to call upon during security incidents with significant physical consequences. BPMN becomes larger as the number of roles (e.g., lanes, pools) increases, making it more complex in terms of readability. Leveraging joint IR plans requires adaptations to the workflow format to include multidisciplinary teams.

[1] The paper does not discuss the computational complexity of the modeling diagrams.

Table 2 Diagram comparison concerning Incident Response (IR) system feasibility. + : "model to some extent", ++ : "model", +++ : "model to a great extent"

	ColD	ClaD	SD	AD	BPMN
Highlights...	IR interactions.	IR organizational structure.	IR role interaction.	activity flows using UML notation.	activity flows using notation for business processes.
Emphasizes...	cooperation between roles.	the hierarchical relationship.	messages between roles.	Task flow and role participation.	equally the individual and the global behavior.
Time sequence	N/A	N/A	Sequential, top-down order	The logical flow.	The logical flow.
Concurrent behavior	N/A	N/A	+	+++	+++
Role representation	Actors	Classes.	Lifelines.	Initiator & receiver in each activity.	Pools/swim lanes.
Model size depends on...	tasks and roles.	classes	messages	tasks	roles and tasks
Ideal for modeling...	IR Role participation in interactions	the static IR structure.	message exchange between IR roles.	IR processes using UML notation.	individual processes in addition to the overall IR process.

5 Study Design

Creating a joint incident response plan requires insights from the industrial sector to understand the domain-specific role coordination and requirements. Roles and interactions are not only based on organizational procedures but are influenced by how employees interpret their roles and responsibilities. It is worthwhile to grasp the interpretations of the organizational structure beyond the company documents. The model-based approach was applied using a case study approach, consisting of documents, interviews, and evaluation workshops. Figure 8 depicts how the study was conducted.

5.1 Qualitative Data Collection & Analysis

The study's objective is to apply the theoretical framework using a qualitative case study approach in the Norwegian oil and gas industry. The primary advantage of case studies and the main reason for selecting this method is the depth and richness of insights gained into the interaction between safety emergency response and security incident response. The perspectives were also needed to gain an understanding of how the framework worked in practice. Due to the comprehensiveness of the case study approach, we decided to focus on one sector, namely the Norwegian oil and gas sector.

First, the process began with semi-structured interviews. The approach is described in a previous paper [36] and is extended with three additional interviews in this paper. Due to the limited number of national experts, recruiting experts to participate in the qualitative study proved challenging. Convenience sampling was used to recruit the interviewees, which may have introduced sampling bias into the sample. However, in the cybersecurity field in the Norwegian oil and gas industry, information power, i.e., the amount of information gathered from each interview, could be considered more critical to obtain than the sampling approach [37]. The sample description for the interviewees is provided in Section 5.2. The interview guide included findings from earlier interviews and the document analysis. All interviewees were considered experts with backgrounds in cybersecurity and incident response for critical infrastructure. Ethical approval, consent form, and interview guide followed the previous paper [36].

To further explore the organizational perspective, incident response plans for detecting and handling cyber-incidents offshore were also analyzed from both companies. Examples of documents include procedures for incidents resulting in a loss of industrial control and safety-critical systems, procedures for detecting cyber incidents, and checklists for operators and the emergency response team during such critical incidents. A similar method was used in the previous study [36], but the data collection is extended with two additional documents concerning cyber incident response. The data analysis followed the same process as explained in the previous publication [36], where an empirically close (EC) coding approach was applied [38] for both the interviews and the documents, allowing for systematic comparison and consistency in the interpretation across the data collection.

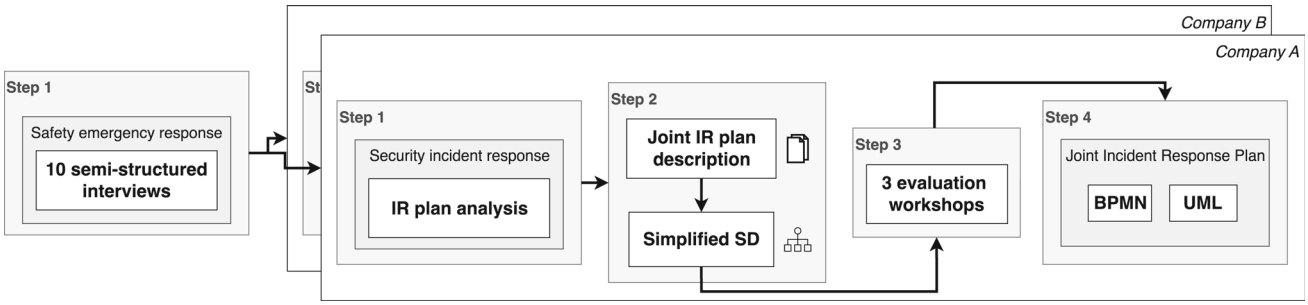

Fig. 8 Summary of the research design using the model-based approach. UML is a collective term for creating ClaD, AD, SD, and ColD

The coding categories remained the same from the last publication, but the final number of codes in each category has changed:

1. Procedures and roles in an outsourced or in-house SOC service (119 EC codes).
2. Procedures and roles in an oil and gas company, both in ordinary and emergency scenarios, and routines and preparations regarding incident response exercises (122).
3. Interaction between IT and OT personnel, equipment, systems, and infrastructure, both in ordinary and emergency scenarios (68).
4. Procedures and roles at OT system vendors regarding cyber-incident response (48).
5. General description of processes and systems in an oil and gas company that do not fit the previous categories (31).
6. Other irrelevant codes to the study (18).

In total, the final number of EC codes increased to 406. The first author used the empirical findings to draft a generic outline from the EC codes. However, since the role descriptions and responsibilities differed, it was necessary to understand the differences among companies to fully comprehend their interactions. Hence, a generic description was added with a simplified SD to include both companies' emergency roles and assess the understanding of these roles within each company. The simplified SD assessed whether the roles followed internal procedures and aimed to improve the experts' comprehension. The simplified SD was applied in the evaluation workshops to provide feedback and facilitate discussion with company representatives, evaluating their understanding of these visual representations. Six evaluation workshops were held, with each company participating in three. The workshops differed in duration (one to four hours) and were conducted in the native language. All workshop participants have a background in incident response in the Norwegian oil and gas industry.

The case study approach, which combined semi-structured interviews, incident response plan analysis, and evaluation workshops, provided a detailed understanding of roles and responsibilities and their interactions during joint incident response. Method triangulation was achieved, mitigating biases during the sampling procedure. Based on the input from the evaluation and the four perspectives discussed in Section 3.1.3, the textual representation of the joint incident response was developed (see Section 6.1). The modeling diagrams from the model-based approach were developed based on the iterative feedback from the evaluation workshops. The five modeling diagrams were developed using the open-source tool PlantUML[2], BPMN.io[3], and Draw.io[4], and are described in Section 6.2.

5.2 Sample Description

Table 3 depicts the ten interviewees participating in the interview study. Four interviews were conducted with employees from two Norwegian oil and gas companies. The remaining six worked in companies concerned with different aspects of OT security (e.g., system vendors, Managed Security Service Providers (MSSPs)). They addressed essential topics within the joint incident response in critical infrastructure (e.g., IT/OT priorities and team collaboration in normal versus emergencies). The participants have between 3 and 20 years of experience in the industry.

Companies A and B, with their distinct organizational cultures and structures, provided two different contexts for developing the joint incident response plans. Although both are considered large companies in Norway, A is larger than B in terms of the number of employees and revenue.

Company A adopts an in-house Security Operations Center (SOC) service, comprising a detection and response team operating during office hours. They leverage an outsourced SOC service with limited access to the OT domain outside office hours. The in-house SOC alerts critical personnel more swiftly because they are familiar with the organizational structure and roles. Due to their organizational size,

[2] https://plantuml.com/

[3] https://www.bpmn.io/

[4] https://www.draw.io/

Table 3 Sample description for the interview study. Years of experience describe the collected work experience with OT security.

Job position	Stakeholder	Years of experience
Chief Commercial Officer	System vendor	5
OT engineer	Company B	15
Offshore Installation Manager	Company B	9
Product Manager	MSSP	12
Security Analyst	MSSP	3
Cybersecurity Director	System vendor	10
Security Analyst	Company A	19
Cybersecurity Director	MSSP	20
OT engineer	Company A	12

they have multiple layers of management, which limits the decision-making authority of each manager. They depend on standardizing the incident response across all platforms to limit customization and react quickly. The in-house SOC serves as the incident coordinator. The offshore personnel execute all measures unless they are unable to do so and require additional assistance from the SOC or onshore facilities, which is continually evaluated throughout the incident.

Company B leverages an outsourced OT and IT SOCaaS for its platforms, indicating that IT and OT SOC environments, to a larger degree, handle their domain-specific issues. In some installations, SOC services are provided through different companies, while others have a single MSSP. The IT and OT MSSPs have limited communication across the services, meaning that all communication originates from Company B's onshore premises to the offshore management. Company B has a Security Operations team responsible for IT and OT security, handling the alerts from the SOC. Due to its organizational size, Company B employs fewer individuals for coordination compared to Company A. The installations at Company B are characterized by the uniqueness of its personnel, processes, and training, which is also a result of previous company acquisitions. Nonetheless, the platforms follow a company-wide incident response plan.

6 Results from Two Companies

This section presents the similarities and the differences between Company A and Company B regarding the joint incident response plan. Before illustrating the differences through the modeling diagrams and detailed role descriptions, the similarities are represented through a common joint incident response plan.

6.1 Joint Incident Response Plan

The common joint incident response plan includes all cyber incidents or attacks originating from IT or OT systems that may cause physical implications for production. However, it excludes incidents that only affect the IT systems. OT systems refer to maritime systems, process control, communication, wells, or drilling systems at offshore installations. An *actor* describes the job position or entity, while *roles* depict their part during an emergency response. The incident response plan answers the following questions (described as actors) in the oil and gas industry:

- Who detects and alerts other roles about the cyber incident?
- Who makes the decisions based on the potential consequences of the cyber incident offshore?
- Who executes the actions based on the decisions made?
- Who leads the evacuation from the platform?
- Who performs digital forensics and system recovery?

The plan has two origins: the security incident may be detected (1) by an observer at the platform or (2) by a SOC. For detection onshore, a SOC might be alerted by its tools and network sensors detecting Indicators of Compromise (IoC) or external information sources (e.g., Computer Emergency Response Teams (CERTs), Cyber Threat Intelligence (CTI)). When the SOC detects an incident, it is usually communicated to the offshore personnel through a "translator", meaning any personnel with domain-specific and cybersecurity knowledge, who further alerts the first-line and second-line emergency response team. This might not be the case if the SOC is in-house.

For detection offshore, an observer (e.g., process engineer) could notice faulty or unresponsive values (e.g., smelling gas even when the gas detectors indicate no leakage). If any suspicions are triggered, they alert the offshore management. After assessing the physical impact and consequences, they alert the second-line emergency response team. When the second-line emergency team is mobilized, the in-house cybersecurity resources are also mobilized (e.g., in-house team, SOC).

Besides having two distinct detection alerts, the incident response plan proceeds and ends similarly for both compa-

nies. The joint incident response plan focuses on minimizing and mitigating damage to the physical environment. Hence, performing digital forensics (which depends on the root cause) is not emphasized in the incident response plan and is only addressed briefly. Table 4 describes how the joint incident response plan is linked to the distinct phases during and after the security incident. These are further mapped into the security incident response and safety emergency response standards from Section 2. The phases from the joint incident response plan are represented in all the phases outlined in the standards. The first two phases address the detection and the strategic planning necessary to perform the remaining phases. "Hazard limitation", and "remove malware" addresses two phases tailored to the safety emergency response and the recovery phase in incident response, and is therefore only considered by one phase from each response.

Due to regulatory requirements, internal actors are assigned to a broader set of roles, which are identical in most Norwegian oil and gas companies. Table 5 illustrates the internal actors occupying positions within the company under normal conditions. The plan primarily concerns company roles, but also includes outsourced SOC services and specific system vendors, as they play a central role in joint incident response. Hence, the plan does not mention CERTs, authorities, and emergency services to limit the scope. Some actors have the same role and responsibility during emergency response as during normal operations, and are considered similar to those during normal operations.

6.2 Modeling Diagrams

The joint incident response plan is modeled after the six phases described in Section 6.1 for each company. Five types of modeling diagrams depicting the joint incident response plan are developed to help analyze different phases, scenarios, and the roles, responsibilities, and interactions between them. Each company has different procedures for detecting cyber incidents, both offshore and onshore. The diagrams are referenced by using the following naming convention:

`X.Y.w.Z`

where $\texttt{X} = \{\texttt{SD}, \texttt{AD}, \texttt{BPMN}, \texttt{ColD}, \texttt{ClaD}\}$ is the diagram type, $\texttt{Y} = \{\texttt{A}, \texttt{B}\}$ is the company, $\texttt{w} = \{\texttt{on}, \texttt{off}\}$ denotes whether the incident is detected onshore or offshore, and $\texttt{Z} = \{1, 2, 3, 4, 5, 6\}$ represents the different phases specified in Section 6.1. If some fields of the naming convention remain unused, it is assumed to cover all elements in the specific field. Note that not all diagrams are displayed in full in this paper. They are available in a public repository [39]. However, excerpts from each type of diagram and company are presented in this section to explain the roles and interactions highlighted during each phase. 33 diagrams were developed using five distinct types of modeling diagrams. The following two sections present the findings using structural diagrams, while the last three present diagram excerpts from the behavioral diagrams.

Table 6 represents the internal roles relevant to the joint incident response modeling diagrams in companies A and B. Some roles are similar and share the same tasks among the companies, while others differ. Some roles (e.g., Chief of Staff) are not included to simplify the plan. Each actor can assume multiple roles and responsibilities depending on the organizational structure and size.

6.2.1 Class Diagram (ClaD)

One ClaD was developed for both companies, demonstrating the relationship between the roles and internal actors. Figure 9 visualizes the roles or actors, their attributes and tasks, and their associations. Please refer to Figure 4 for an overview of the used notation. The role aggregation indicates an inheritance of attributes and responsibilities (e.g., OIM is responsible for alerting the incident, making decisions, and evacuating). The ClaD demonstrates that the actors and roles are clustered around three specific role groups: the onshore emergency team, CSIRT, and offshore emergency team. The primary task of the CSIRT and onshore emergency team is to support the offshore emergency team in handling incidents in the cyber or physical domain. The Area of Expertise denotes an array of distinct expertise on the installation: *Area of Expertise* = [*telecom, electro, automation, maritime*], specifying one area the role might possess in-depth knowledge.

The ClaD represents a "snapshot" of the roles and actors during the joint incident response and provides a structured overview. The notation also clearly distinguishes the relationships between the specific actors and roles in terms of their associations. For example, the offshore EMT can only comprise one Emergency Leader, who can only be assumed by one OIM during emergencies. However, it does not indicate how and when the responsibilities and tasks are performed.

6.2.2 Collaboration Diagram (ColD)

As discussed in Section 3, ColDs are similar to ClaDs in terms of representation of the participants. However, they differ in explaining how the roles are related to each actor. ColD further specifies how the roles interact with each other to perform a joint task represented as a smaller sub-collaboration. One ColD per phase per company was necessary to create, meaning a total of 14 diagrams (`ColD.A.off.1`,..., `ColD.A.6`, `ColD.B.off.1`,...,`ColD.B.6`). Please refer to Figure 3 for a detailed notation description. Figure 10 displays the collaboration diagram for the evacuation phase of the joint incident response plan. For example, the OIM interacts with the OTR for *help to make decision* via a sub-

Table 4 The distinct phases of the joint incident response plan (JIR), and the relevant mapping to the ISO 22320, ISO 27035, and NIST SP 800-61's phases from Section 2.

JIR Phase	Description	Safety (S) & security (CS) phases
Detection & alerting	It includes the observation of an ongoing security incident and alerting of all relevant internal roles.	CS1, CS2, S1
Hazard limitation	The phase requires limiting the potential physical damages done by the security incident by assessing the hazard potential and the need to bring the oil and gas platform to a fail-safe mode. There will also be a physical search of the perpetrator on the platform (i.e., in case the attacker is offshore or onshore at the companies' premises). If the attacker is located, other incident response plans will determine the next actions (i.e., plans for criminal acts involving law enforcement), which fall beyond the scope of the joint incident response plan.	S2
System saving	After assessing the hazard limitation, actions towards system isolation and production shutdown are evaluated and executed, if necessary.	CS3, S3
Evacuation	The phase includes evacuating (non-)essential offshore personnel, depending on the incident severity, from the platform and further assessing the physical dimension of the security incident (e.g., potentially injured, casualties, equipment damage). Non-essential personnel denote service employees (e.g., chefs, cleaning staff, etc.). The cybersecurity aspect is addressed by the onshore personnel, who assist the essential offshore personnel in troubleshooting systems and identifying and removing malware.	CS3, S3
Recovery	It includes determining and installing the latest, clean backup, and continuous communication between internal roles and external actors (e.g., CERTs, regulators, law enforcement). An independent team provides an audit report, based on evidence material from the forensics team, and lessons learned during the response phase.	CS4, CS5, S3, S4
Remove malware	During this stage, the security providers might initiate digital forensics procedures (e.g., log collection, analysis, and evaluation of the malware spread to other installations), provided they have sufficient information. This phase may occur concurrently with the other phases, as security teams may work at any time after a cyber incident is detected.	CS4

Table 5 Responsibilities of internal actors in the Norwegian oil and gas industry during joint incident response.

Responsibility	Internal actors
Detection and alerting	Field personnel, safety personnel, SOC, offshore management
Decision-making on the offshore installation	Offshore Installation Manager (OIM), Technical System Responsible (TSR)
Execution based on the decision-making	Control Room Operations (CRO), Discipline Lead (DL), OT/IT system vendor
Evacuation	Offshore Installation Manager (OIM), Chief of Staff, Emergency Management Team (EMT)
Digital forensics & system recovery	Security Operations Centre (SOC), Managed Security Service Provider (MSSP), OT/IT system vendor, OT/IT security personnel, OT/IT safety personnel

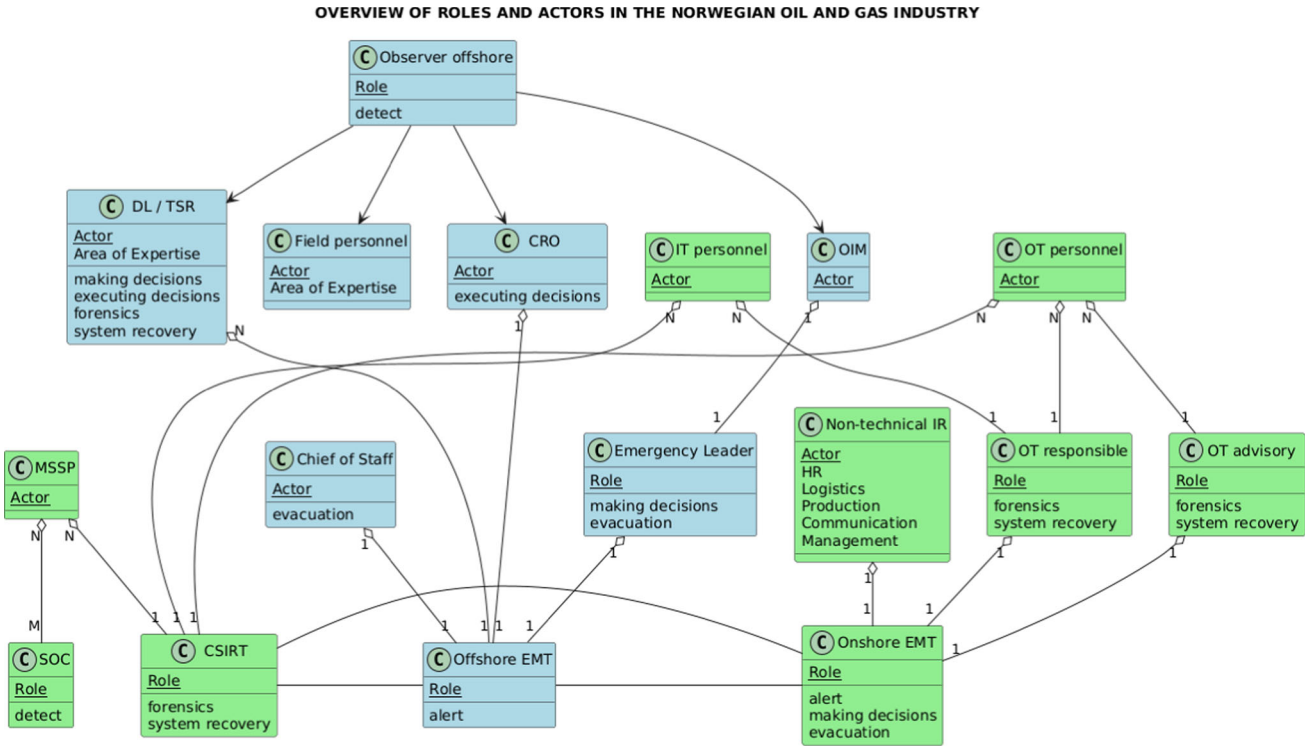

Fig. 9 Diagram (`ClaD`) presents the role overview from Company A and B

collaboration that has been given the same name as that of the interaction being occurred, where the OIM plays the role of *Requester* in this interaction. The offshore's responsibility is primarily to consider the platform evacuation, while OTR guides the decision. It can be observed that the diagram contains fewer details on the interactions (message exchanges) involved in terms of which collaboration occurs first. The sequential task order is not expressed, making it challenging to consider resource allocation during critical events during IR. The absence of this feature makes ColD appear more compact than SDs. Removal of the sequence details provides a static representation of the interactions between actors and roles.

6.2.3 Sequence Diagrams (SD)

One SD for each incident response description from each company and scenario was developed. Four SDs were created to understand the sequential message order (`SD.A.on`, `SD.A.off`, `SD.B.on`, `SD.B.off`). Please refer to Figure 5 for a detailed notation description. Figure 11 depicts the detection and warning phase of the incident response plan

Table 6 The relevant roles for the joint incident response plan for Company A and B.

Roles	Company A	Company B
Offshore observer	The observer is the role alerting the offshore management (e.g., automation/maintenance engineer, discipline leads).	
First-line emergency response leader / Offshore Installation Manager (OIM)	OIM becomes the leader when the team is mobilized. The overall person responsible for an offshore installation.	
First-line emergency response team	The team consists of the Chief of Staff, evacuation response, and multiple TRS for different areas of expertise. The team is not explicitly mentioned in the plans, only OIM.	
Discipline Lead (DL)	DLs possess in-depth expertise in specific systems. They are responsible for distinct areas (e.g., electro, automation, telecom).	
Technical System Responsible (TSR)	TSR serves as another line of technical expertise, together with DL.	N/A
The second-line emergency response team (EMT)	EMT teams handle the emergency response, while separate advisories are provided for IT and OT operations. CSIRT manages security.	The team consists of the leader, IT/OT responsible, production responsible, communication responsible, and logger. The most relevant roles in the team are the leader and the IT/OT responsible.
The OT Advisory	Industrial Automation and Control System (IACS) team acts as translators for the in-house SOC service, providing further assistance in interpreting data from offshore installations.	OT/IT responsible (OTR) handles all communication between the outsourced SOC service and the offshore installation.
Computer Security Incident Response Team (CSIRT)	The in-house SOC service provides incident response and digital forensics services.	OT/IT security personnel, and incident response service from MSSP. They act as a "task force" for the security incident.
Security Operations Center (SOC)	in-house during office hours, otherwise outsourced to an MSSP.	Outsourced to different MSSPs. Some installations have even separate MSSPs for OT and IT monitoring services.
System vendor (SV)	System vendor is the supplier responsible for the affected systems. The companies have emergency contacts to initiate an investigation quickly.	

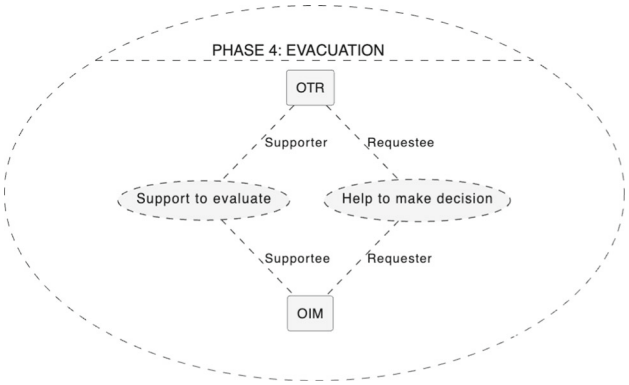

Fig. 10 The fourth phase in Diagram (ColD.B.4)

during a cyber-incident detected onshore. Company A's SOC in-house service detects a potential security incident with physical consequences and inquires with offshore management to perform an initial investigation. The installation is responsible for accessing, collecting, and sending the logs while CSIRT performs the log analysis. Specific installations are modern or have been recently upgraded and may possess digital infrastructure capable of storing and transmitting logs, whereas others may require the use of portable storage devices. The offshore installations at Company A are responsible for establishing contact with the system vendor to initiate digital forensics. At the same time, at Company B, it is the responsibility of the onshore facilities.

To help interpret the logs and information accurately, the in-house SOC service may receive support from the OT advisory that provides in-depth, installation-specific knowledge about the affected installation(s) systems, existing issues, and planned maintenance, among others. However, asking for help is optional (indicated by the "opt" frame), and the in-house SOC service may have sufficient resources to locate the cause of the security incident. After the initial investigation, Company A's incident response plan also assesses the validity of the incident (e.g., false positives) before proceeding to the next phase of incident response. The sequence is stopped (indicated by the "break" frame) if the security incident is perceived as a false positive.

Message exchange flow in SDs displays more information about interaction details than task-oriented diagrams (i.e., BPMN and AD). This may not be necessary in all cases, but it can provide helpful details for roles that require a detailed information flow. The disadvantage is that increasing the number of roles and actors increases the size of the SD, making it prone to errors when reading.

6.2.4 Activity Diagrams (AD)

Concurrent behavior is modeled more clearly in ADs than in any other type of diagram. Branches are created to display parallel activities, meaning that the first phase of detection and warning (i.e., offshore or onshore) could be modeled into the same diagram. One AD for each company (AD.A and AD.B) was created. Please refer to Figure 6 for a detailed notation description. Figure 12 displays the saving phase. Connectors (with single letters) link the current AD to the phases "Remove malware" (A), "Evacuation" (F), and "Recovery" (E). "Remove malware" may occur anytime after the first phase, as the CSIRT or SOC may initiate identifying the root cause while the offshore team follows emergency protocols. Work permits are temporary permits issued to individuals working on an offshore oil or gas installation. When entering an escalated incident, they must be removed to limit access to the safety-control systems. The phase ends with OIM initiating either the evacuation phase or transitioning directly to the recovery phase. Another advantage is that increasing the number of roles will not affect the size of the AD, but in SDs, the diagram might become too large.

6.2.5 Business Process Model and Notation (BPMN)

One BPMN diagram for each phase per company was created (BPMN.A.off.1,...,BPMN.A.5, BPMN.B.off.1,...,BPMN.B.5), totaling 12 diagrams. Please refer to Figure 7 for a detailed notation description. One pool represents the company, and swim lanes represent the roles. The BPMN is task-oriented, meaning that the diagram highlights the task each role performs, i.e., the local or individual behavior of an actor or role. This is the advantage that BPMN has over AD; i.e., in BPMN, one can also view the local or individual behavior of an actor or role, in addition to the overall coordination. Roles send messages, perform technical tasks, or execute decisions. External actors (e.g., outsourced SOC services, system vendors) are modeled as separate pools, as their specific tasks are unknown and outside the scope, except for the fact that the company communicates with them. However, creating other pools limits sequence flow usage in the diagram, as gateways cannot cross pools. Figure 13 displays the hazard limitation phase in the joint incident response plan using Company B's organizational structure. The objective of the phase is to limit the physical consequences of the offshore installation. It further demonstrates the decision-making power of OIM since they are solely responsible for the offshore installation. After making the decision, the tasks are delegated to the rest of the offshore management.

The advantage of BPMN is the explicit task distribution among the roles and the task order. However, BPMN struggles with increasing roles, such as SD, which limits the diagram's readability. A solution could be to create aggregated role descriptions and address only interactions between specific groups (e.g., offshore and onshore, security and safety). The BPMNs are further divided into joint incident response phases to limit their size. Time and role aggregation

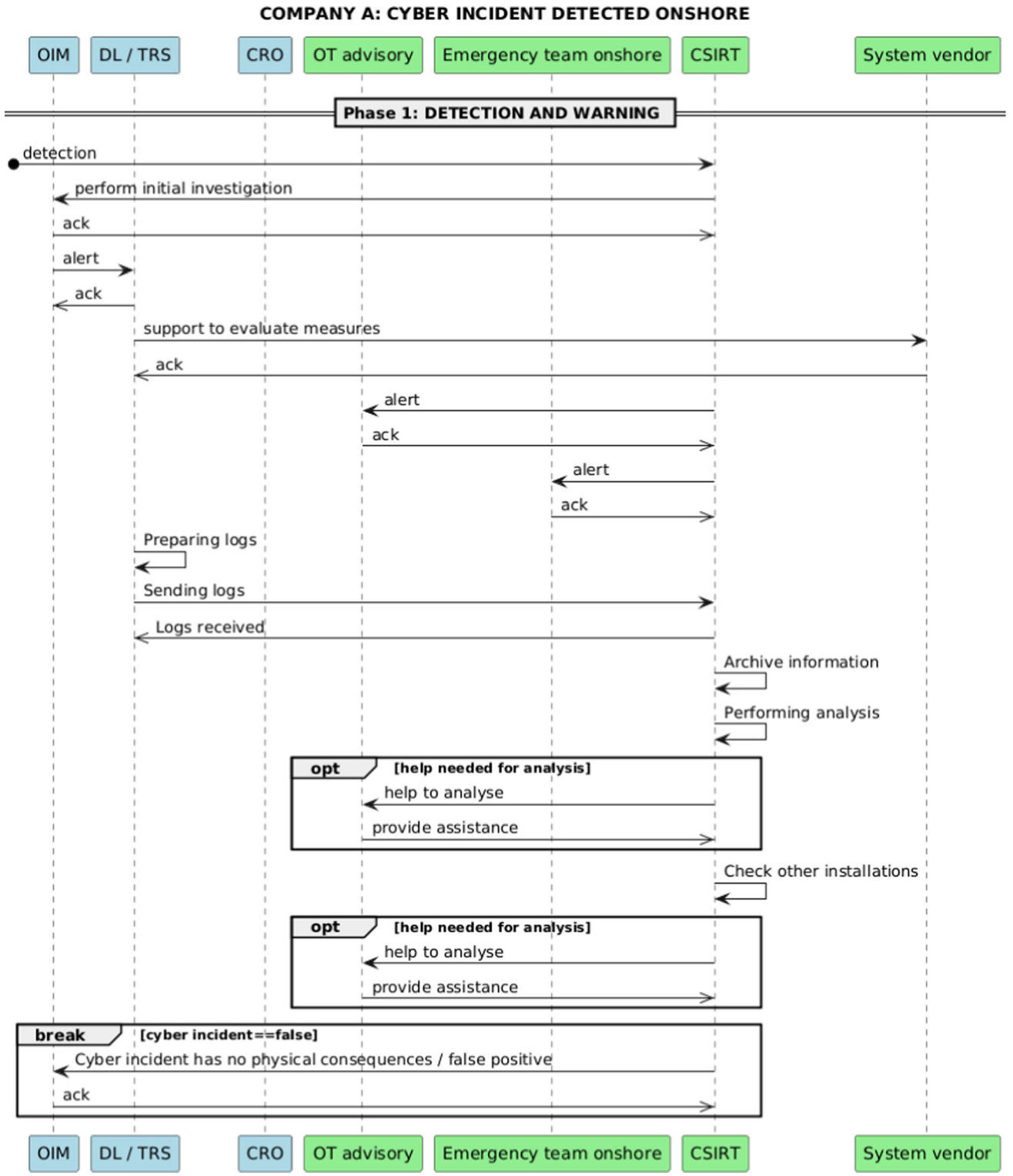

Fig. 11 The first phase in Diagram SD.A.on

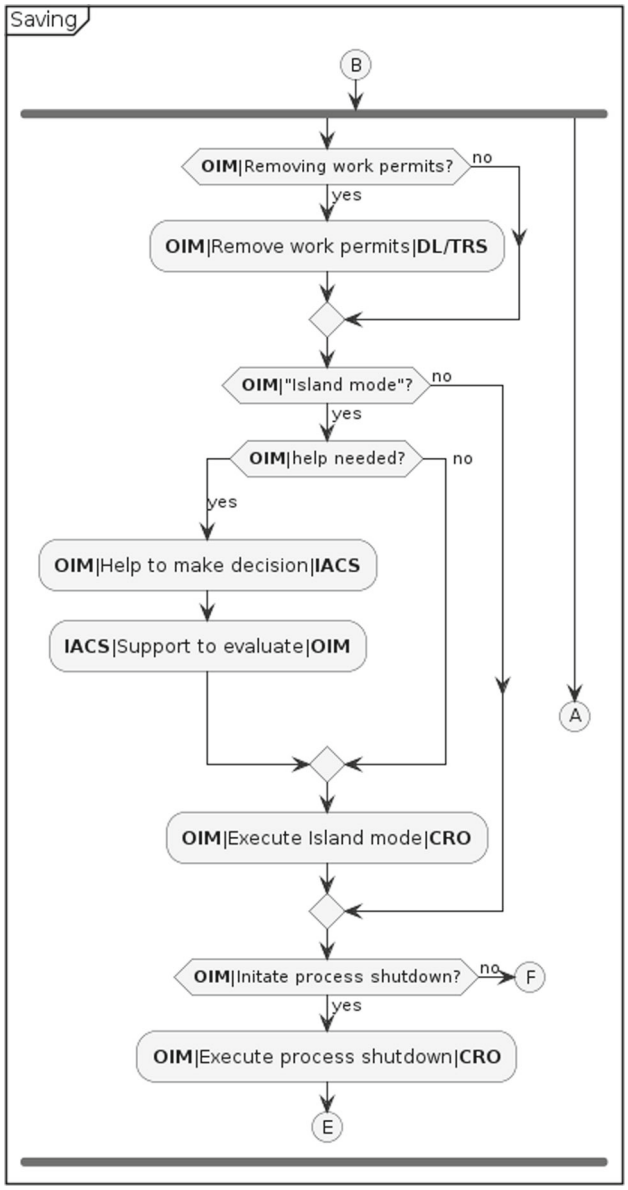

Fig. 12 The third phase in Diagram AD.A

are necessary to prevent cluttering the graphical representation in the joint incident response and to provide relevant information for each role.

7 Discussion

A holistic approach to incident response and emergency response and handling has become necessary due to the increased interaction and interdependencies between security and safety personnel in industrial sectors. The joint incident response plan users have various backgrounds, from OT engineers and control room operators to management, security operations, and IT service providers. This paper presents a framework for developing a joint incident response plan and models to enhance collaboration among various roles. The framework was applied in two Norwegian oil and gas companies, confirming that a model-based approach facilitates the effective analysis and representation of role interactions and responsibilities. Five distinct types of diagrams represent the joint incident response plans. The distinct diagrams illustrate different perspectives, focusing on roles and responsibilities. The framework may also be used to establish activities before, for example, when applying SOAR platforms from a security perspective [12]. For instance, "detection and alerting" phase might be automated by applying pre-defined e-mails to safety personnel, or asking offshore personnel to prepare for log extraction. Other cybersecurity researchers may apply the use cases to further understand the dynamics between safety and security roles and responsibilities during critical incidents in different industrial sectors.

Although we opted for UML and BPMN diagrams, the industrial organizations are free to choose another graphical representation (e.g., flowcharts). The model-driven approach can be applied regardless of the underlying technology and the system's age, since it focuses on the roles and responsibilities of personnel. Although these models are not intended to serve as run-books, but rather as tools for readiness and preparation, future work could explore methods that enable involved teams and personnel to actively monitor the progress of each relevant plan during incidents with physical consequences.

The model-driven approach supports the upcoming regulations (e.g., the EU's NIS2) by clearly structuring the tasks and responsibilities during and after cyber incidents with physical consequences for both safety and cybersecurity personnel. The joint incident response may further include non-cybersecurity personnel (e.g., safety, OT engineers) to participate in a common awareness training and contribute to developing concise business continuity and disaster recovery plans.

The joint incident response plan and the phases of the joint incident response, as displayed in Figure 1, align to some extent. Since the emergency response is considered more critical than collecting logs offshore, digital forensics may not occur until much later during incident response. This contrasts with the IEC 27035 incident response but corresponds with the ISO 22320 safety emergency response cycle. As pointed out by other works [5, 8], standardization on performing digital forensics and incident response in ICS is highly needed. The graphical modeling of the joint incident response plan provides input for improved preparedness planning by identifying resource congestion and proposing alternative time points during the incident response to perform live forensics.

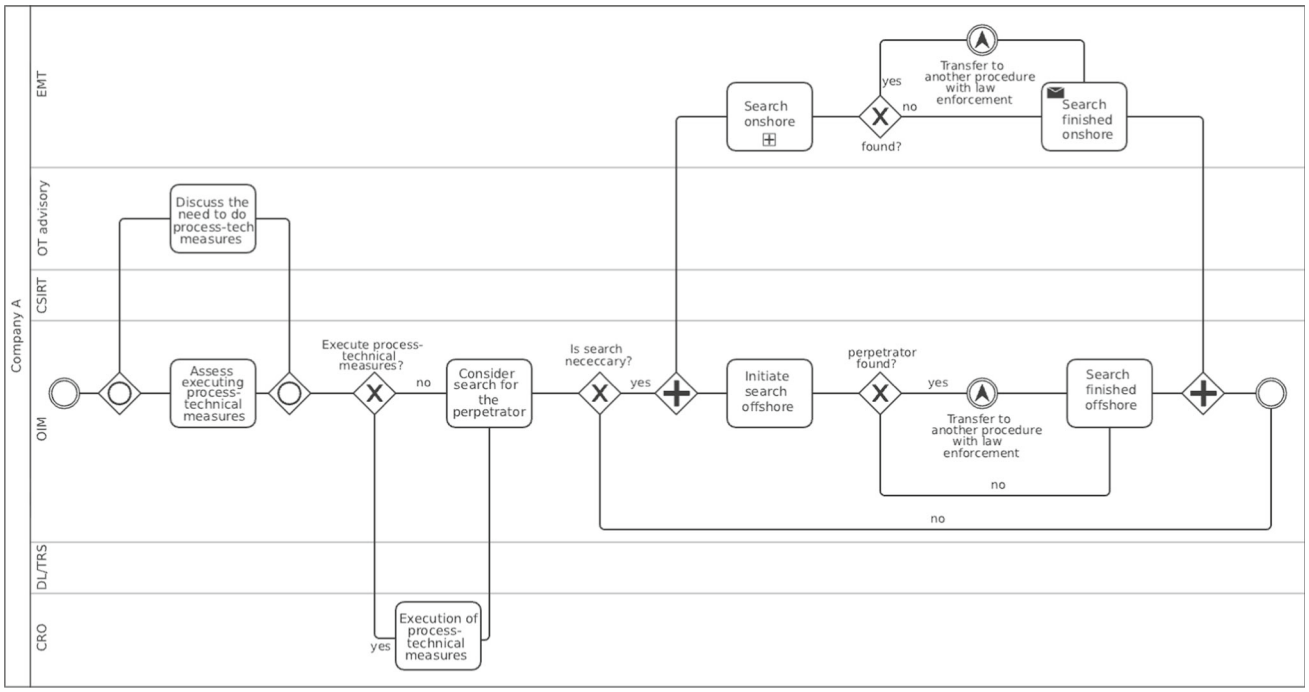

Fig. 13 The second phase in Diagram BPMN.A

However, the distinct security and safety priorities for the joint incident response personnel should be considered during the development of the plans, particularly roles that are in the intersection of security and safety (e.g., "OT advisory" in the case study). However, the personnel are still bound to follow the CAIC (Control, Availability, Integrity, and Confidentiality) safety properties. High-risk environments carry the risk of rapid, physical changes in the incident outcome that might require a swift response. The managing safety employee ultimately decides the facilities, such as the "Offshore installation manager" (OIM) in the case study. Such a swift response might be the only approach to limiting significant physical consequences. In high-risk environments, safety should always take priority over security.

The joint incident response plan used to exemplify the diagrams assumes the following: (1) a security incident is present at the offshore installation, and (2) the security incident needs to be so severe that it may affect and potentially bring harm to the physical environment. This demands an adversary with extensive domain- and even installation-specific knowledge and access to resources, with a stroke of luck to attack broadly and infiltrate successfully. A security incident should, in most cases, not affect the equipment and lives on the installation, meaning that the safety-critical systems would trigger and relieve the installation of pressure. Hence, a cyber-attack with significant physical consequences indicates that the security incident induced a failure of the safety-critical systems. Provoking malfunctions or zero-day vulnerabilities on such systems requires access to the system through the system vendor (e.g., exploiting their administrative or super-user access). Although such incidents are considered less likely, it is essential to acknowledge that the SOC monitoring system may not detect some security incidents. A potential insider may compromise the organization due to being blackmailed or disgruntled. Such actions are more challenging to observe, as they are likely to go unnoticed. If the perpetrator obtains legitimate access from the organization, it takes time to discover the attack until the control room or other observers notice anomalies in the system behavior. Insider risks in the ICS environment pose another significant security threat that can be challenging to detect.

7.1 Future Work

Future work includes verifying the common joint incident response plan and modeling diagrams with safety and cybersecurity experts, either within or outside the petroleum sector (i.e., energy, manufacturing). The objective of modeling role interactions in joint incident response is to enhance employees' understanding of their responsibilities and foster cooperation. Deadlocks and critical events are more visible. The safety and security employees gain a better understanding of their roles through discussions about their responsibilities and tasks, as well as through conducting tabletop exercises (TTX) across domains. The lessons learned activities could be further elaborated by modeling, e.g., how the roles should interact versus how they did during the incident. Overlaps in competence can be more readily

identified and considered as part of preparedness plans when assessing single points of failure, which is highly necessary in joint incident response [3].

However, no diagram fits all needs. The stakeholders should assess the modeling diagrams by conducting a mixed-method evaluation. A potential research avenue includes planning usability studies with mixed teams (e.g., IT vs. OT management) to compare the readability of the diagrams and evaluate the features elicited in this paper. The diagrams could be assessed based on the time spent understanding the plans (e.g., time-to-decision accuracy) to prove efficacy in real incidents, cognitive demand, and other quantitative factors. In addition, stress testing the diagram comprehension using full-scale simulations or even operationally testing during real incidents could be conducted to evaluate it more closely under realistic conditions.

7.2 Limitations

Convenience sampling in the recruitment process might limit the generalizability of the study findings. Although interviews, documents, and evaluation workshops contributed to method triangulation, conducting a similar study with participants outside the petroleum sector (i.e., power, healthcare) could further improve the validity of the findings. In addition, future work could investigate extending the scope of the paper also to include incidents originating from enterprise systems or incidents with fewer physical disruptions, and examining how the roles and responsibilities alter for such scenarios compared to the identified ones.

One shortcoming of modeling incident response is the level of detail in the diagrams. Sometimes, the model may be too detailed and broad (i.e., under- or over-modeling the joint incident response plan). This challenge is known in the system modeling field. The teams need to select the type of diagram depending on its intended purpose. The modeling diagrams risk becoming outdated due to the inclusion of new technology and solutions that involve other organizational roles and newly acquired responsibilities. Having said that, a too-generic model could risk potential stakeholders not identifying their duties. Discovering the silver lining in such an environment requires close interaction with employees performing the tasks to receive a sufficiently realistic idea of their actions.

Completeness (specification of all desired behaviors) in the diagrams addresses confusion in terms of enhancing the clarity of understanding the modeled behavior. The more complete the diagram, the less confusion it creates. Completeness will bring in more constructs (i.e., additional specialized notation). However, if one follows them step by step, comprehension of the behavior becomes easier and less confusing. As complexity increases, modeling languages alone may not be the most suitable choice. In addition to the modeling languages, methods may be required that include guidelines describing a systematic approach to using the modeling languages and diagrams to produce the required results [19, 35]. Investigating and designing such methods lies at the core of a discipline like systems engineering. Modeling methods have been proposed in the past (e.g., in [35, 40]) to address the complexity of distributed communicating systems, such as incident response, from different perspectives. However, our framework is not confined to any specific modeling method. The framework offers flexibility and adaptability, allowing any method that utilizes UML and BPMN languages to be employed, depending on the modeling requirements of the specific problem we want to address in a system.

Modeling diagrams can be decomposed or tailored for organizational needs. Smaller companies may not have sufficient onshore personnel, or multiple roles may be assigned to the same individual, but they often possess informal contact points. Larger companies often possess more explicit roles and procedure descriptions, but they lack flexibility and adaptability due to their rigid structure. Creating more compact diagrams in larger companies can also be solved by creating role groups. This brings us back to the scenario of over- or under-modeling.

The intent of the diagrams is not to serve as a textbook answer on how to bounce back from security incidents. It is intended as a preparation *before* the incident to assess the performance of participating roles upon detecting the security incident. The actions in the behavioral diagrams may be expected to be performed in the same order during an actual incident. It is impossible, and not the objective of the modeling diagrams, to "predict" future cyber attacks but to provide an overview for all involved parties in their roles and responsibilities. The goal of modeling a joint incident response plan is to understand roles better and facilitate resilience among them. Rather than only learning from previous incidents, the modeling approach highlights how the collaboration between security and safety personnel could occur, which is considered a critical issue in incident response [1, 5, 41].

8 Related Work

This section provides a two-fold perspective on related work. First, we review existing approaches for developing incident response plans. Second, we describe contributions that use process or system modelling in incident response.

Standardized frameworks such as NIST SP 800-61 [15], or ISO/IEC 27035 [16] define phase-based response processes that generally include preparation, detection, response, recovery, and post-incident activities. While these models provide important procedural structure, they usually address either security or safety concerns in isolation. As a result, they offer

limited support for combining both perspectives into a single, coherent response plan. To address this gap, we use the phase structures of NIST SP 800-61 and ISO 22320:2018 as a baseline (see Fig. 1). While both offer robust guidance, they lack integration instructions. Our framework builds on them by detailing each phase for a unified security and safety incident response plan.

Kamal et al. [42] propose a workshop-based process based on collaboration engineering techniques to help diverse stakeholders jointly develop incident response plans. While the process they propose provides means for creating initial plans and fostering engagement, it is not designed for long-term operational integration or cross-functional execution.

Shinde and Kulkarni [43] analyze how organizations apply existing incident response standards in practice and propose a flexible framework that combines elements from NIST, ISO, and other models. While they provide a useful synthesis of existing approaches, their focus remains on describing current practices rather than offering a detailed methodology for developing an integrated, organization-wide incident response plan.

Ahmad et al. [44] propose a structured framework for developing incident response capabilities based on a case study in the financial sector. Their model focuses on aligning strategic, tactical, and operational roles within the IT and security domain. While similar in intent to our approach, their work is limited to the IT perspective and does not address the integration of safety-related stakeholders or cross-domain coordination.

To summarize, previous work on developing incident response plans has focused on incident response from a purely security-driven perspective. In contrast, our approach aims to integrate both security and safety perspectives. Thereby, to the best of our knowledge, this paper is the first to provide a framework for developing a detailed joint incident response plan.

As the approach that we propose suggests using a model-based approach that uses established modelling languages, we also want to give an overview of the prior use of system process modeling in incident response, specifically with a focus on critical infrastructures.

Ota et al. [45] use diagrammatic representations for tabletop exercises in critical infrastructures to guide ICS operators through incident response procedures. While these visual aids help structure decision-making, they lack temporal detail and do not clearly assign responsibilities over time. This approach is valuable for fostering a general understanding of incident response logic and can support training and preparedness; however, it lacks the specificity and granularity required for direct application during a live incident.

Other prior works [46, 47] propose a structured modeling method for critical infrastructure using a customized UML extension (UML ClaD). Their approach provides a graphical notation for security incident handling but focuses mainly on the roles of security analysts, without including broader organizational actors such as operations or management. Therefore, it represents only selected parts of an overall incident response process, rather than a comprehensive, organization-wide perspective.

Erstad et al. [6] specifically address the challenge of merging cybersecurity incident response procedures with traditional safety emergency plans, specifically focusing on the maritime sector. We share a common understanding that effective incident response must bridge organizational domains and be aligned with real-world operational constraints. However, our contribution differs in method and scope. While Erstad et al. build on the assumption that both a security and a safety incident response plan already exist and simply need to be merged, our study addresses that joining the two domains requires an in-depth understanding of all involved processes, assets, and stakeholders. Furthermore, while Erstad et al. opt for using informal process models based on ISO 5807, our approach suggests using established modelling languages that offer better understanding across domains and can express both technical system behavior and organizational processes.

9 Concluding Remarks

In the digitization of industrial sectors, a joint incident response plan is crucial. However, the current literature lacks practical tools for systematically developing joint incident response plans to enhance collaboration between the security and safety domains, as well as for understanding tasks and roles in joint incident response. This paper presents a framework for developing a joint incident response plan using a model-based approach. The framework was applied in two Norwegian oil and gas companies, utilizing qualitative methods to elicit the needs and current practices in safety emergency response and cybersecurity incident response, as well as to evaluate the models. Thirty-three models, based on five types of modeling diagrams, were developed to understand the interactions between the roles in joint incident response.

Each type of diagram highlights the distinct features required to understand the interaction at various levels of the joint IR plan. The sequence diagram is the most detailed representation of the interaction between key actors during joint incident response. Activity diagrams model overall coordination among actors by displaying the ordering of joint tasks performed among roles. BPMN also provides the added benefit of showing the responsibilities of an actor at the individual or local role level. The disadvantage is the complexity of the notation (in terms of its readability). Structural diagrams provide a high-level overview of the joint incident

response, relevant for management and other personnel, and do not require detailed interactions.

The study contributes to improving the understanding of roles in joint incident response. The diagrams present a potential approach to bridge the knowledge gap between security and safety personnel, sharing their procedures and experiences across domains. The comparative analysis offers different perspectives on which type of diagram to use for representing the role interactions. Using a framework based on a model-based approach to focus on the interactions provides a first step toward unifying the understanding of a joint incident response, making it understandable to both security and safety domain personnel and experts.

Acknowledgements The authors would like to thank the industry representatives and companies that contributed to the development of the incident response procedure.

Author Contributions Conceptualization: V.G., U.R., P.E.H.; Methodology: V.G., U.F., M.G.; Formal analysis and investigation: V.G., U.F.; Writing - original draft preparation: V.G., U.F., M.G.; Writing - review and editing: V.G., M.G., U.F., P.E.H.; Supervision: U.F., P.E.H.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital).
This research was funded by the Research Council of Norway, *Cybersecurity Barrier Management*, project number 326717.

Data Availability All modeling diagrams produced for the study are publically available in the DataverseNO repository: https://doi.org/10.18710/XAKJY6. The empirical data accumulated for developing the incident response procedures is not permitted to be shared.

Declarations

Conflict of Interest The authors declare that they have no conflict of interest, competing financial interests, or personal relationships that could have appeared to influence the work reported in this paper.

Informed Consent The interview participants gave informed consent. This paper does not contain any other studies with human participants or animals performed by the authors.

Competing interests The authors declare no competing interests.

References

1. Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J.P., Andrews, W., Harish, A.V., Giménez, P., Crichton, T., Jones, K.: Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. Journal of Transportation Technologies **12**(01), 1–27 (2022). https://doi.org/10.4236/jtts.2022.121001
2. Kozak, P., Klaban, I., Slajs, T.: Industroyer cyber-attacks on Ukraine's critical infrastructure. 2023 9th International Conference on Military Technologies, ICMT 2023 - Proceedings, 1–6 (2023) https://doi.org/10.1109/ICMT58149.2023.10171308
3. Pfeifer, J.W.: Preparing for Cyber Incidents with Physical Effects. The Cyber Defense Review **3**(1), 27–34 (2018)
4. Gnanasekaran, V., Neudert, R., Heegaard, P.E., Pernul, G.: A Role Taxonomy in Security-Safety Incident Response. In: Proceedings of the 22nd International Workshop on Trust, Privacy and Security in the Digital Society (TrustBus). Springer, Cham (2025). https://doi.org/10.1007/978-3-032-00633-2_17
5. Cook, M., Marnerides, A., Johnson, C., Pezaros, D.: A Survey on Industrial Control System Digital Forensics: Challenges, Advances and Future Directions. IEEE Communications Surveys and Tutorials **25**(3), 1705–1747 (2023). https://doi.org/10.1109/COMST.2023.3264680
6. Erstad, E., Hopcraft, R., Palbar, J.D., Tam, K.: CERP: A Maritime Cyber Risk Decision Making Tool. TransNav **17**(2), 269–279 (2023). https://doi.org/10.12716/1001.17.02.02
7. Kargl, F., Van Der Heijden, R.W., König, H., Valdes, A., Dacier, M.C.: Insights on the security and dependability of industrial control systems. IEEE Secur. Priv. **12**(6), 75–78 (2014). https://doi.org/10.1109/MSP.2014.120
8. Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., Hutchison, D.: A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. International Journal of Critical Infrastructure Protection 37(March 2021), 100505 (2022) https://doi.org/10.1016/j.ijcip.2021.100505
9. Micskei, Z., Waeselynck, H.: The many meanings of UML 2 Sequence Diagrams: A survey. Softw. Syst. Model. **10**(4), 489–514 (2011). https://doi.org/10.1007/s10270-010-0157-9
10. Easttom, C.: SecML: A Proposed Modeling Language for CyberSecurity. 2019 IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2019, 1015–1021 (2019) https://doi.org/10.1109/UEMCON47517.2019.8993105
11. Sechi, F., Gran, B.A., Jorgensen, P.A., Kilyukh, O.: Better Security Assessment Communication: Combining ISO 27002 Controls with UML Sequence Diagrams. Proceedings - 3rd International Workshop on Engineering and Cybersecurity of Critical Systems, EnCyCriS 2022, 49–56 (2022) https://doi.org/10.1145/3524489.3527304
12. Schlette, D., Empl, P., Caselli, M., Schreck, T., Pernul, G.: Do you play it by the books? a study on incident response playbooks and influencing factors. In: 2024 IEEE Symposium on Security and Privacy (SP), pp. 3625–3643 (2024). https://doi.org/10.1109/SP54263.2024.00060
13. National Institute of Standards and Technology: incident response plan - Glossary | CSRC — csrc.nist.gov. https://csrc.nist.gov/glossary/term/incident_response_plan. [Accessed 16-05-2025]
14. National Institute of Standards and Technology: Guide to Operational Technology (OT) Security. Technical report, U.S. Department of Commerce (2023). https://doi.org/10.6028/NIST.SP.800-82r3.ipd
15. National Institute of Standards and Technology: Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. Technical report,

U.S. Department of Commerce (2025). https://doi.org/10.6028/NIST.SP.800-61r3
16. ISO 27035:2023: Information technology - Information security incident management - Part 1: Principles and process. Standard, International Electrotechnical Commission (February 2023)
17. ISO 22320:2018: Security and resilience – Emergency management – Guidelines for incident management. Standard, International Organization for Standardization (November 2018)
18. NORSOK Z-013:2024: Risk and emergency preparedness assessment. Standard, Offshore Norge (January 2024)
19. Bræk, R., Haugen, Ø.: Engineering Real Time Systems: an Object-oriented Methodology Using SDL. Prentice Hall International Ltd., UK (1994)
20. Ramos, A.L., Ferreira, J.V., Barceló, J.: Model-based systems engineering: An emerging approach for modern systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 42(1), 101–111 (2012) https://doi.org/10.1109/TSMCC.2011.2106495
21. Nizioł, M., Wisniewski, P., Kluza, K., Ligeza, A.: Characteristic and comparison of UML, BPMN and EPC based on process models of a training company. Annals of Computer Science and Information Systems **26**, 193–200 (2021)
22. Schlette, D., Vielberth, M., Pernul, G.: Cti-soc2m2 - the quest for mature, intelligence-driven security operations and incident response capabilities. Computers & Security 111, 102482 (2021) https://doi.org/10.1016/j.cose.2021.102482
23. Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., Strobel, J.: Managing the inevitable - a maturity model to establish incident response management capabilities. Computers & Security 125, 103050 (2023) https://doi.org/10.1016/j.cose.2022.103050
24. Pereira, J.L., Silva, D.: Business process modeling languages: A comparative framework. In: New Advances in Information Systems and Technologies, pp. 619–628. Springer, ??? (2016). https://doi.org/10.1007/978-3-319-31232-3_58
25. Cook, S., Bock, C., Rivett, P., Rutt, T., Seidewitz, E., Selic, B., Tolbert, D.: Unified Modeling Language (UML) Version 2.5.1. Standard, Object Management Group (OMG) (2017). https://www.omg.org/spec/UML/2.5.1
26. Castejón, H.N.: Collaborations in service engineering:: Modeling, analysis and execution (2008)
27. Fatima, U.: A modular method for high-level service specification and component design derivation (2017)
28. Object Management Group (OMG): Business Process Model and Notation (BPMN) Version 2.0.2 (2013). https://www.omg.org/spec/BPMN/2.0.2/PDF
29. Geambaşu, C.V.: Bpmn vs. uml activity diagram for business process modeling. In: Proceedings of the 7th International Conference Accounting and Management Information Systems AMIS, pp. 934–945 (2012)
30. Curtis, B., Kellner, M.I., Over, J.: Process Modeling. Commun. ACM **35**(9), 75–90 (1992). https://doi.org/10.1145/130994.130998
31. Kluza, K., Wisniewski, P., Jobczyk, K., Ligeza, A., Mroczek, A.S.: Comparison of selected modeling notations for process, decision and system modeling. Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017 11, 1095–1098 (2017) https://doi.org/10.15439/2017F454
32. Van der Aalst, W.: Process Mining: Data Science in Action, pp. 1–467 (2016). https://doi.org/10.1007/978-3-662-49851-4
33. Murtaza, A., Rehman, A., Malik, S.U.R., Ahmed, G., Abbas, A., Khan, M.A.: A model-based approach to enhance the communication between the participants of collaborative business processes. IEEE Access 12, 121780–121791 (2024) https://doi.org/10.1109/ACCESS.2024.3450690
34. Kotronis, C., Routis, I., Tsadimas, A., Nikolaidou, M., Anagnostopoulos, D.: A model-based approach for the design of cyber-physical human systems emphasizing human concerns. In: 2019 IEEE International Congress on Internet of Things (ICIOT), pp. 100–107 (2019). https://doi.org/10.1109/ICIOT.2019.00028
35. Fatima, U., Bræk, R.: The interface-modular method for global system behaviour specification. In: Desfray, P., Filipe, J., Hammoudi, S., Pires, L.F. (eds.) Model-Driven Engineering and Software Development, pp. 339–355. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-27869-8_20
36. 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. EnCyCriS/SVM '24, pp. 53–60. Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3643662.3643958
37. Fujs, D., Mihelič, A., Vrhovec, S.L.R.: The power of interpretation: Qualitative methods in cybersecurity research. ACM International Conference Proceeding Series (2019). https://doi.org/10.1145/3339252.3341479
38. Tjora, A.: Qualitative Research as Stepwise-deductive Induction. Routledge advances in research methods. Routledge, Abingdon, Oxon (2018)
39. Gnanasekaran, V., Fatima, U., Heegaard, P.E.: Replication Data for: A Model-Based Framework for Developing Security-Safety Incident Response Plans. DataverseNO (2024). https://doi.org/10.18710/XAKJY6
40. Mesloub, K., Innal, F., Ducq, Y.: Emergency response plan modeling using idef0 and bpmn approaches. International Journal of Safety & Security Engineering **13**(2) (2023) https://doi.org/10.18280/ijsse.130220
41. Olsen, A.: Responding to and Recovering from a Cyber Attack, pp. 641–647. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-55943-3_48
42. Kamal, M., Davis, A.J., Nabukenya, J., Schoonover, T.V., Pietron, L.R., Vreede, G.-J.: Collaboration engineering for incident response planning: Process development and validation. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), pp. 15–15 (2007). https://doi.org/10.1109/HICSS.2007.128
43. Shinde, N., Kulkarni, P.: Cyber incident response and planning: a flexible approach. Computer Fraud & Security **2021**(1), 14–19 (2021). https://doi.org/10.1016/S1361-3723(21)00009-9
44. Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T., Baskerville, R.L.: How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security **101**, 102122 (2021). https://doi.org/10.1016/j.cose.2020.102122
45. Ota, Y., Aoyama, T., Nyambayar, D., Koshijima, I.: Cyber incident exercise for safety protection in critical infrastructure. International Journal of Safety and Security Engineering **8**(2), 246–257 (2018). https://doi.org/10.2495/SAFE-V8-N2-246-257
46. Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L.E., Ismail, U.M.: Modelling language for cyber security incident handling for critical infrastructures. Computers and Security **128**, 103139 (2023). https://doi.org/10.1016/j.cose.2023.103139
47. Athinaiou, M., Mouratidis, H., Fotis, T., Pavlidis, M., Panaousis, E.: Towards the definition of a security incident response modelling language. In: Furnell, S., Mouratidis, H., Pernul, G. (eds.) Trust, Privacy and Security in Digital Business, pp. 198–212. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98385-1_14