Computers & Security 128 (2023) 103139

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Modelling language for cyber security incident handling for critical infrastructures

Haralambos Mouratidis[a,*], Shareeful Islam[b], Antonio Santos-Olmo[a,c], Luis E. Sanchez[a,c], Umar Mukhtar Ismail[d]

[a] Institute for Analytics and Data Science, University of Essex, UK
[b] School of Computing and Information Science, Anglia Ruskin University, UK
[c] GSyA Research Group, University of Castilla-La Mancha, Ciudad Real, Spain
[d] Department of Engineering & Computing, University of East London, UK

ARTICLE INFO

Article history:
Received 7 September 2022
Revised 27 December 2022
Accepted 12 February 2023
Available online 15 February 2023

Keywords:
Critical infrastructure
Meta-model
Incident response
Cyber incident
Cyber course of action
Cyber threat intelligence
Security requirements

ABSTRACT

Cyber security incident handling is a consistent methodology with which to ensure overall business continuity. However, specifically handling incidents for critical information infrastructures is challenging owing to the inherent complexity and evolving nature of the threat. Despite the number of contributions made to cyber incident handling, there is little evidence of literature that focuses on modelling activities that will enhance developers' abilities to model incident handling processes and activities according to different views. Modelling languages of this nature should integrate essential concepts and a descriptive implementation process in order to enable developers to analyse, represent and reason about the crucial incident handling efforts required to support critical information infrastructures. The aim of this paper is, as part of the CyberSANE EU project, to develop a Cyber Incident Handling Modelling Language (CIHML) that focuses explicitly on modelling incident handling in the context of a critical information infrastructure. The work is innovative in its approach because it consolidates concepts from various domains such as security requirements, forensics, threat intelligence, critical infrastructures and cyber incident handling. The approach will allow the phases of the incident handling lifecycle to be modelled from three different views (critical information infrastructures, threat and risk analysis, and incident response). An implementation process is also proposed, which will serve as a comprehensive guide for developers in order to create these modelling views. Finally, CIHML is evaluated using a real-life scenario from the CyberSANE project to demonstrate its applicability. The incident observed had a severe impact on the overall business continuity of the context studied. The results obtained from the study show that CIHML can help critical information infrastructure operators to identify, evaluate, represent and model cyber incidents in critical information systems, in addition to providing the support required to determine the response strategies needed in order to mitigate these cyber-attacks.

1. Introduction

Critical Information Infrastructures (CIIs), such as energy, transportation and telecommunication networks, are greatly depended upon for the delivery of reliable essential services. The complexity among various components of CIIs (such as people, processes, and technology), make them a prime target for cybercriminals. There has recently been a constant increase in the number of high-profile security incidents that continually target CIIs (Lewis, 2019; Maglaras et al., 2018). Cyberattacks are now becoming increasingly more complex, multi-vector, and rapidly evolving, which results in severe disruptions to critical services and overall business continuity (Kure et al., 2022). Despite the significant investments made in order to implement security controls, organisations must develop incident handling processes with which to prepare for impending incidents (Wang and Park, 2017). The research and industrial communities have made several efforts to provide incident handling processes (Papastergiou et al., 2019; Sabillon, 2022; Salvi et al., 2022; Staves et al., 2022). However, there is a lack of focus on the model-based approach for a comprehensive incident analysis that will provide a common understanding of possible incidents and their mitigation. This limitation poses a significant challenge for the extensive study and representation of a security incident

* Corresponding author.
E-mail address: h.mouratidis@essex.ac.uk (H. Mouratidis).

https://doi.org/10.1016/j.cose.2023.103139

handling process, especially for CIIs. It also hinders the ability of CII operators to understand the security and privacy-related requirements for incident handling.

This paper presents a new Cyber Incident Handling Modelling Language (CIHML) that supports the analysis, reasoning and representation of cyber incident handling processes in CII. The CIHML is part of research efforts in CyberSANE[1] to develop a modelling language that will enable CII operators to reason about cyber incident handling requirements, security and privacy requirements. The main aim of the CyberSANE project is to improve the security and resilience of Critical Information Infrastructures through the use of a dynamic collaborative response system with which to manage incidents and analyse and forecast threats. The project places emphasis on the effective interactions among the CII operators and develops correlation techniques and standards that can be employed to analyse events and information sharing. To this end, CIHML contributes with systematic incident management and the coordination of CII operators in order to support the objectives of the CyberSANE. This signifies that CIHML is requirements driven – it uses requirements-based concepts (such as actor, goals, constraints) to analyse and model cyber incident handling. The key contributions of this paper are summarised as follows:

- A meta-model that consists of a set of concepts with which to specify and express cyber incident handling according to the specific requirements and contexts of CIIs. It extends requirements engineering concepts, including relevant cybersecurity and privacy domains, in addition to a wide range of industrial best practices, guidelines and standards.
- The provision of a process that guides the effective modelling of security and privacy concerns related to incident handling processes, including the analysis of incidents such as potential impact and the likelihood of an attack, the CII assets affected, the consequences of threats and risks, and incident response strategies.
- The formulation of modelling views with which to represent specific requirements for incident handling. The objective of these modelling views is to drive the practical analysis, prevention, detection, response and mitigation of various cyber incidents. The modelling views entail graphical visualisation that will also facilitate understanding and enhance the ability of CII operators to model and reason about security and privacy requirements.
- CIHML is validated through a real-case study from the CyberSANE EU funded project. Our results show that CIHML enables operators to perform the detailed modelling of a cyber incident (Jigsaw Ransomware). It also supports the explicit representation of the potential impact of a cyber incident (according to high, medium and low priority) on the different assets of the context studied in a structured and analysable manner. Moreover, CIHML enables the modelling of mitigation strategies that improve upon existing control measures and more adequately defend against cyberattacks, which are vital to incident response. In general, CIHML provides a better understanding of the entire CII setting and overall incident response decision-making and communication process among stakeholders.

The paper is structured as follows: Section 2 covers the related works, while Section 3 presents a description of the approach/methodology, along with the criteria considered in order to develop CIHML. This section also introduces new concepts, a conceptual model, and a process for CIHML. The implementation and evaluation of CIHML is provided in Section 4 by means of a real-life case study derived from the CyberSANE Project. A general discussion is presented in Section 5, and the paper concludes in Section 6.

2. Related work and background

This section presents the existing work that is relevant to our work, including incident handling, security modelling, and relevant standards.

Possible attacks by attackers may lead to various cybersecurity incidents, including critical service operation disruption, data leak and software interruption (Gaidarski and Minchev, 2021; Lehto, 2022). Cybersecurity incident management deals with multiple steps with which to analyse and manage these incidents. Security incidents are undesired events that impact on the different dimensions of the valuable assets that make up a company's information systems (Mahima, 2021). These incidents are caused by failures in the implementation of the security controls that protect these assets, i.e. by vulnerabilities that exist in the information systems. These vulnerabilities are exploited by attempts to reach these assets and cause damage to them (Ramsay et al., 2020).

In order to minimise the damage of these incidents, organisations attempt to apply the most appropriate incident response methods (Prasad and Rohokale, 2020). Many organisations have focused on managing risks through integrated services in Computer Security Incident Response Teams (CSIRT), as these have proved to be one of the best solutions with which to improve cybersecurity by collaborating with each other, sharing knowledge and learning from cross experiences (Tanczer et al., 2018). However, the implementation of a CSIRT comes at a considerable cost, which makes it suitable only for large organisations, thus implying need to create simpler and more effective incident management systems for small and medium-sized enterprises (Plėta et al., 2020).

Security incident management and response can be considered a hot research topic with some relevant open questions (Grispos et al., 2017). One of the most relevant question is how to achieve a reasonable situational awareness in order to discover the situation regarding vulnerabilities, threats and possible security incidents (Ahmad et al., 2021). Intense research has recently been carried out in this area by, for example proposing models with which to explain how organisations should achieve situational awareness of cybersecurity (Ahmad et al., 2020). It is argued that providing a rapid and efficient response to security incidents clearly supports cybersecurity awareness and improves the overall cybersecurity performance of companies (Naseer et al., 2021), or that misinformation should be considered as one of the key reasons for the lack of situational awareness (Ahmad et al., 2019). Indeed, it is often claimed that attackers take advantage of the lack of corporate communication following cybersecurity incidents (Knight and Nurse, 2020) and the lack of learning from their experiences of incidents (Ahmad et al., 2020). One study concluded that learning from a low impact incident should not be ignored when compared to a high impact incident, thus allowing the organisation to aim for initial and early events (Ahmad et al., 2012).

A number of research proposals have emerged in response to these problems in incident management, and several incident management approaches and frameworks have been introduced with the main objective of providing guidelines with which to enhance incident handling capabilities. Tøndel provides a systematic overview of current incident management practices based on the underlying phases of the incident management process. The study emphasizes more empirical studies, tactic knowledge and the identification of root causes in order to understand and manage the incident (Tøndel et al., 2014). Nnoli et al. (2012) meanwhile, highlight the importance of effective forensic investigations while analysing the incident owing to the lack of guidance with which to investigate forensic evidence.

[1] CyberSANE: https://www.cybersane-project.eu/

The aforementioned work also emphasizes the consideration of root cause analysis from all dimensions for incident analysis. Metzger et al. (2011) proposed a process-based integrated incident management approach that combines all incident reporting channels for rapid incident response . Papastergiou et al. (2019) presents an overview of the CyberSANE system that tackles the incident, concentrating particularly on European Critical Information Infrastructures. The approach integrates active incident handling with a reactive approach in order to provide a real-time insight into attacks and alerts related to cyber events using multiple subcomponents. Athinaiou et al. (2018) developed a security incident response modelling language by integrating a cyber-physical system with incident response considered for health-based critical infrastructures . Incidents are specifically modelled by means of reflexive associations that cascade the influence from one incident to another incident. The model is visually presented using various notations without providing any details on how the incident could be a response.

There are also works that aim to evaluate the incident handling experience. Kuypers (2017) evaluates how cybersecurity incidents are dealt with in large organisation. The investigation considers many incidents over a period of time and observes that small incidents are increasing while large incidents are remarkably constant over time. The result shows that organisations have become more efficient at dealing with large cyber incidents when compared to small incidents. Metzger employed real-world incident investigation as the basis on which to recommend a security incident response process, including clearly defining the roles and responsibilities required to manage an incident (Metzger et al., 2011). The study also emphasizes the need for centralised monitoring tools and highlights that there is a specific low-risk security incident which may occur frequently. Fombona Cadavieco et al. (2012) investigated incidents in a higher education institute over a period of time, and the results show that software-related incidents are more frequent than other incident types, and that incident rates are constant despite the fact that the number of devices is increasing. Chockalingam proposed the development of an ontology for security incident management, which aims to make security incident response more practical, and validated it in a case study (Chockalingam and Maathuis, 2022).

Furthermore, various standards have emerged that focus on attempting to solve some aspects related to security incident management. NIST SP 800-61 (Cichonski et al., 2012) is a widely used structural approach that guides the planning, detects access, and provides reports and lessons learned in order to manage the incident. ISO provides a basic definition of concepts and phases for information security incident management, including a structured guideline with which to plan and prepare incident management. NIST SP 800-61 provides an incident response guideline that aims to provide practical guidance in order to respond to cybersecurity incidents. The guideline comprises detailed recommendations that can be used to establish an incident response programme with a focus on the structure of an incident response team, the steps required in order to perform incident handling (such as incident detection and analysis), and incident response coordination and information sharing. Furthermore, ETSI_TR_103_331_V1.2.1, 2019 provides threat information sharing and exchange in a standardised and structured manner. ENISA (2010) also provides guidelines for incident handling by combining both ISO/IEC and NIST and focuses mainly on the incident response. ISO27035:2016 provides guidance for Incident Management Principles (ISO/IEC_27035-1:2016, 2016) and Guidelines for Planning and Preparing for Incident Response (ISO/IEC_27035-2:2016, 2016).

Upon concentrating on the case of incident management when focused on critical infrastructures, it will be noted that researchers highlight its importance, as derived from the interdependence of organisations and Advanced Persistent Threats (APTs) (Settanni et al., 2017). Other research highlights the importance of having an effective model that regulates the management of security incidents in critical infrastructures and analyses the characteristics that an incident management model should have, focusing on the energy sector (Plėta et al., 2020). Focusing on the critical sector of airports, attempts have been made to develop some models based on ontologies, which include aspects such as incident management, and the attempts made to correlate them and enrich them with information from external databases (Canito et al., 2020). With regard to the aviation sector, research has also been carried out based on the analysis of the most serious incidents suffered in recent years, reaching the conclusion that it is necessary to develop specific CSIRTs for this sector and that they should be based on NIST principles (Lekota and Coetzee, 2019). Other researchers have focused on analysing current SIEMs in order to determine their strengths and weaknesses when applied to incident management in critical infrastructures, reaching the conclusion that the current models should be strengthened so as to improve reaction time and decision-making capacity in the face of a high number of incidents (González-Granadillo et al., 2021). What all the research does agree on is that it is necessary to further develop models with which to manage security incidents in this type of infrastructure.

If we focus on the development of meta-models for incident management in critical infrastructures, there are very few publications. In the naval sector, attempts have been made to develop some models for incident response management, such as the Cyber Incident Response Decision Model (CIRDM), which is based on a metamodel whose main elements are component, system, mission, function, vulnerability and countermeasure (Visscher, 2021). Within the hydrocarbon transport sector, an ontological model for security incident management is also presented, focusing on the relationships that exist between the different elements, which are: CyberIncident, AttackVector, Vulnerability, Asset, Victim, Offender, Request, Investigator, ActionPlan, ApplicationAnalysis, CortainIncident, and Financial (Chockalingam and Maathuis, 2022). As can be seen, there is little research on the development of these meta-models for critical infrastructures, and they tend to have little in common when it comes to defining their constituent elements.

Other research is oriented towards the construction of a modelling language for security incident response (Athinaiou et al., 2018). The creation of a system that can support security managers in incident management in CIIs is also dealt with (Papastergiou et al., 2019), as is incident handling, targeting critical sectors such as energy and transport (Papastergiou et al., 2021). But all this research is linked to partial results obtained from the Cybersane project, of which the research proposed in this publication is also part.

Below (see Table 1), a comparison has been made of the elements that make up the CIHML proposal along with other proposals for meta-models for security requirements that currently exist.

As can be seen, 6 proposals have been selected, in addition to CIHML. The main conclusions that can be drawn from the comparative analysis are the following:

- All of them differ as regards the selection of the elements that make up the meta-models. Most of them coincide as regards taking into account the central elements (Actor, asset, goal, vulnerability), but they tend to differ in the case of the other elements.
- It is also possible to see that, although most of them are oriented towards critical infrastructures, they are focused on different sectors (Energy, Water and sewage treatment, Naval Sector, Hydrocarbons, etc.).

Table 1
Comparison of meta-model proposals for security requirements.

	CIHML	Faily and Fléchais, (2010)	Simou et al. (2016)	Yeboah-Ofori and Islam (2019)	Visscher, (2021)	i-CSRM (Kure et al., 2022)	Chockalingam and Maathuis, (2022)
Actor	Yes	Yes	Yes	Yes	No	Yes	No
Malicious Actor	Yes	Parc	Parc	No	No	Parc	No
Asset	Yes	Yes	Yes	No	No	Yes	Yes
Vulnerability	Yes	Yes	No	Yes	Yes	Yes	Yes
Threat	Yes	Yes	No	Yes	No	Yes	No
Impact	Yes		No	No	No	No	No
Risk	Yes	Yes	No	Yes	No	Yes	No
Goal	Yes	Yes	Yes	Yes	No	Yes	No
Constraint	Yes	No	No	No	No	No	No
CyberIncident	Yes	No	Yes	Yes	No	Yes	Yes
Control	Yes	Parc	Parc	Yes	No	Yes	No
Mechanism							
CCA	Yes	No	No	No	No	No	No
Evidence	Yes	No	Yes	No	No	No	No
TTP	Yes	No	No	Yes	No	Yes	No
Dependency	Yes	Yes	No	No	No	No	No
OtherElement		Scenario, Misuse case, Security Attribute, Requirements, Task,	Protective, Cloud provider, Documentation, Resource	CSC Requirements, InformationSharing	Component, System, Mission, Function, Countermeasure	Indicator, Plan, Threat Actor,	AttackVector, Victim, Offender, Request, Investigator, ActionPlan, pplicationAnalysis, CortainIncident, Financial
Orientedto	CII - Energy	CII - Water and sewage treatment	Cloud system	SuplyChain	CII - Naval Sector	CII - General	CII - Hydrocarbons

- Moreover, some proposals use similar concepts, but they are not exactly the same, and they differ in their sub-elements.
- Finally, another interesting conclusion of the comparative study is that other elements included in other meta-models could be analysed in order to discover whether they could enrich the proposal made by CIHML. And it would be possible to analyse whether the variability in the meta-models is associated with their sectoral or technological focus.

We have made several observations regarding the existing works, standards, and practices relating to incident management. Firstly, the existing works place more emphasis on the technical solutions required in order to manage the incident rather than a root cause analysis of the incident by taking into account assets, threat intelligence, vulnerabilities, evidence, incident, and control. Secondly, little effort has been made to develop an incident management modelling language specifically focusing on critical information infrastructure. Finally, the incident analysis needs to consider security requirements, threat intelligence, risk and forensic evidence from a holistic perspective if it is to tackles today's sophisticated incident and complex system context. Our work contributes to addressing these limitations. In particular, the main contribution of this work is: (i) the development of a cybersecurity incident handling modelling language from a holistic perspective; (ii) the visual analysis of the incident from three distinct views, including the critical information infrastructure, threat and risk analysis, and incident response, and (iii) an evaluation of the applicability of the CIHML using a real industrial use case scenario.

3. Methodology used to develop CIHML

In this section, we present a summary of the approach followed when developing CIHML, which comprises two important parts, namely (i) the identification of concepts and (ii) the development of a conceptual model and a process.

The development of any modelling language principally requires a structured definition, elicitation, and reasoning of domain-related concepts, along with the application of a well-established methodology (Nordstrom et al., 1999). Moreover, Kosar carried out a systematic mapping study in order to analyse the different existing proposals regarding Domain-Specific Languages (Kosar et al., 2016), in which it was concluded that the adaptation of this methodology and a guideline implies the integration of new context-specific concepts and consolidation with pre-existing ones in a comprehendible and consistent manner that satisfies the requirements for incident handling. CIHML, therefore, leverages and extends the existing requirements engineering concepts in Secure Tropos (Mouratidis et al., 2016) with relevant concepts from such domains as digital forensics, cyber resiliency and cyber threat intelligence. The rationale behind adopting Secure Tropos is that it is well suited to the modelling of security requirements and provides an in-depth analysis of the security issues in an organisation and its social setting.

Secondly, a conceptual model is developed in order to provide the foundation for the specification and representation of the extracted concepts. The main reason for the conceptual model is to provide a high-level understanding of the concepts and their relationships in order to model incident handling activities so as to provide shared knowledge among developers and the CII incident response team (IRT). The conceptual model for the language is developed using a UML class diagram, which employs a graphical notation to construct and visualize object-oriented systems by representing a system's classes, their attributes, operations and the relationships among objects (Idani, 2009). Each concept is presented as a class with a list of attributes, the concepts are related to each other using relationships such as association and generalisation, and a glossary is provided in order to elucidate the meaning of the concepts. Moreover, a process with which to supplement the meta-model is included. The process serves as a guide for developers in the course of implementing the conceptual model. The process consists of activities and tasks, and it encompasses various techniques, methodologies, and industrial standards so as to ensure validity, comprehensibility and compliance with generally accepted guidelines.

3.1. Research objective and criteria for CIHML

In order to develop a more elaborate alignment between CIHML and standard methods, we consider the main objectives of the re-

search and present several core criteria that should be fulfilled to achieve the objectives. The criteria consider the specific requirements of the CyberSANE Project stakeholders, i.e. the artefacts the prospective users of CIHML expect from it. These artefacts have been established by analysing the patterns of actions, expectations and decision making that should be supported.

The review of the existing works and practice as presented in Section 2 was used as the basis on which to define the main objectives of this work, which are provided below, while the criteria were defined according to specific design principles and requirements that every modelling language should aim to satisfy (Kolovos et al., 2006). We have defined the following criteria for the CIHML:

- Improve the incident handling of critical infrastructure by providing a modelling language that includes a comprehensive understanding of the critical infrastructure context.
- Systematically guide the incident response process on the basis of a control mechanism and its categorisation and cyber course of action. This supports determination control types which are more important for CI context.
- Develop an incident modelling and handling approach, from the critical infrastructure context to the analysis of threats, vulnerabilities and risks relating to the incident, thus allowing appropriate reasoning and modelling views to be obtained for the incident and suitable actions with which to tackle the incident to be determined.
- Integrate the existing best practices, guidelines and concepts for the development of a unified incident handling process, including impact assessment, with a view to more widespread adoption in any specific CI sector.
- Requirements-Driven Modelling Approach: CIHML shall provide the mechanisms required in order to elicit, collect and analyse requirements associated with security and privacy requirements towards cyber incident handling in CIIs.
- Embed Essential Domain Specific Concepts and industry specific best practice: CIHML shall consider a certain set of domains specific concepts, relevant properties, and industry specific standards and practices, thus allowing it to provide comprehensive support for incident handling. CIHML shall, therefore, encapsulate domain specific concepts from security requirements, incident handling, forensics, risk management and incident handling.
- Different Levels of Abstraction: CIHML shall provide adequate modelling capabilities from a conceptual, strategic, and tactical point of view, each focusing on various aspects that promote the modularity and separation of incident handling processes and supports the reasoning and analysis of incidents and selected controls.
- Analysis of Cyber and Representation of Incidents: CIHML shall facilitate a systematic analysis of cyber incidents by enabling the effective representation of operational and security threats, vulnerabilities and risks to CII assets. It shall provide easy ways in which to create dynamic models that are capable of showing various incident assessment outcomes, such as the severity of threat elements, affected assets, and the corresponding control measures.

3.2. CIHML concepts

This section presents a detailed description of the essential concepts used when developing CIHML. As mentioned earlier, the concepts were mostly conceived from various domains including security, forensics, threat intelligence, critical infrastructure and cyber incident handling, which are relevant for the development of the modelling language. The rationale behind the inclusion of these concepts is based on the analysis, elicitation and documentation of stakeholders' requirements in the CyberSANE project (CyberSANE, 2022). This will additionally make it possible to develop a unified approach that will be provide broader adaption of the proposed approach. Some of the concepts are, therefore, generic, but others such as CIIs focus on understanding the whole CII system context, in addition to which our approach links the control mechanism with the course of action required to tackle the incidents. The underlying goal is to ensure that the concepts are integral for the effective and efficient prevention, detection, response and mitigation of various cyberattacks against the CIIs. We have, therefore, identified and consolidated the following concepts in CIHML

- Critical Information Infrastructure (CII): this implies communication networks, information-based facilities, cyber-physical assets or systems that support the operations of critical infrastructure, which if damaged, would result in serious consequences for the proper functioning of critical public, government or industrial services. CII can also be considered to be those systems that provide resources or services upon which essential functions depend, of which possible incapacitation or destruction would result in a significant effect on the economy, security and/or health of society.
- Actor: this represents an entity with intentions, goals, and objectives within a system. An actor also participates in a process, performs a task, or carries out an action within an organisational setting. An actor is categorised according to type (such as a developer), including the role performed by an actor (such as system development and administration).
- Assets: these are cyber resources that can be used by the actors to support the critical functions such as systems, software, data, network devices, or other components that enable information-related activities, management, service delivery. Assets are characterised by varying attributes such as categorisation and criticality. An asset can be categorised according to network, software, or data. An asset's criticality expresses the importance or degree to which the asset is relied upon for the delivery of critical functions.
- Goal: this represents a strategic interest that an actor aims to achieve. Goals are mainly introduced in order to achieve possible security constraints that are imposed on an actor or that exist within CIIs. A goal consists of attributes such as type and purpose; for example, authentication and authorisation controls could be the goal of an asset whose purpose is to ensure security protection.
- Constraint: a set of restrictions related to security and privacy that must be satisfied for a specific asset or actor goal to be achieved. It consists of a 'type' attribute that distinguishes security and privacy constraints.
- Malicious Actor: this represents an individual, groups or organisations that participate in hostile actions or operate with malicious intents in order to have harmful effects on CIIs. It is imperative to identify and represent different types of threat actors on the basis of distinctive characteristics and motives (such as goals, motivation, tactics, and procedure) to compromise CIIs. Threat actors can, therefore, be characterised by their goals, and the tactics, techniques, and procedures that they use.
- Cyber Incident: this implies a security-related event that produces unanticipated consequences, unwanted occurrences or instances that will probably compromise, breach, or violate the security policy. A cyber incident has an adverse effect on the organisation's information system owing to any potential disruption and impacts on confidentiality, integrity and availability. A cyber incident provides a useful understanding of possible threats within the organisation. For example, a cyber inci-

dent can include but is not limited to the unauthorised disclosure of classified information, the unauthorised modification of classified information, and the malicious disruption, use or processing of CIIs.

- Impact: the measurable implications or consequences caused by a security incident for assets within CIIs. The intention is to measure the potential severity of the adverse effect that a security incident has on CIIs. The impact contains attributes such as description, type, affected, affected infrastructure, and severity.
- Vulnerability: this refers to weaknesses in an asset or a security mechanism that can be exploited by a threat and which could result in degradation or loss (incapacity to perform its designated function).
- Threat: this implies any cyber-event with the potential to have an unwanted effect on or harm the asset because of vulnerabilities being exploited by a threat actor. The attributes of threat include a category that describes the class of threat (such as a denial of service), the severity of the threat with regard to its potential impact and affected assets in order to identify the assets affected by the threat.
- Risk: this is the potential consequence of an incident, threat or vulnerability that can result in a range of negative consequences, loss, damage, or the undesirable change to assets. Risk is associated with attributes such as the likelihood, which measures the possibility of a potential risk occurring, and impact, which estimates the potential losses associated with an identified risk.
- Control Mechanism: this represents any technical safeguards, systems, or processes that are used to safeguard assets, manage risk, control threats, manage security incidents and mitigate vulnerabilities. The concept is characterised by attributes according to type, goals, and measure of effectiveness to either remove, counter, or mitigate risks or cyber-incidents. There are three distinct types of control mechanisms:
  - Detective Mechanisms: these include security control measures implemented to detect and send an alert regarding impending threats or incidents.
  - Preventive Mechanisms: these are designed to prevent a security incident, a threat or risk from occurring, and reduce or avoid the likelihood of them and their potential impact on CIIs.
  - Corrective Mechanisms: these include control measures that are taken to address existing damage or restore CIIs to their prior state following a security incident.
- Evidence: this represents electronic data concerning observable patterns, artefacts, or behaviour that can be used to analyse a security incident. Evidence is generated from various sources such as log files, error messages, intrusion detection systems, or firewalls. For example, evidence of an incident may be captured in several logs that each contains different types of data. It includes attributes such as type, to indicate the evidence type, and the source from which evidence is extracted, such as intrusion detection system logs.
- Cyber Course of Action: this is related to a set of security controls with which to tackle the incident. It is characterised by procedural and technical courses of action that are applied within an operational setting in response to the impact of cyber-incident. The control focuses mainly on the vulnerabilities that are exploited for the incident, and suitable remediation. In contrast to Control Mechanism, Cyber Course of Action is intended to integrate a combination of technologies and administrative procedures with which to recover from and adapt to adverse security incidents, risks and impacts on CIIs that have not been sufficiently prevented by the Control Mechanism.
- Tactics, techniques, and procedures (TTP): These represent the behaviour or mode of operation of the adversary or threat actor. The TTP could be used to gather information about the attack pattern, resources deployed, and exploits used. TTP is relevant as regards identifying threat actors and gaining knowledge about the attacker's motives and expected impact.
  - Tactics: these describe how threat actors operate during different types of attacks.
  - Techniques: these are the strategies used by the adversary to facilitate initial attacks, such as the tools, skills and capabilities deployed.
  - Procedures: these are the set of tactics and techniques put together to carry out an attack. Procedures may vary depending on the threat actor's objective, purpose and nature of the attack.

3.3. Conceptual model

Fig. 1 shows the conceptual model for CIHML, which provides an interpretation of and highlights the relationship among the concepts. The concepts in the meta-model are represented as boxes, while the attributes are properties inside the boxes, and the relationship between the concepts is created using arrowed lines. The critical information infrastructure provides vital functions and operations within a specific sector such as health and energy, whose disruption could result in severe disruption to the economic wellbeing, security, or safety of society. The critical infrastructure is usually operated and used by actors who have different types of goals (security and privacy goals). Moreover, each critical infrastructure consists of and requires a wide range of cyber assets for it to deliver critical functions. The critical infrastructure is, therefore, appraised in order to specify the underlying domain and boundary of operations, the actors whose interest and goals must be represented, the particular security and privacy constraints imposed on actor goals, and the supporting cyber assets.

Assets have varying levels of criticality and are usually associated with vulnerabilities. In particular, misconfigurations or lapses in controls can introduce vulnerabilities, and they can be subject to exploitation by a malicious actor. A malicious actor possesses a different set of skills and goals with which to compromise an asset. A malicious actor's activities could result in a threat. A threat entails different characteristics and is categorised according to type and severity. Moreover, the manifestation of a threat could result in a risk such as the interruption of critical functions that would lead to a cyber incident and subsequently have a variety of impacts on one or more assets. Fundamentally, a prioritised set of control mechanisms in the form of procedures or technical safeguards is typically implemented in order to address vulnerabilities and threats, prevent risks, and ultimately mitigate the impact of cyber incidents on the critical infrastructure. Control mechanisms are implemented according to the detective, preventive and corrective mechanisms for various purposes, such as detecting threats, minimising the potential impact of a threat, and restoring cyber assets to a prior state, respectively. In addition, the evidence is generated and collected by security mechanisms containing information about threat patterns and cyber incidents. The evidence collected can be aggregated and analysed with the purpose of detecting patterns and trends, along with responding to cyber incidents. The occurrence of a cyber incident triggers the process for incident handling, which has the goal of mitigating the impact of a cyber incident, and of eradicating the root cause of a cyber incident. Cyber course of action expresses the measures required in order to address and respond to an impending incident by utilising the procedural course of action and technical courses of action and is initialised by an actor such as IRT. The cyber course of action also improves the existing control mechanism and an overall security posture of critical infrastructure.

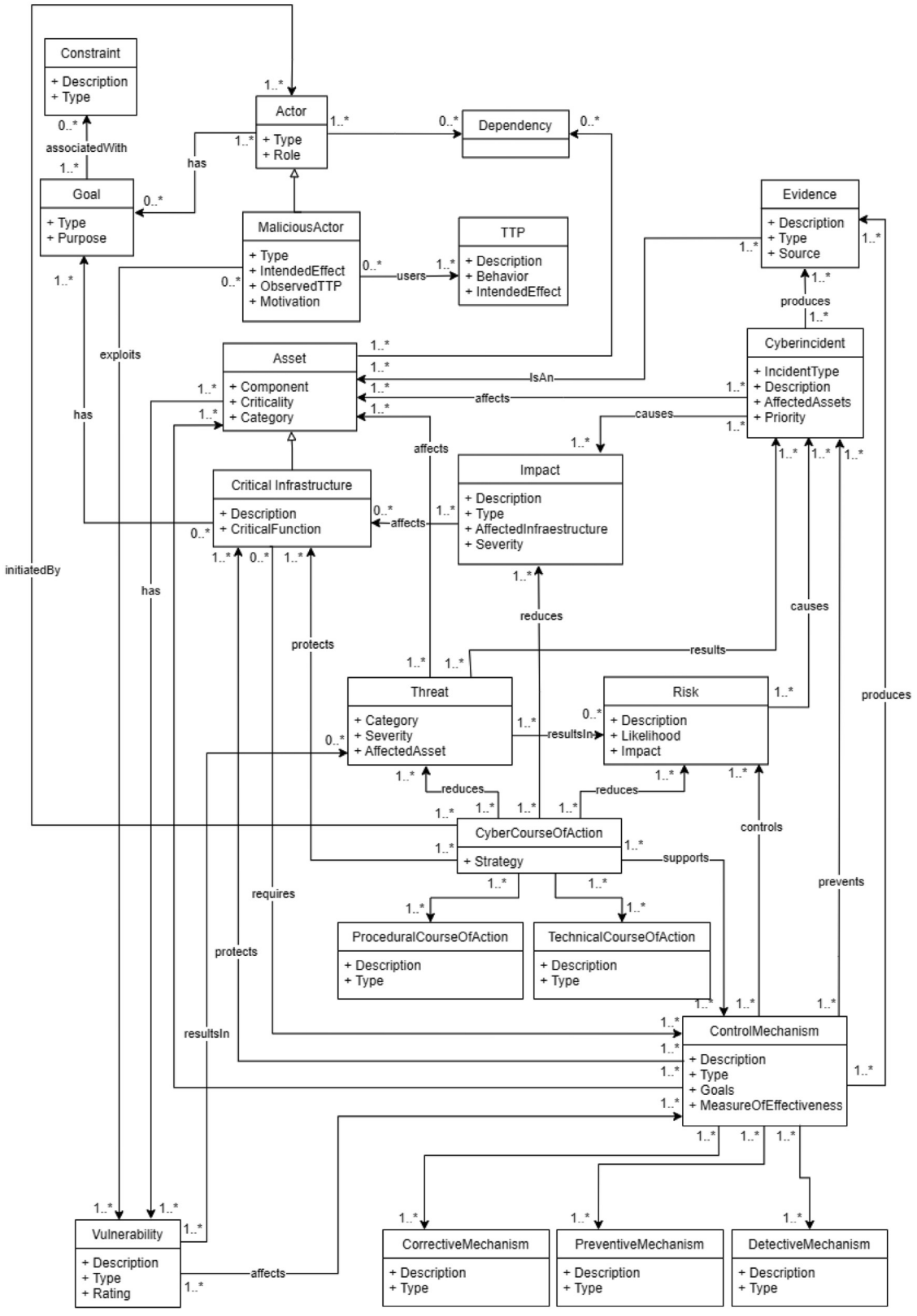


Fig. 1. Conceptual Model for Cyber Incident Response Modelling.

3.3.1. Modelling views

It is worth mentioning that a distinctive facet of CIHML is that it embraces the notion of decomposing the conceptual model according to three key sub-models/views, namely CII *analysis, threat and risk analysis, and incident response view*. The goal of this decomposition is to enable the creation of a graphical view of the different phases of incident handling in CII. The decomposition will enhance the developers' understanding of the main elements of the meta-model, mostly because it becomes more expressive in order to improve knowledge and facilitate the full im-

Table 2
CII Analysis View.

MODEL 1: Analysis Of CII	
Motive: The basis of this model is to provide a graphic representation of the CII with regard to its boundary. The model will enhance the developer's awareness and understanding of the connection between the CII and assets, critical functions being supported, and the consideration of the human elements that influence the operations of CII.	
Key Concepts	Description
CII	It will facilitate the understanding and identification of the critical infrastructure and its associated functions. The goal is to ensure that the CII is modelled according to the predetermined services or functions
Asset	The ICT systems that are essential for the operation of the CII are modelled according to criticality level or support for CII functions.
Goal	Actor goals are included in the modelling in order to analyse and reason about privacy and security requirements from the CII point of view, as well as actors' interest from incident response viewpoint.
CII	The model includes the CII, which contains a set of assets that could be exploited by a Malicious Actor, and which are affected by the impact of a Cyber Incident.
Constraint	The security and privacy constraints imposed that must be met for the satisfaction of security and privacy goals are also modelled.
Actor	The model will aim to identify the different actors involved or who have a strategic interest in the CII (such as owners, users, operators, and regulators)
Perceived Result: The main result is to provide an awareness of the CII in an organisational context and identify and assess potential vulnerabilities, threats, and risks that could lead to a cyber-incident, along with incident response activities.	

Table 3
Threat and risk Analysis View.

MODEL 2: Threat and Risk Analysis	
Motive: The model provides a general representation of potential threats, vulnerabilities and risks that could lead to a cyber-incident, including the analysis of the potential impact on assets.	
Key Concepts	Description
Vulnerabilities	The underlying and emerging vulnerabilities associated with assets are included in the model
Threat	Provides a clear articulation and granular characterisation of prevailing cyber threats
Risk	Potential Risk is identified by modelling the threat scenarios within the context of relevant vulnerabilities.
CII	The model includes the CII, which contains a set of assets that could be exploited by a Malicious Actor, and which are affected by the impact of a Cyber Incident.
Threat Actor	Captures the different threat actor types that could compromise assets, including characteristics such as the commonly used tactics, techniques and procedures.
ControlMechanisms	The existing control mechanisms that perform certain functionalities such as removing, identifying, or mitigating a cyber-incident are also included in the model—the inclusion of control mechanisms in the model assists as regards determining the controls that are in place.
Perceived Result: The result shows a threat and risk analysis report, including a list of threats, threat intelligence information, and controls.	

plementation of the concepts and their relationships. Tables 2–4, therefore, provide a summary of the different views, the motives behind creating the views, the concepts that can be utilized to create the views, and the perceived outcome of each view.

3.4. CIHML process

As mentioned earlier, CIHML comprises a process whose objective is to serve as a guide with which to analyse, specify and graphically model incident handling processes in CIIs. The process consists of three different sequential sets of activities, as shown in Fig. 2, that are tailored according to the three modelling views presented in the previous section. When formulating the process, we used various guidelines, standards and best practices relating to multiple domains, such as ISO 27,000 (Humphreys, 2016), ENISA guidelines (Mattioli and Levy-Bencheton, 2014), NIST (Cichonski et al., 2012), and OWASP (2014). These standards have been widely adopted in different CII sectors, and their integration within the process provides numerous benefits. Standards mostly involve inputs from a wide range of domain experts and primarily ensure conformity to requirements, assessment criteria and methodologies, and usually reflect recommended practices (Viegas and Kuyucu, 2022).

3.4.1. Activity 1: analysis of CII

The objective of this activity is to identify and analyse CIIs, along with operational context. The identification of operational context that influences an organisation's services and functions is key aspect as regards a successful incident response process. In this respect, the analysis of CIIs involves the modelling of critical infrastructure from an organisational and operational perspective in order to establish a clear awareness of the current factors that may influence an organisation. The goal is to present the CII sector, functions and assets that are used to manage, control, and support the provisioning of critical services. The concepts that support the creation of a modelling view in this activity include Critical information infrastructure, Asset, Goal, Constraint and Actor. An actor such as a developer or security analyst with significant familiarity with and knowledge of an organisation' operational context could, therefore, initiate this activity according to the critical service-dependent approach proposed by ENISA (Mattioli and Levy-Bencheton, 2014).

The identification of critical services as a critical task consists of two different techniques, namely state-driven and operator-driven. In the state-driven approach, the process used to identify CIIs is guided by governmental agencies that have the mandate to identify and protect CIIs, and it is more relevant for scenarios in which governmental agencies are involved in the process of identifying CIIs in a generic context. The operator-driven approach is, however, more specific, and the leading role of identifying CIIs is, therefore, assigned to the operators or asset owners of CIIs within an organisation. It is more context-specific and more suited to supporting the stakeholders within an organisation who are knowledgeable about their infrastructure and the critical sector within which an organisation operates. The developer may, therefore, consider adopting the operator-driven approach in this activity because actors such as owners or operators of CIIs are more involved in the

Table 4
Incident Response View.

MODEL 1: Analysis Of CII	
Motive: aims to capture incident response strategies that can be used to identify cyber-incidents, contain and minimize the impact, and recover from cyber-incidents. It will enhance the understanding of relevant response strategies that are suited to an organisation in order to effectively and efficiently contain or mitigate the impact of potential threats, vulnerabilities, risks and cyber-incidents.	
Key Concepts	Description
Cyber Course of Action (CCoA)	The model represents a combination of operational and technological processes that are used to respond to, protect and recover from cyber-incidents. CCoA consists of such strategies as Procedural and Technical CCoA. Procedural CCoA models cyber-incident handling strategies by human elements (including security awareness and management oversight), policies and plan, and regulatory compliance. Technical CCoA comprises those actions that enable the orchestration and automation of incident response mechanisms with which to ensure that the desired security and privacy posture of the CII is maintained during an incident. Technical CCoA is categorised according to key elements, such as protection actions and recovery actions.
Assets	The CCoA is comprehensively mapped onto each Asset in order to highlight and correlate the CCoA strategies (procedural or technical strategy) that are most suitable for or applicable to the security and privacy contexts of a CII as far as handling the incident is concerned
Impact	The efficiency and scope of CCoA strategies are included in the model to highlight the extent to which the specific impacts of a cyber-incident that can be mitigated.
CII	The model includes the CII, which contains a set of assets that could be exploited by a Malicious Actor, and which are affected by the impact of a Cyber Incident.
Actor	Similarly, actors (such as IRT) are included in this model in order to identify the role that each Actor plays in the direction, implementation and achievement of the different CCoA strategies.
Control Mechanism	The existing control mechanisms that perform certain functionalities such as removing, identifying, or mitigating cyber-incident are modelled.
Perceived Result: Specification of the relevant incident handling strategies that are applicable to a given context of cyber-incident within the CII, including the actors involved in the initialisation and maintenance of the incident handling process.	

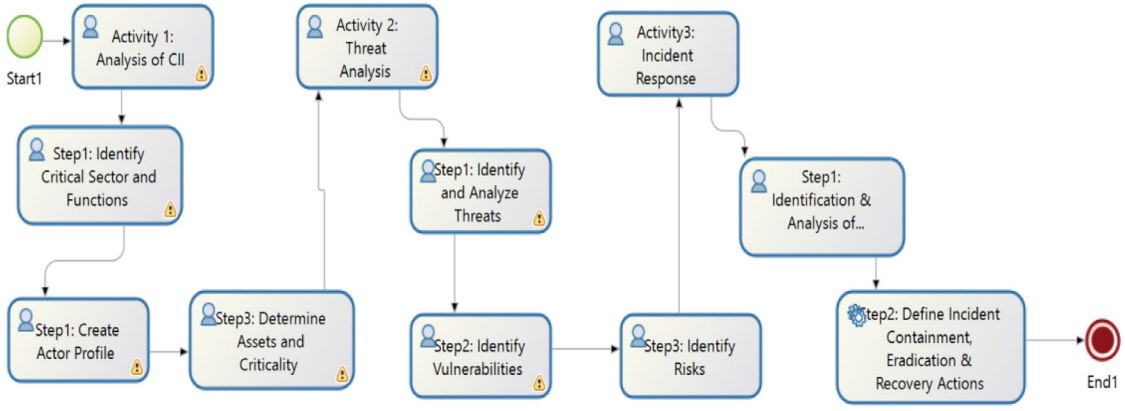


Fig. 2. CIHML Process.

process. The activity includes three tasks, which are explained below. The SPEM 2.0 diagram defining the basic pattern of inputs, tasks and outputs of this activity is shown in Fig. 3.

Task 1.1: identify critical sector and functions. This task enables the representation of a critical sector pertinent to an organisation based on the Critical information infrastructure concept. An organisation that provides critical functions is represented as a CII within a defined boundary. Essentially, the output of this task provides an overview and understanding of critical information infrastructure and the critical functions whose interruption could lead to severe damage or consequences. The critical infrastructure extends across many sectors, such as healthcare, transport, energy, etc. A sufficient identification of a critical sector that applies to an organisation's operational setting and the critical functions being provided are fundamental points for the analysis of a CII activity. This implies the understanding of the critical sector in which the organisation operates in order to clear the path for the performance of subsequent activities.

One viable technique that can be used to identify a critical sector and functions is that of exploring strategic and operational objectives in order to understand the critical sector that is relevant for an organisation. It can be supported by following the guidance provided by the European Programme for Critical information infrastructure Protection framework (EPCIP) (EPCIP, 2008). EPCIP identified a total of 10 sectors that are defined on the basis of various impact assessments and studies carried out by stakeholders. A diverse range of critical functions is provided in order to relate these critical sectors and the critical functions they support. In addition, ENISA (Mattioli and Levy-Bencheton, 2014) has provided an indicative list of critical sectors, associated sub-sectors and services that could be consulted by developers. This classification provides a channel that could guide the modelling of critical sectors and functions. Another important source to consider is the ENISA report entitled "Baseline Security Recommendations for the Internet of Things in the context of critical information infrastructures" (Sklyar and Kharchenko, 2019). IoT and CPS devices are becoming incresingly key elements of CIIs, and the majority of CPS-security related works are focusing on these critical infrastructures for any sector (Adepu et al., 2019). Rosado et al. (2022) have, therefore, developed a pattern called MARISMA-CPS that builds the scaffolding for the management of risk analysis processes that is specifically oriented towards CPS-based environments and is, owing to its nature, extensible to ICIs. This pattern contains catalogues of different types of key elements involved in the technical infrastructure of an SCP environment. We have taken the families and types of assets

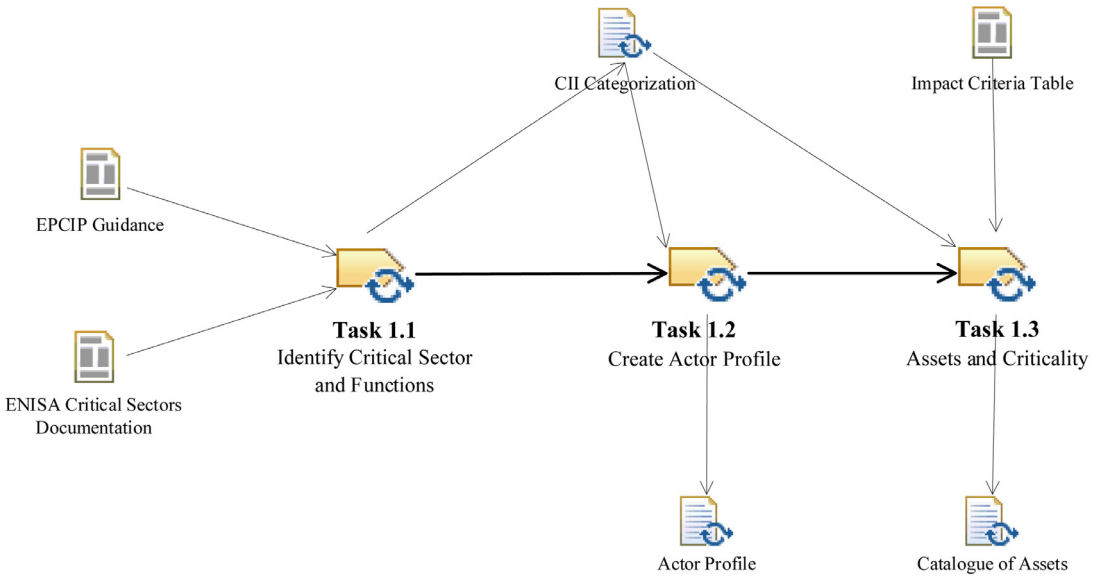


Fig. 3. SPEM 2.0 diagram of Activity 1: Analysis of CII.

Table 5
Families and types of assets for CIIs based on MARISMA-CPS pattern.

Family of Assets	Type of Assets
Devices	Hardware, software, actuators, and sensors.
Ecosystem Devices	Devices to interface with Things, devices to manage Things, and embedded systems.
Communications	Networks and protocols.
Infrastructure	Routers, gateways, power supply, and security.
Decision Making	Algorithms for data mining, and data processing and computing.
Applications & Services	Data analytics and visualisation, device and network management, and device usage.
Information/Data	Information stored in a database (at rest).
	Information sent or exchanged through the network (in transit).
	Information used by an application, service, or IoT element (in use).

defined by Rosado and that are, according to ENISA report, typical in CPS systems, and which are essential components for CIIs. Table 5, therefore, shows the different types of assets to be incorporated into our asset catalogue, based on MARISMA-CPS asset classification, grouped by family of assets.

These families of assets are the basis for CIIs because they cover all the elements of any given CII. For example, for a health environment such as a smart hospital, the relevant assets that form part of the asset family, such as information/data, may include patients' clinical results and medical files, along with their personal data. Other examples of assets could include laboratory information systems, hospital information systems, health monitoring devices, or even the hospital power system, etc. to name but a few. Similarly, an alternative way in which to identify critical functions is to consider which functions will result in significant adverse impacts such as loss or destruction or the interruption to function or data. These categories can be further expanded with respect to the requirements of the critical sector and the organisation's goals and objectives.

Task 1.2: create actor profile. This task creates the actor profile, including actors, roles, goals, and constraints. This task assists as regards attaining a better understanding of the specific role of actors and their intentions within an organisational setting. In summary, the task can be achieved by:

- Specifying Actor according to types (such as developers, users, operators, regulators), and strategic hierarchies within the organisation (such as managers, directors, providers), etc.
- Specifying the role of actors by presenting details of the associated influence, responsibilities, and participation in critical infrastructure operations.
- Associating actors with the goals they pursue, such as ensuring the security and privacy of data.
- Specifying security and privacy constraint. Constraints can be determined by identifying essentially relevant non-functional requirements (with emphasis on security and privacy), such as data encryption and authentication.

Task 1.3: – determine assets and criticality. It is crucial to determine the criticality of assets that are essential to sustaining critical functions (such as networks and systems). The aim is to support the analysis and modelling of assets according to a specific category, including asset components and criticality level.

The first step in this task is, therefore, to identify and categorise assets according to a classification scheme. Assets can be categorised according to different types of identification elements, such as literal identifies, relationship identifiers, synthetic identifiers, and extension identifiers (Wunder et al., 2011). Each identification element considers the different type of information. For instance, the relationship identifiers are used when assets are to be identified on the basis of their relationship with another asset. The next step in this task is to determine asset criticality. We advocate the use of an existing asset criticality rating specific to an organisation or based on the impact ratings proposed in this paper.

With regard to the Asset Criticality Rating, different impact factors can be used to determine criticality, such as: (a) service impact - the impact on the loss or degradation of a critical function, (b) population affected - the percentage of the population affected by the disruption of critical functions, and (c) economic impact – the financial cost of service disruption (Theoharidou et al., 2009). The critical information infrastructure owners will decide which criteria to use on the basis of compliance with several requirements. The service impact criteria have, therefore, been employed in order to provide a table of indicative impact criteria that will serve as a reference with which to determine asset criticality. This is done in conjunction with potential levels of impact provided by the FIPS impact rating, as shown in Table 6 (EPCIP, 2008).

Table 6
The impact on loss of services owing to the failure or malfunction of an asset.

Potential Impact	Definition	Impact Rating
Low	The loss of or damage to an asset is expected to have a limited adverse effect that: (i) causes degradation to the extent that critical functions are provided but the effectiveness of the functions is noticeably reduced; (ii) results in a minor disruption to other assets, or (iii) results in a minor financial loss.	1
Medium	The loss or damage of an asset will; (i) cause the significant degradation of critical functions to the extent that a critical function will be provided, but effectiveness is significantly reduced (ii) result in significant damage to other assets and components, or (iii) result in a significant financial loss	2
High	The potential loss or damage of an asset will: (i) cause the severe degradation to the extent that critical functions cannot be provided; (ii) result in severe damage to or the loss of other assets, or (iii) result in a major financial loss.	3

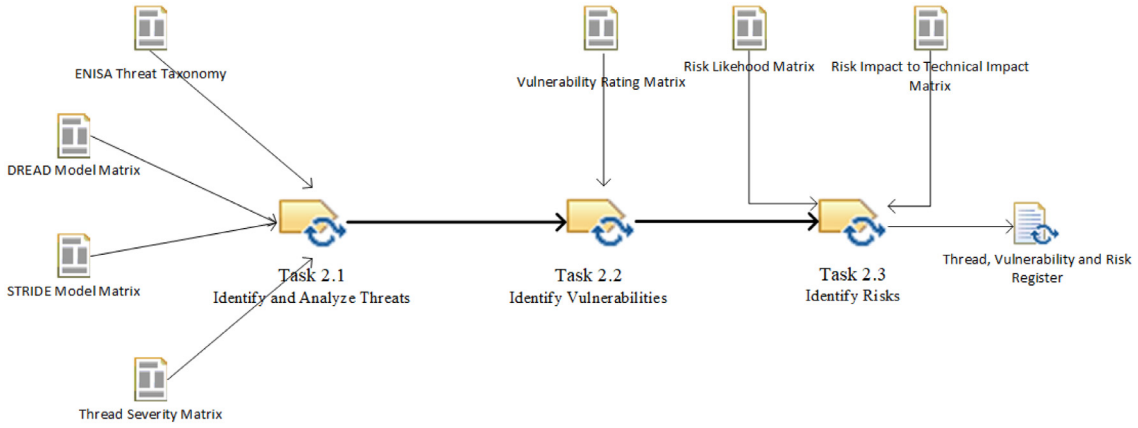


Fig. 4. SPEM 2.0 diagram of Activity 2: Threat Analysis Model.

3.4.2. Activity 2– threat analysis model

Upon completing the CII analysis, it is necessary to understand the risk and threat landscape. This activity, therefore, comprises techniques with which to identify and assess vulnerabilities, threats and risks that could result in a cyber incident that could potentially impact on the CII. The activity requires a structured representation of threat information that expresses valuable situational and contextual threats that are specific to the organisation. We advocate the use of two different methods, i.e. a threat classification approach and a cyber incident operationalisation approach for this activity. On the one hand, the threat classification approach focuses on the analysis of the commonly listed threats and vulnerabilities found in threat taxonomies, classification, and information sources (such as ENISA Threats taxonomy) that are likely to affect CIIs. This approach is broad-ranging, and involves the identification, review, and assessment of an extensive list of potential threats, and the likely impact they will have on CII. However, as threats vary over time and the techniques used by cybercriminals continue to evolve, this could be resource consuming and difficult for use by non-security experts.

On the other hand, cyber incident operationalisation is more specific to the assessment of specific threats, vulnerabilities and risks that have materialized and resulted in a cyber incident from a holistic viewpoint of the Threat Actor. It focuses mainly on the cyber incidents that are caused by a threat actor in order to systematically explore, characterise and determine the strategies that could be used to operationalise the incident. However, one limitation of this approach is that it potentially overlooks a vast pool of threat information that developers can use to understand and analyse emerging cyber threats. Both approaches are suitable as regards assisting developers to attain a better understanding and assessment of a cyber incident in detail. This activity, therefore, consists of the following tasks. The SPEM 2.0 diagram defining the basic pattern of inputs, tasks and outputs of this activity is shown in Fig. 4.

Task 2.1 – identify and analyse threats. This is the first task in this activity that deals with the identification of potential threats, vulnerabilities, and risks. In other words, the assets identified in the previous task are used as the basis on which to profile all possible threats that could negatively impact on the assets. It requires a sound approach that enables the gathering of valuable insights based on the analysis of situational and contextual threats that are more specific to an organisation's threat landscape. The use of the threat classification approach therefore makes it possible to leverage threat taxonomies and models in order to identify potential threats that may compromise assets, including exploitable vulnerabilities, which will improve the developers' ability to understand the nature of threats in a more structured manner.

This task is accordingly enabled by the Threat concept. At this juncture, the first attempt to identify threats is to consider information sources that provide a comprehensive list of threats. Many sources provide timely and relevant threat information, such as cyber threat intelligence platforms, tools and standards. In this context, ENISA published a Threat Taxonomy with the objective of assisting in the understanding of threats related to information and communication technology assets. The ENISA Threat Taxonomy can, therefore, be adopted as a reliable source of threat information. The ENISA Threat Taxonomy provides a comprehensive and well-structured taxonomy of threats that aims at improving the understanding of threats related to CII (ENISA, 2016)

Once the threat information source has been identified, the next task is to methodically analyse the threats in terms of classification and severity and create an association with the assets that are most affected by the threat. This analysis is enabled the Category and Severity attributes. It is imperative to perform this analysis according to standard methodologies. In this respect, threat evaluation models such as STRIDE Model (Microsoft, 2007) can be used. The STRIDE model is particularly utilised to categorise threats according to exploits such as Spoofing Identity, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of

Table 7
Threat Categorisation Matrix.

Category	Consideration
Spoofing (S)	Attackers masquerade as a legitimate user, system or application element
Tampering (T)	Attackers modify or tamper with assets in transit or in-store
Repudiation (R)	Attackers perform actions that cannot be traced
Information Disclosure (I)	Attackers disrupt or interrupt normal operations of the asset
Elevation (E)	Attackers obtain access privilege to an asset without legitimate authority.

Table 8
DREAD Model.

Category	Question
Damage Potential (D)	How extensive is the damage potential?
Reproducibility (R)	How easy it is for the threat to be repeated or reoccur?
Exploitability (E)	How easy is it to launch the treat?
Affected Users (A)	Approximately how many users will be affected?
Discoverability (D)	How easy is it to discover the vulnerabilities?

Privilege. In addition, Microsoft's DREAD model (Meier, 2003), provides a framework with which to rate, compare, and prioritise the severity of various threats by rating them on an ordinal scale. The model consists of five main categories: Damage, Reproducibility, Exploitability, Affected user, and Discoverability. These two models can be utilised to categorise and determine the severity of threats.

The use of the ENISA Threat Taxonomy in conjunction with the STRIDE and DREAD models therefore makes it possible to create a threat analysis matrix reflecting the severity and category of potential threats. In particular, the threats listed in sources such as the ENISA taxonomy can be modelled according to exploits in order to represent the threat actor's intention according to STRIDE (as shown in Table 7). Moreover, threats can be rated by following the customised and accompanying questions shown in Tables 8 and 9.

The above scales can be used to rate and determine the severity of each threat according to the DREAD model. The questions can also be modified or extended accordingly. A rating table is used with corresponding values of 3, 2 and 1 to represent (3) high, (2) medium and (1) and low, respectively. The outcome can fall within the scope of 5 to 15 to denote threat severity from low to high. The threats with an overall rating of 12–15 can be treated as having 'High Severity', 8–11 as 'Medium Severity', and 5–7 as 'Low Severity', as shown in Table 10.

Task 2.2 – identify vulnerabilities. The second task involves the identification of vulnerabilities that can be exploited by the threat. The identification and modelling of vulnerabilities are supported by the Vulnerability concept, whereby the different types of vulnerabilities associated with assets are identified using the Type attribute. At this point, the developer must explore databases to identify vulnerabilities efficiently. CIHML uses the National Vulnerability Database (NVD), (Booth et al., 2013) and Common Vulnerabilities and Exposures (Common Vulnerabilities and Exposures CVE., 2023) as sources of vulnerability information. The vulnerabilities identified need to be rated according to their severity, which is enabled by the Rating attribute. A vulnerability severity rating system can be used for reasons of consistency. The security severity rating helps developers to determine how best to approach a vulnerability based on the CVSS (NIST, 2022) rating, which consists of a formula made up of three main metric groups: base, temporal and environmental. The Base metric assesses the severity of a vulnerability on the basis of its intrinsic characteristics, which are mostly constant over time. The Temporal Metrics is based on factors that change over time, such as the availability of exploit code (Cichonski et al., 2012). Environmental metrics consider factors such as the presence of mitigations in the cyber environment. The rating system also consists of a numerical score that produces a score ranging from 0 to 10, which can be mapped onto qualitative ratings, as shown in Table 11. Once vulnerabilities have been identified and assigned a severity score, an association is created in the model between the potential threats that could exploit the vulnerability, along with the assets associated with the vulnerability

Task 2.3 – identify risks. The goal of this task is to identify and assess the potential outcomes of a successful threat to a cyber asset, such as the possibilities of the destruction of, modification of, or interruptions to assets or critical functions. This can be instantiated by using the Risk concept of the meta-model. Moreover, there are many approaches with which to perform risk analysis that can be utilised for this purpose. The developer needs to define an approach that makes the identification and accurate estimation of risks possible. This will help to ensure that major or prioritised risks are not overlooked. The key factors that are considered in order to estimate risk likelihood include threat agent and vulnerability factors, while others used to estimate risk impact include technical and business impact factors. The threat factors employed in order to estimate risk likelihood involve assigning a set of options to each factor, and each option contains an associated likelihood rating from 0 to 9 (as shown in Table 12).

Technical impact factors are similarly used to determine the impact of risks. Each factor is assigned a set of options, and each option is associated with an impact rating from 0 to 9, (as shown in Table 13). The developer can, therefore, determine the severity of risks for assets and business functions, in addition to ensuring that priority is given to more severe risks. This activity produces a summary of threat, vulnerability and risk register within the CII context, as shown in Tables 14 and 15.

3.4.3. Activity 3– incident response

This is the last activity that involves the specification and representation of incident response activities. The objective of this activity is to capture incident response strategies on the basis of threats and vulnerabilities and to improve the understanding and analysis of incident response strategies in terms of containment and eradication actions. The output is, therefore, the modelling of incident response activities according to the specific needs of critical infrastructure. The activity is, therefore, decomposed into multiple parts in order to enable the creation of different views or sub-models, as described in the following section. The SPEM 2.0 diagram defining the basic pattern of inputs, tasks and outputs of this activity is shown in Fig. 5.

Task 3.1 – identification and analysis of incidents. This task provides a meticulous analysis of one or multiple incidents. The analysis considers attributes such as the severity and priority of incidents. Primarily, the task consists of two steps, namely cyber incident detection and analysis, which pave the way for the subsequent task for containment, eradication, and recovery.

In the case of Incident detection, this phase entails the application of different techniques and tools with which to detect cyber incidents. A developer must collect and log security event data for the detection of incidents and the support of incident analysis using the Evidence and Incident Type attribute of CyberIncident concepts. The Evidence concept enables the various automated detection capabilities that are used to identify a cyber incident to be identified. Incidents can, therefore, be detected by various means, with varying levels of detail. Automated detection capabilities such

Table 9
Threat Rating Matrix.

Category	3 (High)	2 (Medium)	1 (Low)
Damage Potential (D)	Complete system or data destruction, and unavailability of assets and critical functions	Compromises or impacts on a subset of assets and critical functions	Minor: an impact on a small number of assets and critical functions
Reproducibility (R)	A threat could be reproduced to compromise assets and critical functions	The threat can be reproduced, but only by an authorised user	It is improbable that the threat will be replicated.
Exploitability (E)	A novice threat actor can easily compromise assets and bring down critical function.	Attack tools freely available, or an exploit is easily performed using novice tools	Advanced programming and in-depth knowledge, with custom or advanced tools
Affected Users (A)	All users	Some users but not all	None
Discoverability (D)	Vulnerabilities in the asset are very noticeable and can be easily exploited	Weaknesses in the assets are rarely discovered.	Vulnerabilities are hardly present and rarely discovered.

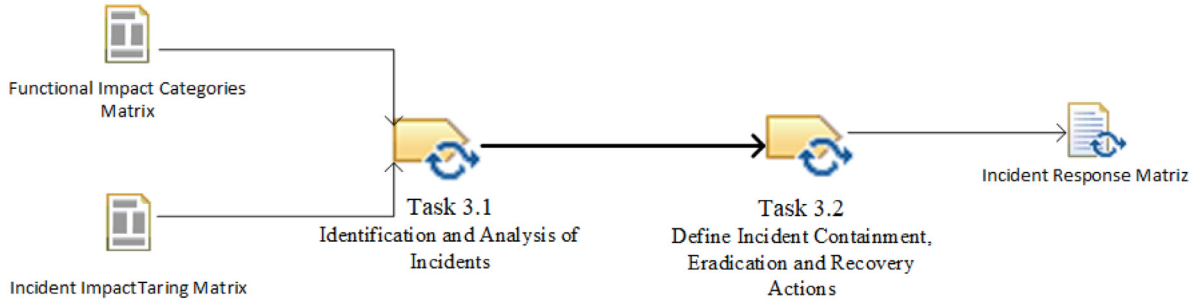


Fig. 5. SPEM 2.0 diagram of Activity 3: Incident Response.

Table 10
Threat Severity Matrix.

Values	Rating
12 to 15	High
8 to 11	Medium
5 to 7	Low

Table 11
Vulnerability Rating.

Rating	Score
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

as log management tools, antivirus software, intrusion detection systems, intrusion detection systems, and vulnerability scan data can be used to detect incidents. Incidents may also be detected by manual means such as user reports, especially because some incidents can be easily detected manually, whereas others can go undetected without automated processes.

Furthermore, in the case of Incident analysis, the analysis focuses on evaluating an incident in order to determine its scope, the methods used, and the vulnerabilities exploited. It is necessary to review the collected evidence and attack vectors that the threat action is using in order to exploit the vulnerability, The task is, therefore, enabled using concepts and attributes of the modelling language such as Priority, AffectedAssets Impact, Threat, Vulnerabilities, Risks, and Control Mechanism. Some incidents are relatively more important and require a more urgent response than others. A developer should, therefore, assign an incident priority scheme based on its impact and urgency for resolution. This "Priority" attribute enables a developer to determine incident priority according to a prioritization matrix. The attribute "AffectedAssets" is used to identify the assets that have been affected by a cyber incident by creating an association between the cyber incident and the assets perceived to be affected.

The consequences of an incident for assets are similarly quantified using the Impact concept and on the basis of the qualitative or quantitative value. The Control Mechanism concept enables the developer to represent the existing control actions, processes and mechanisms being used to prevent or mitigate potential incidents, which are categorised according to the Corrective Mechanism, Preventive Mechanism, and Detective Mechanism. Furthermore, it is worth noting that control mechanisms do not always provide the complete security and protection of assets as desired, and the attribute Measure of Effectiveness consequently enables the assessment of the effectiveness of existing control measures in terms of relevance and robustness to control mechanisms in order to ad-

Table 12
Risk Likelihood.

Threat Factor Factor	Description	0 to < 3 (Low)	3 to < 6 (Medium)	6 to 9 (High)
Ease of Discovery	How easy is it for this group of threat agents to discover this vulnerability?	Practically impossible	Difficult	Substantially easy
Ease of Exploit	How easy is it for this group of threat agents to exploit this vulnerability?	Theoretical	Difficult	Substantially easy
Awareness	How well known is this vulnerability to this group of threat agents?	Unknown	Obvious	Public knowledge
Intrusion Detection	How likely is it that an exploit will be detected?	Active detection mechanisms	Logged & reviewed	Not reviewed

Table 13
Risk Impact to Technical Impact.

Technical Impact						
Factor	**Question to ask**	**2**	**4**	**6**	**7**	**9**
Loss of Confidentiality (C)	How much data could be disclosed and how sensitive is it?	Minimal non-sensitive data disclosed	Minimal critical data disclosed	Extensive non-sensitive data disclosed	Extensive critical data disclosed	All data disclosed
Loss of Integrity (I)	How much data could be corrupted and how damaged is it?	Minimal slightly corrupt data	Minimal seriously corrupt data	Extensive slightly corrupt data	Extensive seriously corrupt data	Extensive seriously corrupt data
Loss of Availability (A)	How much service could be lost, and how vital is it?	Minimal primary services interrupted	Extensive secondary services interrupted	Extensive primary services interrupted	Extensive primary services interrupted	All services completely lost
Loss of Accountability (AC)	Are the threat agents' actions traceable to an individual?	All services completely lost	Possibly traceable	Possibly traceable	Possibly traceable	Completely anonymous

Table 14
Threat, Vulnerability and Risk Register.

Threat Type	**Threat Category**						**Target Assets**	**Threat Severity**					**Severity**
	S	*T*	*R*	*I*	*D*	*E*		*D*	*R*	*E*	*A*	*D*	

Table 15
Threat, Vulnerability and Risk Register.

Vulnerability Type	**CVE Reference**	**Rating**	**Risk**	**Technical Impact of Risk**

dress the cyber incident. These considerations will, therefore, provide the developer with sufficient insight with which to assess the subsequent containment and mitigation strategies according to the order based on which cyber incidents should be handled.

It is vital to use an incident prioritisation matrix to determine incident priority. Cyber incident prioritisation can be performed according to three criteria: (a) functional impact of the incident (such as current and likely future negative impact on critical functions), (b) information impact of the incident (such as the confidentiality, integrity and availability of assets), and (c) recoverability from the incident (such as time and types of resources that are required in order to recover from the incident) NIST (Cichonski et al., 2012). The purpose of this prioritisation is based on the presumption that highly rated incidents must be handled and resolved before low rated incidents. Although the developer can best decide an appropriate criterion, the functional impact criteria are more suitable as regards prioritising incidents according to negative impacts on critical functions, and this is consequently considered in this process and presented in Table 16.

Furthermore, as mentioned earlier, the impact or magnitude of harm resulting from a cyber incident is estimated using the Impact concept. The Severity attribute of the concept is specifically used to determine an impact in terms of loss, failure or damage that could result in an adverse effect on critical functions or assets. A matrix with which to determine the impact on organisational assets and functions can be used. The assessment scales shown in the impact matrix can be tailored according to organisation-specific conditions, as shown in Table 17:

Moreover, the effectiveness of control can be determined by using standard quality metrics for each of the control categories. ISO/IEC 27004:2016-12-15 provides guidelines that are intended to assist organisations in evaluating the information security performance and the effectiveness of the ISMS" (ISO/IEC_27004:2016, 2016). The guideline identifies a measurement method and four groups of controls that can be measured: (a) management controls such as security policy, security procedures, business continuity plans; (b) business processes such as risk assessment and risk management process; (c) operational controls such as operational procedures, change control, problem management, back up, and secure disposal, and (d) technical controls such as patch management, antivirus controls, IDS, firewall and content filtering. Ultimately, this ISO guideline can be used to assess the effectiveness of controls using the attribute Measure of Effectiveness.

Task 3.2 – define incident containment, eradication and recovery actions. The goal of progressing through the preceding task is to define actions that will contain and eradicate an incident. In other words, it is crucial to implement strategies with which to contain and remove incidents in order to avoid incidents of overwhelming assets. This task, therefore, focuses on the analysis of appropriate and implementable incident response strategies with which to address cyber incidents. The goal is to enable a developer to create an independent model that captures the essential strategies required in order to contain and reduce the potential impacts of an incident, along with the strategies for the actual restoration of affected assets. As occurs with the previous models, the modelling activity in this task uses concepts from the incident handling modelling language, along with the integration of various techniques and practices in order to support the modelling activity.

The central concept that enables modelling at this level is fundamentally the CyberCourseOfAction, which entails a combination of processes or measures with which to respond to or mitigate the potential impacts of predefined or anticipated cyber incidents. As the control actions for incident containment and eradication may vary according to incident types, strategies for a cyber course of actions consider these variations in order to enable the implementation of different strategies for each significant incident type. Cyber course of action strategies can, therefore, be implemented from two perspectives, namely (i) a procedural course of actions dealing with control actions such as security policies and awareness and training, and (ii) a technical course of actions such as cryptography and access control. These two categories of cyber course of action are modelled according to *ProceduralCourseOfAction* and *TechnicalCourseOfAction* inherence.

When defining and modelling technical and procedural courses of actions, it is, therefore, essential to consider a set of standard

Table 16
Functional Impact Categories for Incident Prioritization.

Category	Rating	Definition
None	0	No effect on the ability to provide all users with critical functions.
Low	1	The minimal effect. All users can be provided with critical functions but with limited efficiency.
Medium	2	The inability to provide a subset of users with critical functions.
High	3	Complete incapacity to provide any users with critical functions.

Table 17
Incident Impact Rating.

Qualitative Values	Semi-Qualitative Values		Description
Very High	95–100	10	The impact of an incident is sweeping, affecting almost all of the assets and critical functions.
High	80–95	8	The impact of an incident is extensive, affecting most of the assets, including many critical functions.
Moderate	21–79	5	The impact of an incident is substantial, affecting a signification portion of assets, including some critical functions.
Low	5–20	2	The impact of an incident is limited in nature, affecting some assets but not involving any critical functions
Very low	0–4	0	The impact of an incident is minimal and negligible, involving a few if any assets and involving no critical functions.

Table 18
Incident Response Matrix.

Cyber Incident					Impact	Control Mechanism			CCoA	
Type	Affected Asset	Severity	Affected Assets	Incident Priority	Severity	Detective	Preventive	Corrective	Procedural	Technical

actions for cyber defence that provides actionable practices and mechanisms with which to contain, mitigate and eradicate most of the pervasive and dangerous cyber-attacks. We follow CIS CSC controls to determine the suitable controls. This activity produces an incident response register summarising all the information related to the CyberCourseOfAction, as shown in Table 18.

3.5. CyberSANE tool

In order to support the implementation and application of the CIHML Process, a tool called CyberSANE has been developed. It is a Cloud web application developed using HTML5 (HTML, CSS and JavaScript) and Node.js technologies, complemented with an API that, through a series of endpoints, allows the integration of the models and data generated in the web tool into other external systems in a manner that is easy and transparent for the operator. The tool can run through the use of a standard web browser and can be accessed at https://cybersane-4af7f.web.app/. It is necessary to create credentials prior to accessing the portal. The initial page, therefore, allows users with valid credentials to log in so as to carry out the activities provided in the dashboard.

The objective of the tool is to automate the incident handling process. It consists of two main interfaces, Critical Information Infrastructure (CII) and incident analysis, which are associated with the relevant functionality required to perform tasks. The main features include modelling, reporting, prioritisation and attack path Discovery, which are required for the CII and incident analyses. The CII analysis considers assets, goal, constraint, vulnerability, and actor based on the specific context. The modelling feature makes it possible to visually present all these entities using standard notations for the purpose of critical analysis. One of the key benefits of the tool is the prioritisation of the incident through the adaption of an incident heat map. The incident heat map, therefore, visually presents the incidents in different coloured segments on the basis of their priorities. This makes it possible to understand which incidents need immediate attention, thus allowing appropriate control actions to be taken into consideration in order to tackle the incident. The tool includes the reporting features required in order to produce a detailed incident based on the tasks performed in the incident identification and prioritisation activities.

CyberSANE tool allows the different models developed through the CIHML Process to be generated graphically and intuitively. The tool, therefore, allows the creation, customisation and adaptation of each model to the context of the infrastructure in which the process is being applied, defining each of its elements and connections related to the managed security incidents. In addition, the models generated can be used as a knowledge base to support the rapid and effective categorisation of future incidents. Fig. 6 shows an example of a CII Analysis Model created in CyberSANE. As stated previously, the CII analysis includes asset, goal, constraint, actor, vulnerability and specific CI sector, signifying that this information can be used to identify and analysis possible incidents.

Furthermore, the tool makes it possible to collect, compile and summarise all the information obtained from security incidents through the CIHML Process. It consequently provides the tasks of analysis, categorisation, prioritisation and decision-making with automated support for incident management and resolution. Fig. 7 shows an example of the incident prioritisation task implemented in CyberSANE, which includes the incident heat map in order to visually present and prioritise the incidents. This will support informed decision making in terms of a specific incident that requires immediate attention.

4. Implementation

We have implemented the proposed modelling language in a real industrial context. The goal of the implementation is to provide a detailed description of how the proposed model can be used to improve the understanding and representation of cyber incident handling activities. The study context is based on an energy company that specialises in solar energy production, storage and distribution services. In order to protect the confidentiality of our study context, we have used a fictitious name "ABZ" to refer to our case study. the objective of the implementation is, therefore, to: i) Demonstrate the applicability of the cyber incident modelling language to a real studied context; ii) Determine the suitability of modelling for the CII, and iii) Generalise our findings to existing works.

4.1. Study context

ABZ operates an integrated platform (SIDE/Smartly Integrated Distributed Energy platform), with several digital services on top

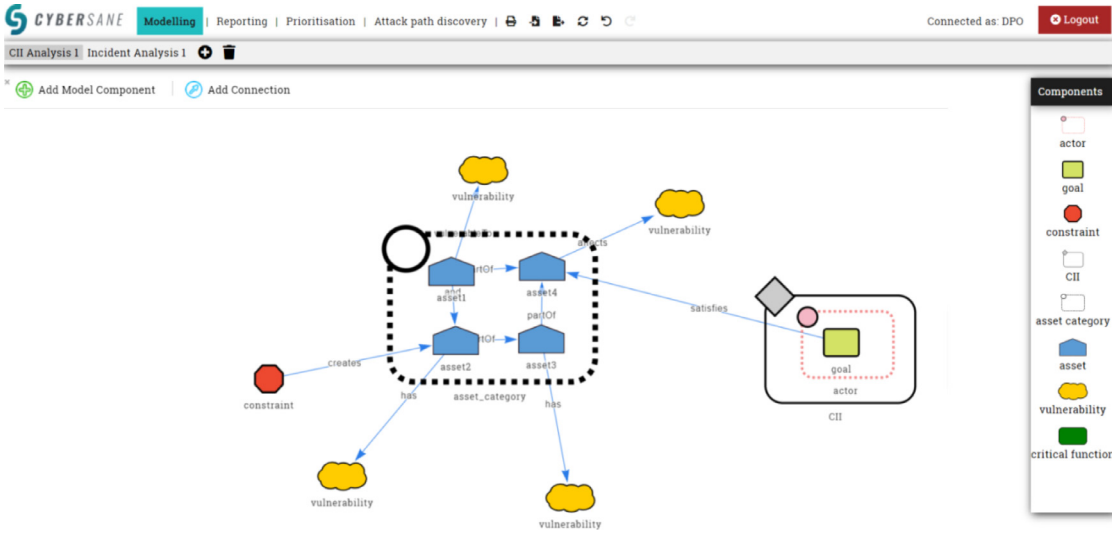


Fig. 6. Example of CII Analysis Model in CyberSANE tool.

Fig. 7. Example of incident prioritisation in CyberSANE tool.

that help energy "customers", utilities and grid operators to optimise power flows, secure the electricity grid and finally reduce the cost of electricity. The SIDE platform constitutes a smart software-hardware solution optimised for Grid 2 Home / Home 2 Grid optimisation of a distributed generation system. The platform incorporates a bundle of components such as:

- A range of web apps for the end-user (SIDE UIs) that enable users to see the power flow between the solar system, the battery and the grid of their households in real-time.
- The SIDE gateway, which is an intermediate device between sensors, smart meters, inverters, the battery and appliances and the SIDE Platform that creates value from data collection and control.
- The SIDE Virtual Power Plant (VPP), which is a cloud infrastructure and software platform that operates a smart grid network of a population of distributed assets that are securely interconnected via Side Gateway.
- The SIDE CRM, which is a bespoke back-office CRM application that automates the entire business process.
- The SIDE Panel, which is an electric panel specially designed to accelerate the installation process of the system and eliminate connectivity errors; and the SIDE IoT platform, which is our abstract software running framework.

Attacks on "Solar Energy Production, Storage and Distribution Service": Various combined cyber-attacks may affect the solar energy service examined. With regard to the cyber part, there may be attacks on the back-end SIDE Platform, such as gaining unauthenticated, remote access to IoT components and other components in order to disrupt services. Other cyber-attacks may target the IT and communication systems that are used to process the sensed data and transmit them to the corresponding IT systems.

4.2. Cyber incident

ABZ experienced a cybersecurity incident on multiple systems across their network. The in-house security team determined that a large-scale malware incident had occurred and had quickly spread across the network, affecting several CII assets, including customer information and system/process data. A detailed analysis

Table 19
Analysis of CII Table.

Critical Infrastructure		Asset		
Critical Sector	Critical Functions	Category	Type	Criticality
Electricity	Solar energy management services Production, distribution and transmission of solar energy	Communication Network	Customer Premises Network	2
			Distribution Grid Network	3
			Transmission Grid Network	3
		Systems	Distribution Management Systems	3
			Advanced Metering Infrastructure	2
			Supervisory Control and Data Acquisition	2
			Smartly Integrated Distributed Energy Platform	3
		Data	Personal/Private Data	2
			Process Data	2
			Metre configuration data	2
			Software/Hardware Data	1
		Security Controls	Security Information and Event Management (SIEM)	2
			Network Security and Monitoring Tools	1

of the actual nature and scale of the malware attack revealed the presence of a "Jigsaw Ransomware attack", which is a form of malicious code that infects systems and typically performs operations such as file encryption. The attack propagated and encrypted multiple hard disks containing processes, systems and customer data, rendering them inoperable and inaccessible to both users and customers. This resulted in the unavailability of the production, distribution, and transmission functions of solar energy. A ransom note was subsequently generated demanding payment in Bitcoins and threatening to delete encrypted files for every hour of non-payment of the ransom. In summary, the Jigsaw Ransomware incident resulted in solar energy management systems becoming completely unfunctional, thus incapacitating the distribution of energy to customers.

After realising that the situation existed, the company saw the need to have a holistic and integrated approach for the identification, assessment and recovery from the cyber incident. Furthermore, the decision-makers required a modelling approach that could improve the understanding and representation of the processes, threats and vulnerabilities while simultaneously facilitating incident resolution in an easy-to-use and easy-to-understand fashion.

4.3. Process implementation

In this section, we present a summary of the implementation process of CIHML. It is essential to mention that the implementation processes, details and artefacts are summarised in this paper owing to space limitations.

4.4. Activity 1 – identify critical sector and functions

The implementation activities were initiated in conjunction with a team of Security Analysts and IRT. Formal engagements and briefings concerning the implementation process were carried out in order to prevent any misunderstandings regarding the contextual aspects of our approach and to prevent premature conclusions. Inputs from multiple stakeholders were, therefore, used as the basis on which to develop the first step towards identifying the critical functions' peculiar to ABZ. In this direction, having analysed its context in terms of its strategic and operational objectives, ABZ's domain of operations falls under solar energy production, storage and distribution. The analysis yielded a detailed list of assets and their criticality, actors, security and privacy constraints, as shown in Tables 19 and 20, respectively. This activity also produces a CII analysis model that visually captures the critical functions, Actor, and constraints (Fig. 8).

4.4.1. Activity 2 – threat analysis model

This activity identifies and analyses the threat and generates the risk register on the basis of the incident pertinent to ABZ. We emphasized the identification, analysis and modelling of the potential threats that may lead to the exploitation, interruption or destruction of assets and critical functions negatively. This was achieved by exploring the ENISA Threat Taxonomy, which provides a tier-based classification and grouping of threats into various categories. The engagement and support of the Security Analysts, therefore, allowed us to perform an overall assessment that produced a complete overview of those threats and vulnerabilities that could result in the assets being compromised. Tables 21 and 22 present the main threats and vulnerabilities.

A threat analysis model (Fig. 9) was subsequently designed in order to graphically and accurately represent the possible severity of threats, a vulnerabilities rating, and the level of the impact associated with risks. The model provides the ability to articulate complex information and enhances awareness of threat landscape, in addition to enabling ABZ to clarify its threat assumptions. The model, therefore, represents ABZ within its boundary as a critical infrastructure consisting of multiple assets and potential threat actors – cybercriminals and the malicious insider. Each threat actor is mapped onto a specific threat, including the vulnerabilities that are typically exploited in order to compromise assets, and the resulting risk or consequences of threat actor activities. In this instance, a cybercriminal using a set of TTP, identifies missing authentication vulnerabilities existing in a decision support system that assists the operators to monitor, control, and optimise the performance of the electric distribution system, and security configuration vulnerabilities in communication networks. The cybercriminal launches an entire attack set that would include multiple threats and purposes. A malicious code is specifically injected that enables the threat actor to change the configuration of network communications and allows them to gain access to and modify sensitive data. The actions of the threat actor resulted in multiple forms of risks – unauthorised tampering and the disclosure of sensitive data and unavailability of service, which consequently affected the production, distribution, and transmission of solar energy.

The modelling of all the elements related to an incident, along with the relationships among them, therefore allows both the operators and the specific cyber security personnel involved to visually obtain an accurate overview of all the aspects related to the context of the cyber incident. The model thereby provides a better understanding and analysis of the existing vulnerabilities, the threats involved in the incident, the attack mechanisms and even the behaviour of the cyber attacker.

In addition, as a result of this activity, a qualitative assessment of the different factors that allow the contextualisation and an un-

Table 20
Actor Profile.

Actor Type	Role	Goals Type	Constraints Security	Privacy
Generation and distribution operators	The operating managers responsible for the optimisation of production, distribution and transmission of solar energy	Ensure efficient delivery of critical functions	Protection against cyber incidents that could cause blackouts, power overloads, device malfunction, and data tampering	Share/use private customer data and system data only when approved
Technology vendors	Provision of third-party software and hardware solutions such as SCADA Software	Provision of reliable cyber solutions to support workflow, production and distribution of solar energy	Integrity and availability of and hardware and software solutions	Complete compliance with GDPR rules for Data Privacy
End-user	Consumption/use of solar energy at domestic and industrial levels.	Consumption of stable, cost-effective and reliable solar energy	Secure access to energy services and monitoring and control	Proper notification regarding the purpose of use, processing and transfer of personal data
System Operator	Responsible for the configuration, supporting and maintaining cyber assets.	Maintain security procedures for assets and customer data security	Authorised access and use of assets	Share/use private data only when approved.

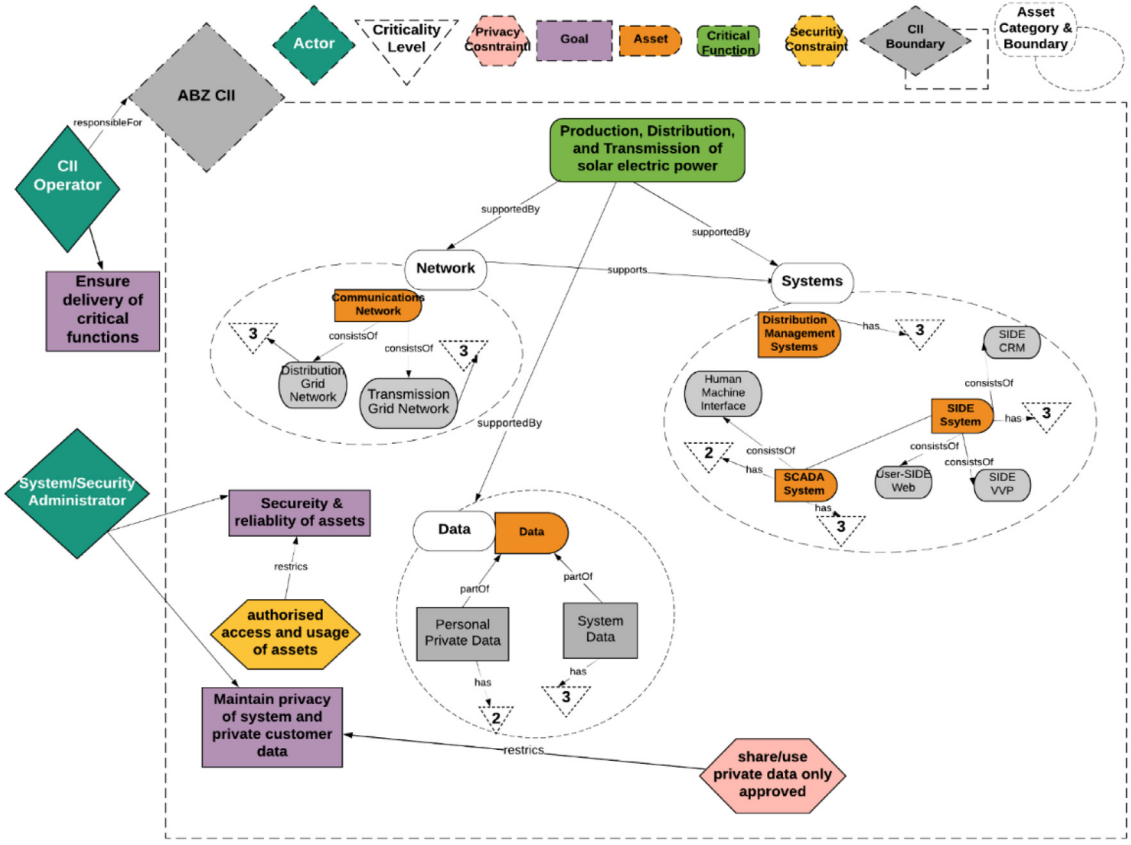


Fig. 8. Analysis of CII Model.

Table 21
Threat Analysis.

Threat Type	Threat Category						Target Assets	Threat Severity					Severity
	S	*T*	*R*	*I*	*D*	*E*		*D*	*R*	*E*	*A*	*D*	
Malicious Code	*			*		*	Overall Assets	3	2	3	3	3	High
Elevation of privilege	*	*					Overall Data	2	2	3	1	3	Medium
Data tampering		*		*			Private, Metre and Process Data	3	2	3	2	3	High

Table 22
Vulnerability Analysis.

Vulnerability			Risk	Risk Technical Impact			
Type	CVE Reference	Rating		C	I	A	AC
Elevation of privilege vulnerability	CVE-2018-8453	High	Unauthorized tampering and disclosure sensitive data.	7	7	9	6
File Disclosure vulnerability	CVE-2019-11510	Critical	Unavailability of essential functions and services	6	7	9	9

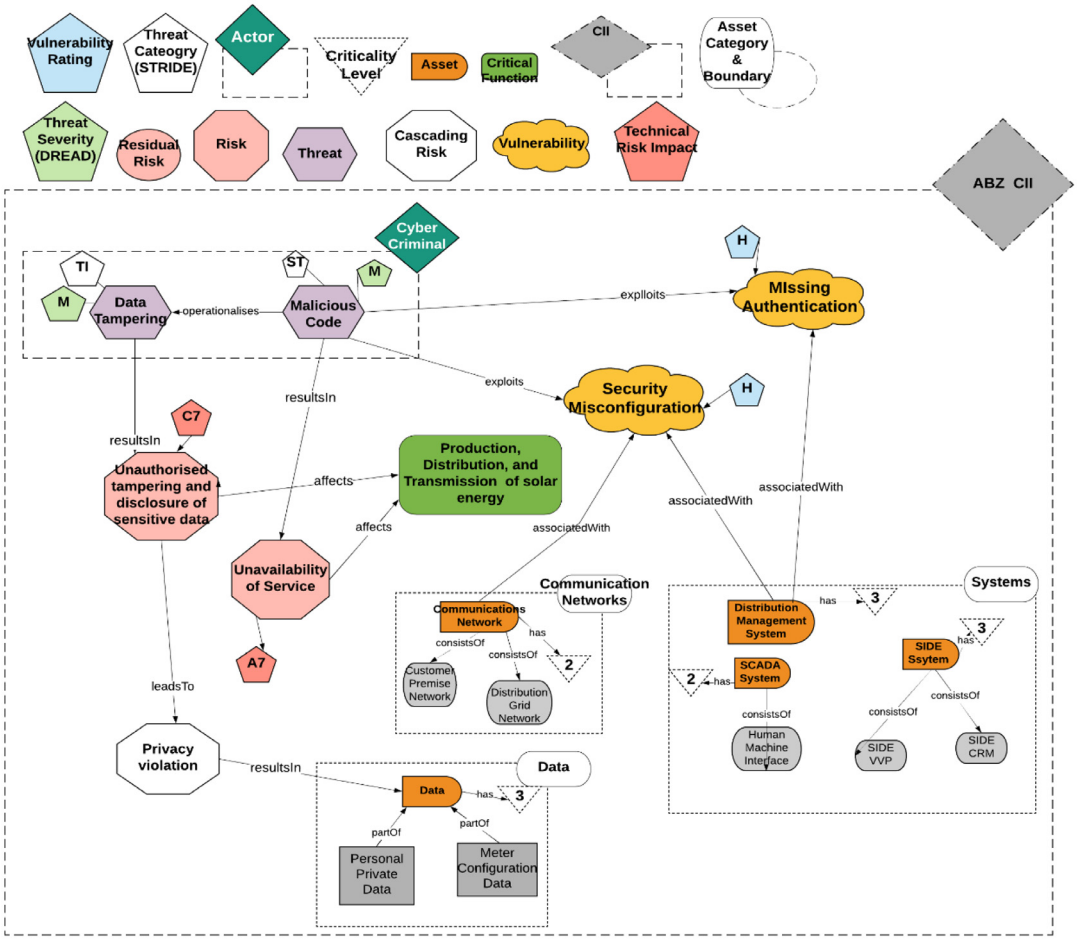


Fig. 9. Threat Analysis Model.

derstanding of the impact of the incident (categorisation and criticality of the threats involved in each incident, evaluation of the related vulnerabilities, assessment and potential impact of the inherent risks) is also generated. This information complements the incident knowledge base and provides initial guidance with which to facilitate an accurate understanding of the context, causes and effects of each event after modelling. The modelling language also includes a comprehensive understanding and the specific vision of the critical infrastructure context.

In addition, and as mentioned previously, the Cybersane software offers tools that guide the operator in the analysis and prioritisation of cyber incidents. It also allows the reuse of knowledge generated from the modelling of previous security events as a basis for analysis and decision-making on new incidents that may have common characteristics.

4.4.2. Activity 3 – incident response

The IRT at ABZ initiated a sequence of modelling activities that were aimed at representing the cyber incident analysis and response. The first task was an internal investigation of the cyber incident and its potential impact on assets. The initial application of detection mechanisms and incident analysis activities allowed the IRT to express concerns and establish the operationalisation of a Jigsaw Ransomware as a result of cybercriminal activities that exploited a buffer flow vulnerability and malicious code injection. The analysis accordingly identified the cybercriminal's fingerprints on one of the systems, and a further examination revealed that the incident had impacted on multiple assets and rendered critical functions unavailable. An incident register was created containing analysis information, including the type, affected assets, severity, and other details about the incident, as shown in Table 23.

Furthermore, a holistic and definitive model was developed on the basis of the incident identification and analysis register, which provided a more precise representation of the incident details to ensure streamlined, consistent and coordinated response activities. In particular, the model offers a consolidated view of the specificities of the cyber incident (Fig. 10). The view is underpinned by the analysis result obtained from the IRT. The model highlights the ac-

Table 23
Incident Identification and Analysis.

Cyber Incident Details					
ID	Type		Priority	Affected Assets & Functions	Impact
CI01	Malicious Code Injection (Jigsaw Ransomware)	Data extrusion	1	Private Data	10
		Data encryption	2	Transmission Grid Network	8
		Lateral Movement	1	Distribution Management System	8
				Production, Distribution, and Transmission of solar electric power	8

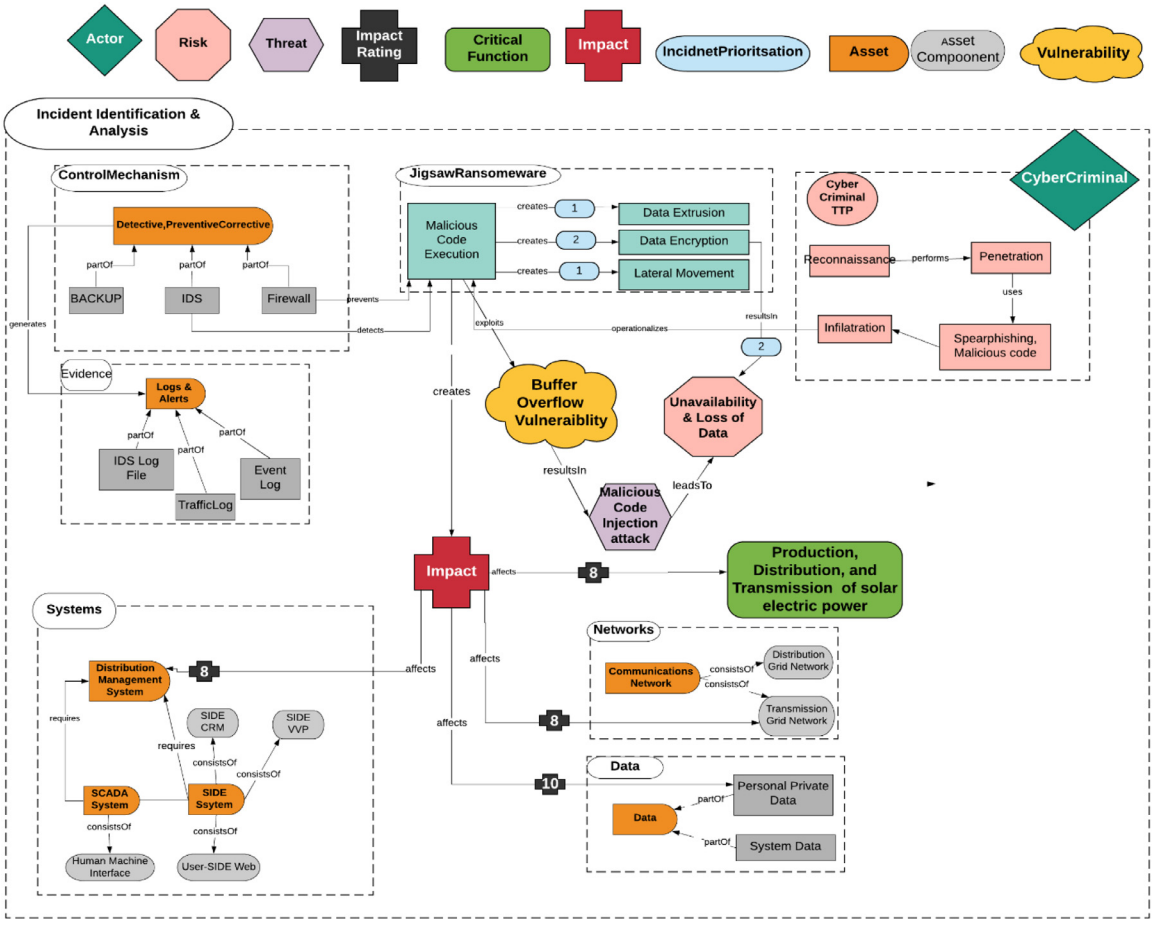


Fig. 10. Incident Analysis.

tivities of a Cybercriminal as the perpetrator of the incident, This person performed the reconnaissance of ancillary communication channels, systems and services in order to identify common existing vulnerabilities. The cyber attacker then used a set of tactics, techniques and procedures to accomplish the injection of malicious code by exploiting a buffer overflow vulnerability. The malicious code followed a succession of stages, from the exfiltration, lateral movement and encryption of data. The operationalisation of the attack enabled the attacker to gain access to and rendered critical distribution management systems, transmission control networks, and personal data unavailable. The model, therefore, provided the basis for IRT and ABZ operators to understand and plan for an implementable cyber course of actions with which to react to the incident.

The second task involved the IRT embarking on a coordinated set of actions that stress the allocation of capabilities and resources for the eradication and recovery from the cyber incident. The actions entail a various coordinated cyber course of action strategies from a procedural and technical perspective, whose main objective was to limit further impact on ABZ assets, along with improving the existing control mechanisms. Before the implementation of the course of action strategies, the IRT had identified weaknesses in existing control measures, thus allowing the cybercriminal to infiltrate all inbound and outbound connections into the communication networks of ABZ. The IRT, therefore, deployed a procedural course of action, which introduced a set of administrative controls in the form of policies and standard operating procedures. For example, policies mandating automated patch management to systems, along with regular data backup, were introduced. In addition, the technical course of actions was introduced, imposing a set of monitoring, detection and control systems for incident containment and eradication purposes. The IRT consequently proceeded to develop an incident response model based on the cyber course of action strategies highlighted in Table 24. The model played a vital role in providing a realistic representation of multiple actions and enabling the IRT to articulate the elements of incident response strategies in terms of the strategic and functional course of actions, thus helping ABZ to develop a clear incident response roadmap (Fig. 11).

Table 24
Incident Response Strategies.

Actor	Goal	Control Mechanism Detective	Preventive	Corrective	CCoA Procedural	Technical
IRT	Eradicate and recover from incident	Intrusion Detection Systems	Firewalls	Data and Process Backup	Management and software update tools Regular data backup and proper protection using encryption	Manage Network Devices Using Multifactor Authentication and Encrypted Sessions Host-based firewalls on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed

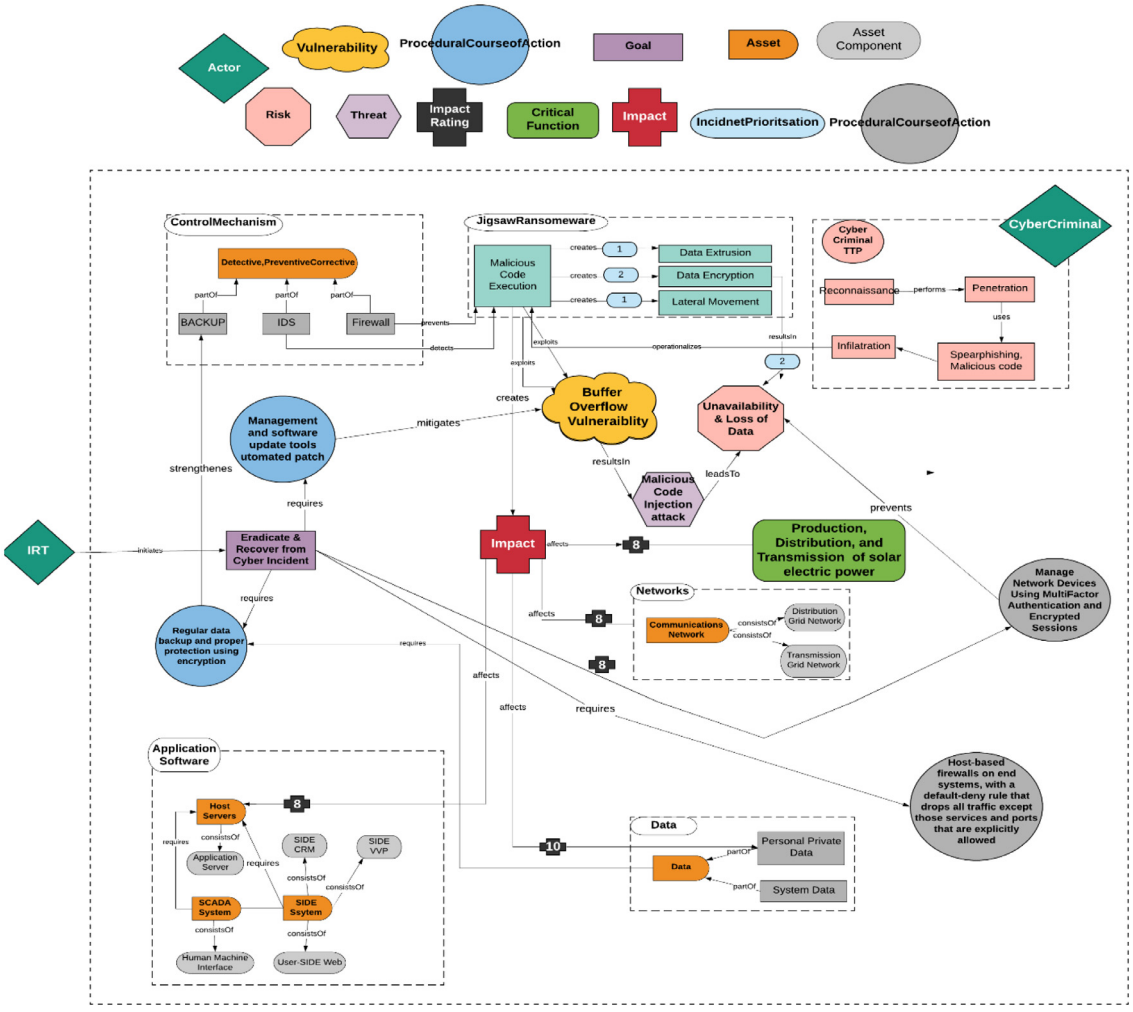


Fig. 11. Incident Containment, Eradication and Recovery.

The incident analysis information was, therefore, used as the basis on which to generate models, including specific action planning to tackle the threats identified. The cyber courses of action similarly also considered the actions required in order to review and correct the vulnerabilities found.

The models generated not only offered the possibility of representing cyber-action strategies, but also of providing a specific context for all the factors to be taken into account and the relationships among the different elements linked in the response plan. In addition, both the context and assessment of the incident and the proposed course of action were modelled by taking into account the control mechanism and its categorisation, and the cyber course of action was adapted to a critical infrastructure context.

In a complementary manner, the added value of the Cybersane tool as regards providing support for decision making should be highlighted. In this respect, heat maps were a valuable resource as regards planning incident response actions based on the defined and depicted priorities calculated from the information gathered in the previous step. The strategic and functional course of actions similarly became part of the tool's knowledge base, thus enhancing Cybersane's decision-making support features based on the future possibilities of reusing the knowledge generated in the incident response for the company itself.

5. Discussion

The proposed modelling language presented in this paper has proved to be effective as regards analysing and representing cybersecurity incident handling processes. We have identified a list of criteria for the modelling language, and CIHML satisfies these criteria. We have considered three different views, namely CII analysis, threat and risk analysis, and incident response views that allow the

visual representation of the incident handling process. The underlying concepts of CIHML are formed according to relevant cybersecurity domains, including security requirements, incident handling, forensics, and risk management. This means that the concepts are vital for analysing the incident and including and determining the suitable cyber course of actions for the incident management. The proposed process consists of three activities that allow CII operators to systematically manage post-incident activities based on the implementation of the concepts and models in CIHML.

5.1. Observed results

Upon observing the studied context, it was found that the proposed approach is promising for the analysis and modelling of incident response processes for critical information infrastructure. In particular, the three distinct models relating to CII, threat and risk, incident response and its visual presentation efficiently connect critical infrastructure and related functions with specific threats, risks and incidents, thus allowing an appropriate cyber course of actions to be determined. The process systematically supports the analysis and control of the cyber incident, in addition to producing various artefacts with which to record threats, risks, incidents, and control actions.

5.2. Lessons learned

The implementation process made it possible to learn lessons and discover opportunities for improvements. Our observations indicate that the CII operators involved in the implementation process of CIHML initially found it challenging to understand and create the different modelling views in CIHML. In other instances, operators successfully created the models without understanding the actual purpose and benefits for creating them. This is mainly because the CII operators had varying levels of knowledge and experience of requirements engineering and modelling, which in some respects hindered their ability to sufficiently understand the concepts and how they could be used to create the different models. However, as the implementation exercise progressed, their understanding improved significantly, and they performed the activities rapidly and spent less time building the models. For instance, the analysis of CII enabled them to gain a new perspective of the critical functions, requirements, roles and actor goals that they had not previously considered. In particular, CIHML initiates with a critical infrastructure analysis, including specific critical sector, assets, possible actors within the sector, their goals and related security and privacy constraints. The underlying model based on these entities visually demonstrates the interdependencies among them and supports the threat analysis.

Similarly, the threat analysis modelling approach fostered implicit analysis. We found that it empowers CII operators to identify new vulnerabilities of the assets, understand the threats that are associated with a specific cyber incident, how an incident occurred, and the priority and impact of the incident. It aims to provide a structured representation of threat information that expresses valuable situational and contextual threats within specific CII context. To this end, CIHML has adopted the STRIDE and DREAD models and links with the CVE for the potential causes for the threats. The vulnerabilities are also ranked on the basis of the CVSS score. The threats and vulnerabilities allow risks to be identified and quantified. The incidents are identified and prioritised on the basis of the threats and vulnerabilities and are linked with the assets and functions. CIHML also guided the practitioners to choose right level of controls and course of action required to tackle the incidents. The incident containment and eradication model also helped the CII operators to achieve consistent results by providing a baseline of control considerations that led them to focus on the appropriate incident response actions and strategies. The controls are categorised in terms of detective, preventive and corrective controls with a procedural and technical course of actions. CIHML integrates industry specific standards and practices such as STRIDE and CVE, which will support the more widespread adoption of CIHML. The underlying activities used for the CIHML are fully operational based on the context studied. The visual modelling of the CII, threat and incident analysis made it easy to communicate the incident by relating information to the relevant stakeholder, and this further supports informed decision making.

5.3. Challenges encountered

A few challenges were observed after implementing the CIHML in the context studied. Some of the challenges encountered appertain the sharing of common knowledge of the concepts among CII operators. Although we proposed a conceptual model and a representation of the concepts and their attributes, we observed that the operators initially struggled to understand the specific terminology/concepts of CIHML, which resulted in inconsistency and an ineffective implementation. Based on the context studied, the users found it challenging to develop the model. Additionally, if the CII context is complex, such as large number of assets, actors, functions and goals, then the model will be much more complex. We, therefore, aim to develop a user manual document that will allow the users to easily follow the process and develop the artefacts. We shall develop guidelines on how to split the model in order to provide a better understanding of the CII. We also plan to include a common point of compromise to allow the controls to be prioritised in order to tackle incidents. We additionally intend to use an ontology as the foundation on which to enhance the conceptual elements of CIHML, whose objective will be to convey a shared understanding of the concepts.

6. Conclusion

Cyber threats are rapidly evolving, which is constantly increasing the security incident, particularly as regards the critical information infrastructure. As recent conflicts (e.g. Ukraine-Russia war) have shown, critical infrastructures are one of the weakest points in the ecosystem of a modern society. Security incidents may, depending on the severity of their impact, have catastrophic consequences for the global continuity of businesses, governments, and affect the quality of citizens' lives.

This paper presents a new proposal with which to deal with incident management in critical infrastructures. To this end, a language and a modelling process have been developed with the aim of analysing and managing security incidents in this type of infrastructure.

The results obtained from its application in the context of case studies show that it is a viable solution for the management of this type of incident. The work decomposes multiple models, which allow the visual representation of and correlation among threats, risk, incident and control. Its application to a critical infrastructure in the energy sector has been presented in this paper.

As future work, we plan to add new case studies, which will allow a transfer of knowledge from the linguistic model to critical infrastructures, and this will provide valuable feedback to improve the modelling language presented. This will also provide valuable datasets to be used in the subsequent phases.

We now plan to extend the model by adding new data analysis techniques associated with the field of deep learning. To this end, the current model will be integrated with machine learning algorithms in order to obtain incident patterns associated with the type of critical infrastructure, and to predict future incidents, along with the severity associated with them. Incident prediction will

also be validated using datasets of cybersecurity incidents on critical infrastructures in different sectors.

Finally, the CyberSANE tool employed to support CIHML will continue to evolve by partially automating the overall process, always seeking to ensure that the automation of the functionalities is of value to professionals by helping them to make decisions but allowing them to make the final decision.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

CRediT authorship contribution statement

Haralambos Mouratidis: Project administration, Conceptualization. **Shareeful Islam:** Supervision, Methodology. **Antonio Santos-Olmo:** Visualization, Formal analysis. **Luis E. Sanchez:** Visualization, Investigation. **Umar Mukhtar Ismail:** Software, Investigation, Validation.

Data availability

The data that has been used is confidential.

Acknowledgments

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833683, AETHER-UCLM (PID2020-112540RB-C42) and ALBA-UCLM (TED2021-130355B-C31) funded by "Ministerio de Ciencia e Innovación", Spain.

References

Adepu, S., Kang, E., Mathur, A.P., 2019. Challenges in secure engineering of critical infrastructure systems. In: Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW), pp. 61–64. doi:10.1109/ASEW.2019.00030.

Ahmad, A., Hadgkiss, J., Ruighaver, A.B., 2012. Incident response teams – challenges in supporting the organisational security function. Comput. Secur. 31 (5), 643–652. doi:10.1016/j.cose.2012.04.001.

Ahmad, A., Webb, J., Desouza, K.C., Boorman, J., 2019. Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput. Secur. 86, 402–418. doi:10.1016/j.cose.2019.07.001.

Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., Baskerville, R.L., 2020. How integration of cyber security management and incident response enables organizational learning. J. Assoc. Inf. Sci. Technol. 71 (8), 939–953. doi:10.1002/asi.24311.

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T., Baskerville, R.L., 2021. How can organizations develop situation awareness for incident response: a case study of management practice. Comput. Secur. 101, 102122. doi:10.1016/j.cose.2020.102122.

Athinaiou, M., Mouratidis, H., Fotis, T., Pavlidis, M., Panaousis, E., Furnell, S., Mouratidis, H., Pernul, G., 2018. Towards the definition of a security incident response modelling language. In: Trust, Privacy and Security in Digital Business. Springer International Publishing, Cham, pp. 198–212. doi:10.1007/978-3-319-98385-1_14.

Booth, H., Rike, D., Witte, G.A., 2013. The National Vulnerability Database (NVD): Overview. ITL Bulletin. National Institute of Standards and Technology, Gaithersburg, MD Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=915172.

Canito, A., Aleid, K., Praça, I., Corchado, J., Marreiros, G., 2020. An ontology to promote interoperability between cyber-physical security systems in critical infrastructures. In: Proceedings of the IEEE 6th International Conference on Computer and Communications (ICCC), pp. 553–560. doi:10.1109/ICCC51575.2020.9345163.

Chockalingam, S., Maathuis, C., 2022. An ontology for effective security incident management. In: Proceedings of the International Conference on Cyber Warfare and Security, pp. 26–35. doi:10.34190/iccws.17.1.6.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., 2012. Computer security incident handling guide. NIST Spec. Publ. 800 (61), 1–147. http://dx.doi.org/10.6028/NIST.SP.800-61r2.

Common Vulnerabilities and Exposures (CVE). MITRE; 2023. Avaliable from: https://cve.mitre.org/.

CyberSANE, 2022. SU-ICT-01-2018: "Dynamic Countering of Cyber-Attacks". CyberSANE Available from: https://www.cybersane-project.eu/.

ENISA, 2010. Good Practice Guide for Incident Management. ENISA Available from: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

ENISA, 2016. ENISA Threat Taxonomy - Data Europa EU. ENISA Available from: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

EPCIP, 2008. Council Directive 2008/114/EC on the Identification and Description of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. EPCIP Union OJotE, editor.

ETSI_TR_103_331_V1.2.1. ETSI_TR_103_331_V1.2.1. Structured threat information sharing. In: (ETSI). ETSI, editor.: Sep, 2019; 2019.

Faily, S., Fléchais, I., 2010. A meta-model for usable secure requirements engineering. In: Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems, pp. 29–35. doi:10.1145/1809100.1809105.

Fombona Cadavieco, J., Rodríguez Pérez, C., Barriada Fernández, C, 2012. Information technology incident management: a case study of the university of Oviedo and the faculty of teacher training and education. Int. J. Educ. Technol. High. Educ. 9 (2), 280–295. doi:10.7238/rusc.v9i2.1399.

Gaidarski, I., Minchev, Z., Tagarev, T., Atanassov, K.T., Kharchenko, V., Kacprzyk, J., 2021. Insider threats to IT security of critical infrastructures. In: Digital Transformation, Cyber Security and Resilience of Modern Societies. Springer International Publishing, Cham, pp. 381–394. doi:10.1007/978-3-030-65722-2_24.

González-Granadillo, G., González-Zarzosa, S., Diaz, R., 2021. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors 21 (14), 4759. doi:10.3390/s21144759.

Grispos, G., Glisson, W.B., Storer, T., 2017. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digit. Investig. 22, 62–73. doi:10.1016/j.diin.2017.07.006.

Humphreys, E, 2016. Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House ISBN: 1608079317.

Idani, A., Halpin, T., Krogstie, J., Nurcan, S., Proper, E., Schmidt, R., Soffer, P., et al., 2009. UML models engineering from static and dynamic aspects of formal specifications. In: Enterprise, Business-Process and Information Systems Modeling. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 237–250. doi:10.1007/978-3-642-01862-6_20.

ISO/IEC_27004:2016. ISO/IEC FCD 27004:2016, Information Technology — Security techniques — Information security management - Monitoring, Measurement, Analysis and Evaluation (Second Edition), ISO/IEC_27004:2016. 2016. Available from: https://www.iso.org/standard/64120.html. [Accessed 22/12/2022].

ISO/IEC_27035-1:2016. ISO/IEC 27035-1:2016, Information technology — Security techniques — Information security incident management — Part 1: principles of incident management; 2016. Available from: https://www.iso.org/standard/60803.html. [Accessed 22/12/2022].

ISO/IEC_27035-2:2016. ISO/IEC 27035:2016-2, Information technology — Security techniques — Information security incident management — Part 2: guidelines to plan and prepare for incident response; 2016. Available from: https://www.iso.org/standard/62071.html. [Accessed 22/12/2022].

Knight, R., Nurse, J.R.C., 2020. A framework for effective corporate communication after cyber security incidents. Comput. Secur. 99, 102036. doi:10.1016/j.cose.2020.102036.

Kolovos, D.S., Paige, R.F., Kelly, T., Polack, F.A., 2006. Requirements for domain-specific languages. In: Proceedings of the ECOOP Workshop on Domain-Specific Program Development (DSPD).

Kosar, T., Bohra, S., Mernik, M., 2016. Domain-specific languages: a systematic mapping study. Inf. Softw. Technol. 71, 77–91. doi:10.1016/j.infsof.2015.11.001.

Kure, H.I., Islam, S., Mouratidis, H., 2022. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput. Appl. doi:10.1007/s00521-022-06959-2.

Kuypers, M.A, 2017. Risk in Cyber Systems. Management Science & Engineering: Stanford University.

Lehto, M., Lehto, M., Neittaanmäki, P, 2022. Cyber-Attacks Against Critical Infrastructure. In: Cyber Security: Critical Infrastructure Protection. Springer International Publishing, Cham, pp. 3–42. doi:10.1007/978-3-030-91293-2_1.

Lekota, F., Coetzee, M., 2019. Cybersecurity incident response for the Sub-Saharan African aviation industry. In: Proceedings of the International Conference on Cyber Warfare and Security. Reading: Academic Conferences International Limited, pp. 536–545 XI-XII.

Lewis, T.G, 2019. Critical Infrastructure Protection in Homeland security: Defending a Networked Nation. John Wiley & Sons ISBN: 1119614538.

Maglaras, L.A., Kim, K.-.H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., et al., 2018. Cyber security of critical infrastructures. ICT Express 4 (1), 42–45. doi:10.1016/j.icte.2018.02.001.

Mahima, D., 2021. Cyber threat in public sector: modeling an incident response framework. In: Proceedings of the International Conference on Innovative Practices in Technology and Management (ICIPTM), pp. 55–60. doi:10.1109/ICIPTM52218.2021.9388333.

Mattioli R., Levy-Bencheton C. Methodologies for the identification of critical information infrastructure assets and services; European Union Agency for Network and Information Security (ENISA). December, 2014. ISBN 978-92-9204-106-9, doi:10.2824/38100.

Meier, J., 2003. Improving Web Application Security: Threats and Countermeasures. Microsoft Press ISBN: 0735618429.

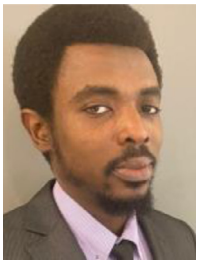
Metzger, S., Hommel, W., Reiser, H., 2011. Integrated security incident management – concepts and real-world experiences. In: Proceedings of the Sixth International Conference on IT Security Incident Management and IT Forensics, pp. 107–121. doi:10.1109/IMF.2011.15.
Microsoft, 2007. Getting Started with the Threat Modeling Tool. Microsoft Microsoft Article.
Mouratidis, H., Argyropoulos, N., Shei, S, Karagiannis, D., Mayr, H.C., Mylopoulos, J., 2016. Security requirements engineering for cloud computing: the secure tropos approach. In: Domain-Specific Conceptual Modeling: Concepts, Methods and Tools. Springer International Publishing, Cham, pp. 357–380. doi:10.1007/978-3-319-39417-6_16.
Naseer, A., Naseer, H., Ahmad, A., Maynard, S.B., Masood Siddiqui, A, 2021. Real-time analytics, incident response process agility and enterprise cybersecurity performance: a contingent resource-based analysis. Int. J. Inf. Manag. 59, 102334. doi:10.1016/j.ijinfomgt.2021.102334.
NIST, 2022. NVD. Common Vulnerability Scoring System. NIST Available from: https://nvd.nist.gov/vuln-metrics/cvss#.
Nnoli, H., Lindskog, D., Zavarsky, P., Aghili, S., Ruhl, R., 2012. The governance of corporate forensics using COBIT, NIST and increased automated forensic approaches. In: Proceedings of the International Conference on Privacy, Security, Risk and Trust and International Confernece on Social Computing, pp. 734–741. doi:10.1109/SocialCom-PASSAT.2012.109.
Nordstrom, G., Sztipanovits, J., Karsai, G., Ledeczi, A., 1999. Metamodeling-rapid design and evolution of domain-specific modeling environments. In: Proceedings of the ECBS'99 IEEE Conference and Workshop on Engineering of Computer-Based Systems, pp. 68–74. doi:10.1109/ECBS.1999.755863.
OWASP, 2014. OWASP Risk Rating Methodology 2014. OWASP Available from: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.
Papastergiou, S., Mouratidis, H., Kalogeraki, E.-M., Macintyre, J., Iliadis, L., Maglogiannis, I., Jayne, C., 2019. Cyber security incident handling, warning and response system for the european critical information infrastructures (CyberSANE). In: Engineering Applications of Neural Networks. Springer International Publishing, Cham, pp. 476–487. doi:10.1007/978-3-030-20257-6_41.
Papastergiou, S., Mouratidis, H., Kalogeraki, E.-M., 2021. Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. Evol. Syst. 12 (1), 91–108. doi:10.1007/s12530-020-09335-4.
Plėta, T., Tvaronavičienė, M., Della Casa, S, 2020. Cyber effect and security management aspects in critical energy infrastructures. Insights Reg. Dev. 2, 538–548. doi:10.9770/IRD.2020.2.2(3).
Prasad, R., Rohokale, V., 2020. Cyber Security: the Lifeline of Information and Communication Technology. Springer ISBN: 303031703X doi:10.1007/978-3-319-98385-1_14.
Ramsay, J.D., Cozine, K., Comiskey, J., 2020. Theoretical Foundations of Homeland Security: Strategies, Operations, and Structures. Routledge ISBN: 0429535562.
Rosado, D.G., Santos-Olmo, A., Sánchez, L.E., Serrano, M.A., Blanco, C., Mouratidis, H., et al., 2022. Managing cybersecurity risks of cyber-physical systems: the MARISMA-CPS pattern. Comput. Ind. 142, 103715. doi:10.1016/j.compind.2022.103715.
Sabillon, R., 2022. Cybersecurity incident response and management. In: Research Anthology on Business Aspects of Cybersecurity. IGI Global, Hershey, PA, USA, pp. 611–620. doi:10.4018/978-1-6684-3698-1.ch028.
Salvi, A., Spagnoletti, P., Noori, N.S., 2022. Cyber-resilience of critical cyber infrastructures: integrating digital twins in the electric power ecosystem. Comput. Secur. 112, 102507. doi:10.1016/j.cose.2021.102507.
Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., et al., 2017. A collaborative cyber incident management system for European interconnected critical infrastructures. J. Inf. Secur. Appl. 34, 166–182. doi:10.1016/j.jisa.2016.05.005.
Simou, S., Kalloniatis, C., Mouratidis, H., Gritzalis, S., Lambrinoudakis, C., Gabillon, A., 2016. A Meta-model for assisting a cloud forensics process. In: Risks and Security of Internet and Systems. Springer International Publishing, Cham, pp. 177–187. doi:10.1007/978-3-319-31811-0_11.
Sklyar, V., Kharchenko, V., 2019. ENISA documents in cybersecurity assurance for industry 4.0: iIoT threats and attacks scenarios. In: Proceedings of the 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), pp. 1046–1049. doi:10.1109/IDAACS.2019.8924452.
Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., Hutchison, D., 2022. A cyber incident response and recovery framework to support operators of industrial control systems. Int. J. Crit. Infrastruct. Prot. 37, 100505. doi:10.1016/j.ijcip.2021.100505.
Tøndel, I.A., Line, M.B., Jaatun, M.G., 2014. Information security incident management: current practice as reported in the literature. Comput. Secur. 45, 42–57. doi:10.1016/j.cose.2014.05.003.
Tanczer, L.M., Brass, I., Carr, M, 2018. CSIRTs and global cybersecurity: how technical experts support science diplomacy. Glob. Policy 9 (S3), 60–66. doi:10.1111/1758-5899.12625.
Theoharidou, M., Kotzanikolaou, P., Gritzalis, D, Palmer, C., Shenoi, S., 2009. Risk-based criticality analysis. In: Critical Infrastructure Protection III. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 35–49. doi:10.1007/978-3-642-04798-5_3.
Viegas, V., Kuyucu, O., 2022. International security standards. In: IT Security Controls: A Guide to Corporate Standards and Frameworks. Apress, Berkeley, CA, pp. 17–65. doi:10.1007/978-1-4842-7799-7_2.
Visscher, C., 2021. Towards Cyber Incident Response on Naval Ships: The Cyber Incident Response Decision Model. EEMCS: Electrical Engineering, Mathematics and Computer Science. University of Twente, Thales Nederland B.V., Hengelo, The Netherlands.
Wang, P., Park, S.-A., 2017. Communication in Cybersecurity: a public communication model for business data breach incident handling. Issues in Information Systems 18 (2). doi:10.48009/2_iis_2017_136-147.
Wunder J., Halbardier A., Waltermire D. Specification For Asset Identification 1.1. In: NIST, ed.: US Department of Commerce, National Institute of Standards and Technology; 2011.
Yeboah-Ofori, A., Islam, S., 2019. Cyber security threat modeling for supply chain organizational environments. Future Internet 11 (3), 63. doi:10.3390/fi11030063.

Haralambos (Haris) Mouratidis is Director, Institute for Analytics and Data Science (IADS) and Professor, School of Computer Science and Electronic Engineering, University of Essex. He holds a B.Eng. (Hons) from the University of Wales, Swansea (UK), and a M.Sc. and PhD from the University of Sheffield (UK). He is also Fellow of the Higher Education Academy (HEA) and Professional Member of the British Computer Society (BCS). Haris has been a visiting researcher at the National Institute of Informatics (NII), Japan, and a visiting fellow at the British Telecom (BT), U.K and the University College London, U.K. He is visiting professor at the University of the Aegean, Greece. His research interests lie in the area of secure software systems engineering, requirements engineering, and information systems development. He is interested in developing methodologies, modelling languages, ontologies, tools and platforms to support the analysis, design, monitoring of security, privacy, risk and trust for large-scale complex software systems. He has published more than 130 papers (h-index 21) and he has secured funding as Principal Investigator from national (Engineering and Physical Sciences Research Council (EPSRC), Royal Academy of Engineering, Technology Strategy Board (TSB)) and international (EU, NII) funding bodies as well as industrial funding (British Telecom, ELC, Powerchex, FORD) towards his research. His e-mail address is h.mouratidis@essex.ac.uk

Shareeful Islam is currently working at the School of Computing and Information Science, Anglia Ruskin University, UK. He was the visiting researcher at the National Institute of Informatics (NII), Japan and SBA research, Austria. His research interests lie in the areas of cyber security, risk management, requirement engineering and information systems. He has pioneered work in developing risk assessment and treatment methods using business and technical goals, modelling language for cyber security risk management. The works are implemented in various application domains including cloud migration, critical infrastructure, and healthcare sector cyber security. He has published more than 70 papers (h-index 26) and he has led and/or participated in projects funded by the European Union (FP7), Innovate UK, FwF, and DAAD. He has experience of acting as evaluator for national and international funding bodies including the EPSRC, FwF, and CHIST-ERA. His e-mail address is Shareeful.islam@aru.ac.uk

Antonio Santos-Olmo is M.Sc and PhD. in Computer Science by the University of Castilla-La Mancha. He is an Assistant Professor at the Escuela Superior de Informática of the University of Castilla- La Mancha in Ciudad Real (Spain). M.Sc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- La Mancha, in Ciudad Real (Spain). His email is antonio.santosolmo@uclm.es

Luis E. SáNchez holds a PhD in Computer Science from the University of Castilla-La Mancha (Spain), a MSc in Computer Science from the Polytechnic University of Madrid (Spain) and holds a degree in Computer Science from the University of Granada (Spain). He is Certified Information System Auditor by ISACA and Leader Auditor of ISO27001 by IRCA. He is Assistant Professor at the University of the Armed Forces of Ecuador. He participates at the GSyA research group of the Department of Information Technologies and Systems at the Castilla-La Mancha University and he is a researcher of Biological Neurocomputing and Cyberdefense within the PROMETEO project. He was Assistant Professor of the Technologies and Information Systems Department of the University of Castilla-La Mancha. He has directed more than 50 projects in multinational companies. He has more than 60 national and international papers and conference on Software Engineering and Teaching. He belongs to various professional and research associations (COIIL-CLM, ALI, ASIA, TUVRheinland, ISACA, eSec INTECO, SC27 AENOR ...). His email is luise.sanchez@uclm.es



Umar Mukhtar Ismail is a Lecturer in the Department of Computer Science and Digital Technologies. He is currently the programme leader for BSc (Hons) Cyber Security Networks and BSc (Hons) Cloud Computing. He is involved in research development projects that aim enhancing the security, privacy and resilience systems and applications in various domains such as critical information infrastructure, cyber physical systems, supply chain, cloud computing, medical and healthcare systems. Umar is a Fellow of the Higher Education Academy, a member of British Computing Society (BCS), Institute of Electrical and Electronics Engineers (IEEE), Information Systems Audit and Control Association (ISACA), and member of organising committee for various international conferences. His email is u.ismail@uel.ac.uk