IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2024.Doi Number

A Unified Ontological Framework for Integrated Regulatory Compliance and Cybersecurity Requirements in Critical Infrastructure

E. Bružė[1], G. Sabaliauskaite[2], R. A. Paskauskas[1], R. Matulytė[1], and T. Lavišius[1]

[1]Security Research Laboratory, Mykolas Romeris University, 08303 Vilnius, Lithuania
[2]Faculty of Public Governance and Business, Mykolas Romeris University, 08303 Vilnius, Lithuania

Corresponding author: G. Sabaliauskaite (e-mail: giedre.s@mruni.eu).

This work was supported in part by the European Union through the Recovery and Resilience Facility (2021–2027 programming period, New Generation Lithuania plan), and co-funded by the state budget of the Republic of Lithuania administered via the Research Council of Lithuania (Lietuvos Mokslo Taryba), as part of the project "Implementation of Mission-Based Science and Innovation Programs" (Project No. 02-002-P-0001).

ABSTRACT The expanding and increasingly fragmented EU regulatory landscape presents significant challenges for critical infrastructure operators. Regulations such as NIS2, the Cyber Resilience Act, the GDPR, and the AI Act introduce extensive cybersecurity, data-protection, and AI-governance obligations. However, these legal instruments are not fully harmonized, evolve over time, and impose overlapping or even conflicting requirements across different sectors and jurisdictions. This regulatory dynamism, combined with the lack of semantic alignment between laws, standards, and technical frameworks, makes it difficult for organizations to ensure and maintain coherent compliance. At the same time, organizations face advanced cyberattacks targeting critical infrastructure systems, underscoring the need for methods capable of integrating regulatory and technical perspectives. To address these challenges, this paper proposes an integrated ontological framework that provides a unified semantic representation to link legal obligations (NIS2, GDPR, AI Act), organisational cybersecurity processes (NIST CSF 2.0), technical controls (IEC 62443), and adversarial behaviours (MITRE ATT&CK for ICS), which enables machine-interpretable traceability from legal obligations to concrete threat mitigations. The framework is validated through an application scenario to Industrial Automation and Control Systems.

INDEX TERMS Ontologies, requirements engineering, regulation, cybersecurity, privacy, critical infrastructure, regulatory compliance

I. INTRODUCTION

The rapid expansion, interdependence, and growing complexity of the European Union's (EU) digital regulatory environment have created significant challenges for organizations operating critical infrastructure. Regulations such as the NIS2 Directive [1], the Cyber Resilience Act (CRA) [2], the General Data Protection Regulation (GDPR) [3], the EU Artificial Intelligence Act (AI Act) [4], the Critical Entities Resilience Directive (CER) [5], and the Digital Operational Resilience Act (DORA) [6] collectively introduce extensive and evolving obligations related to cybersecurity, data protection, and the trustworthy use of technologies. These legal instruments shape a multilayered governance framework that applies across diverse sectors and Member States, creating both horizontal and sector-specific compliance requirements that organizations must navigate.

Critical infrastructure operators must comply not only with high-level cybersecurity obligations but also with detailed provisions governing personal data processing, AI system development and deployment, and safety-oriented technical controls. National-level transposition of EU directives, such as the NIS2 Directive, introduces additional variability, complicating cross-border compliance. Recent policy guidelines and emerging case law from the Court of Justice of the European Union (CJEU) further refine interpretations of permissible data collection, automated decision-making, and AI-enabled security measures,

underscoring the dynamic nature of the regulatory environment.

In parallel, organizations face escalating cybersecurity threats targeting industrial control systems and essential services. Frameworks such as NIST Cybersecurity Framework (CSF) 2.0 [7], sector-specific cybersecurity standards including IEC 62443 [8], and threat-modelling approaches such as the MITRE ATT&CK® for ICS [9] provide structured methods for risk management and threat-informed security controls. However, integrating these technical frameworks with regulatory requirements remains a persistent challenge, particularly as cybersecurity, privacy, and AI obligations increasingly intersect.

Ontology-based Requirements Engineering (ObRE) has emerged as a robust method for formalizing these legal and technical requirements into machine-interpretable structures. ObRE enables the formalization of legal and technical requirements into machine-interpretable structures, supporting consistent interpretation, traceability, and automated analysis [10]. While recent work demonstrates successful application of ontological methods to individual regulations, such as GDPR, the AI Act, and IEC 62443, most existing approaches remain limited to single-framework implementations.

Building on our prior research focused on automating regulatory compliance of dual-use AI systems [11], this paper advances a unified methodology that integrates regulatory requirements, organizational cybersecurity frameworks, sector-specific standards, and threat models into a single ontological framework. By combining NIS2, CRA, GDPR, the AI Act, NIST CSF 2.0, IEC 62443, and the MITRE ATT&CK for ICS, the proposed approach provides a comprehensive foundation for threat-informed, automated regulatory compliance in critical infrastructure environments.

This paper details the EU regulatory landscape, outlines the proposed integrated ontological framework, and demonstrates its application to critical infrastructure systems and organizations. The results highlight the potential for automated, ontology-based methods to support compliance-by-design and enhance cybersecurity resilience of critical infrastructure.

The remainder of this paper is structured as follows. Section 2 describes background information, while Section 3 summarizes related work. Section 4 explains the methodology, followed by Section 5, which proposes an ontological framework for regulatory compliance and cybersecurity requirements specification. Its application to demonstrated in Section 6, and the results are discussed in Section 7. Section 8 describes future work, while Section 9 concludes the paper.

II. BACKGROUND INFORMATION

This section includes the overview of the EU regulatory landscape for critical infrastructure, along with a description of relevant cybersecurity standards, cyber threat classification and intelligence sharing.

A. OVERVIEW OF EU REGULATORY LANDSCAPE FOR CRITICAL INFRASTRUCTURE

1) RELEVANT REGULATIONS AND GUIDANCE

The cybersecurity framework is not only extensive but to some extent also varies from Member State to Member State in the EU.

The primary source for cybersecurity requirements applicable for critical infrastructure in the current legal landscape is the NIS2 Directive. It establishes the highly critical sectors (e.g., energy, transport, banking, health, digital infrastructure, etc.) and other critical sectors (e.g., postal and courier services, waste management, manufacturing, digital providers, etc.). While sectors essentially should not differ among EU Member States, the transposed technical and organizational requirements depend on the approach chosen by the Member State's legislator. The literature review concerning NIS2 outlines the increased complexity and regulatory fragmentation [12].

The CRA lays down rules for products with digital elements to ensure the cybersecurity of such products and define essential cybersecurity requirements for such products and their handling processes [2].

The CER [5] lays down obligations on Member States to take specific measures, to ensure that essential services for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market.

In finance sector, DORA specializes exclusively in the strengthening of the digital resilience of financial entities [6].

In addition to the above, developing a cyber-threat management system that operates across different EU Member States and utilizes a dedicated software technology for data monitoring requires navigating a balance between necessary security measures and strict privacy and artificial intelligence requirements. For example, if the technology aims to collect IP addresses, hostnames, metadata and other information that could be used to identify a natural person, it will inevitably process personal data. Therefore, rigorous compliance with applicable data protection laws, such as GDPR, and national implementing laws must be ensured. Furthermore, if AI models are used for cybersecurity purposes, the AI Act and its requirements can also come into force.

All of the above-listed pieces of legislation introduce a significant number of requirements that need to be implemented for systems dedicated to ensuring. Asynchronous implementation timelines pose a significant challenges: the NIS2 Directive should have been transposed into the law of the member states by mid-October 2024, the

GDPR has been in full force since May 2018, DORA required financial entities in the EU to be fully compliant by January 17, 2025, and the AI Act should enter into full force only in August 2027 (with certain obligations already applicable as of 2026 or even 2025). In addition, recent EC initiatives, such as Digital Omnibus [13], are proposing to simplify existing rules on AI, cybersecurity, data protection and other digital regulation domain, but the challenges for entities that need to comply with the requirements remain quite numerous with a significant threat of deregulation instead of simplification. However, we are yet to see how the Digital Omnibus will be implemented, if implemented at all.

There is an ongoing discussion that, especially NIS2 and CER, while welcomed, provide a certain ambiguity which may make their implementation and subsequent compliance challenging [14]. Moreover, considering the necessity to comply with multiple cybersecurity laws, there is a need for seeking synergies for compliance which underlines the holistic and risk-based approach. Furthermore, concepts of security by design are emerging [15]. Thus, a solution for automated regulatory compliance requirement specification could significantly help organizations to cope with regulatory compliance.

2) RECENT POLICY AND COURT PRACTICES

When it comes to regulatory compliance practice, it should be noted that recent practices are formed not only on the basis of legal regulation but also on the basis of emerging case law in the relevant field and various self-regulatory measures (such as standards, codes of good practice, etc.). This section provides a few examples of recent practices and regulatory updates that influence the overall compliance framework in the EU.

There are a significant number of recent guidelines related to cybersecurity requirements. For example, in 2025, ENISA published NIS2 Technical Implementation Guidance [16]. It is a manual providing technical advice and evidence examples for organizations to meet NIS2 standards. Furthermore, the EU Rolling Work Programme for certification outlines the strategic priorities for European cybersecurity certification, emphasizing the critical interplay between voluntary certification schemes and the mandatory requirements of the Cyber Resilience Act [17].

In 2026, the EC published draft guidance to assist companies in meeting the obligations of the Cyber Resilience Act [18], which focuses on remote data processing solutions and free and open-source software, the notion of ‘support periods’ as well as the interplay between the CRA and other EU legislation. Moreover, the EC is finalizing the Single Reporting Platform for vulnerability and incident reporting, which becomes mandatory in September 2026 [19]. The Single Reporting Platform provided for in the Cyber Resilience Act shall become a technical tool to use for the reporting of actively exploited vulnerabilities and incidents impacting products with digital elements operating in the EU Digital Single Market.

In 2026, the EC introduced the "Cybersecurity Package" to modernize the Cybersecurity Act [20], where it proposed updates to accelerate certification schemes. Key changes include expanding certification scope to include organizational risk management practices, not just products and strengthening ENISA’s role in managing an EU-wide early warning system for threats.

Furthermore, the European Commission adopted the implementing regulation concerning the EU cybersecurity certification scheme on Common Criteria (EUCC) [21]. Voluntary-based, the EUCC scheme allows ICT suppliers who wish to showcase proof of assurance to go through an EU commonly understood assessment process to certify ICT products such as technological components (chips, smartcards), hardware and software.

In the financial sector, the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority released a Guide on oversight activities [22]. The purpose of this guide is to explain the Critical Third-Party Providers oversight framework, including its objectives, underlying principles, structure, activities, implementing processes, and expected outcomes. Moreover, the European Central Bank finalized a guide clarifying expectations for banks regarding cloud outsourcing [23]. While not legally binding, it aligns with DORA’s ICT risk management requirements and provides "good practices" for risk-based oversight.

There is also significant guidance related to the AI Act requirements. For example, Guidelines from the Commission and ENISA on prohibited AI Practices, now provide clearer “red lines” necessary to operationalize these often high-level acts [24]. I.e., while the AI Act sets general rules, Guidelines build on them and detail further about prohibitions on AI systems that manipulate behavior (e.g., it is prohibited to use biometric data to create databases). In addition, the EU Apply AI Strategy directly encourages the creation of tools that “detect anomalies” and “analyze incidents,” aligning with the cybersecurity goals in critical infrastructure [25]. Such tools in the security sector will likely be classified as high-risk; therefore, additional requirements under the AI Act may apply to these systems.

Furthermore, the GDPR has an utmost importance to the development of cybersecurity systems. Following this, the European Commission (in close cooperation with ENISA and EDPB) is working on implementing the GDPR provisions in the area of cybersecurity. For example, ENISA Technical Implementation Guidance on NIS2 provides actionable advice on various parameters, including GDPR, to consider when implementing specific actions and requirements [16]. NIS2 and GDPR intersect to protect both digital infrastructure and personal data, requiring unified risk management. The EU Cloud Code of

Conduct (2020), prepared with reference to EDPB guidance, sets out requirements for Cloud Service Providers, including relevant provisions of the GDPR and applicable international standards, thereby facilitating their practical application and interpretation. EDPB case digest on Security of Processing and Data Breach Notification offers valuable insights on how data protection authorities have interpreted and applied GDPR provisions in diverse scenarios, such as hacking, ransomware, or accidental data disclosure [26].

Considering the sometimes ambiguous EU regulations and their national implementation, the implementation of guidance on recent practices is just as important as the rules directly resulting from regulations to ensure the market-standard operation of the developed systems.

Judicial interpretation is as critical as the legislation itself and recent policy practices.

For instance, the "SCHUFA Holding AG" case clarifies that algorithmic scoring constitutes automated decision-making under GDPR Article 22, thereby necessitating human intervention when significant consequences, such as blocking access, occur. These are the most critical sources for determining which data (e.g., IP addresses and traffic data) can be collected [27].

Furthermore, in the case “La Quadrature du Net”, CJEU ruled that Member States cannot mandate the general and indiscriminate retention of traffic and location data for preventive purposes unless there is a genuine threat to national security [28]. The Court allows automated analysis and real-time data collection only when a serious threat is shown to exist, provided that the criteria for analysis are specific, reliable, and non-discriminatory, and explicitly prohibit criteria based on sensitive attributes.

In addition, the CJEU case “Dun & Bradstreet” addresses transparency and automated decisions, or the so-called "Black Box" issue [29]. If the technology or software automatically decides that a certain traffic flow is a "threat" and blocks it, the user has the right to know the "logic involved" in the decision.

Following judicial guidance allows for the implementation of the rules established in the regulation in a more consistent and clearer manner.

B. CRITICAL INFRASTRUCTURE CYBERSECURITY

Critical infrastructure cybersecurity is increasingly governed by sector-specific standards that address the distinct risks of operational and safety-critical systems. The IEC 62443 series provides a comprehensive framework for securing Industrial Automation and Control Systems (ICS) through a lifecycle- and risk-based approach [8]. In the energy sector, the NERC Critical Infrastructure Protection (CIP) standards establish mandatory requirements for protecting bulk electric systems [30]. Similarly, ISO/SAE 21434 defines cybersecurity engineering practices for road vehicles across their lifecycle [31]. Together, these standards reflect a converging emphasis on risk management, system lifecycle security, and resilience against evolving cyber threats.

At the organization level, various frameworks have been proposed to help manage and reduce cybersecurity risks, including ISO/IEC 27001 [32], which provides a certifiable information security management system; the CIS Critical Security Controls, which focus on prioritized technical safeguards [33]; and NIST Cybersecurity Framework (CSF) 2.0 [7]. NIST CSF 2.0 is a widely adopted risk-management framework that is applicable to organizations of all sizes and sectors, and is organized around six core functions, which support cybersecurity risk management lifecycle: (1) Govern - defines the necessary policies, roles, risk-management framework, and oversight mechanisms that guide cybersecurity operations, supporting clear accountability and coherence with organizational goals; (2) Identify - helps organizations analyze their assets, risks, and dependencies to determine appropriate security priorities; (3) Protect - assigns measures that prevent cybersecurity incidents or reduce their impact, including access control, data protection, staff training, secure development practices, and protective technologies; (4) Detect - involves detecting anomalies, threats, and incidents through continuous monitoring and analysis; (5) Respond - covers actions taken after a detected cybersecurity incident to contain/reduce its impact, including analysis, communication, mitigation, and improvement efforts; (6) Recover - restores services after an incident and improves resilience through recovery planning, repairs, and lessons learned.

Organizations use CSF 2.0 as a flexible, outcome-oriented framework to assess cybersecurity maturity, define target security postures, and prioritize improvement initiatives. It supports the development of internal cybersecurity programs, enhances communication between technical and executive stakeholders, and aligns cybersecurity practices with regulatory and industry expectations. Profiles and implementation tiers allow organizations to tailor the framework to their operational context, resources, and risk tolerance.

Given the complexity of the applicable cybersecurity legislation for critical infrastructure, compliance with EU cybersecurity requirements is increasingly challenging. One illustrative example could be the requirements for security incident reporting – e.g., such obligations apply under NIS2, DORA, and the GDPR; therefore, critical infrastructure or financial entities are required to implement complex reporting solutions to navigate the maze of reporting obligations. Examples like this exist across many domains of the daily critical infrastructure operation; therefore, research questions and accompanying suggestions as provided in this paper are essential for more coherent and effective compliance.

C. CYBER THREAT CLASSIFICATION

Various models and frameworks have been proposed to support threat analysis, modelling, risk assessment, and classification of cyber threats, including MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) [9], Microsoft STRIDE framework [34], Damage, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD) [35], and NIST SP 800-154 [36], among others.

MITRE ATT&CK is the predominant framework, widely adopted across sectors such as government, academia, and industry, including critical infrastructure [37]. It enables the mapping of adversarial tactics, techniques, and procedures (TTPs) and enhances the systematic detection and analysis of cyber threats, particularly advanced persistent threats (APTs).

The MITRE ATT&CK framework is organized into three primary technology domains - Enterprise, Mobile, and Industrial Control Systems (ICS), which involve different tactics and techniques, representing the adversarial behaviors relevant to each domain [9]. It includes 94 techniques, grouped into several categories: initial access, execution, persistence, privilege escalation, evasion, discovery, lateral movement, collection, command and control, and inhibit response function. These techniques can be linked together to create an attack chain, which can be used to characterize cyberattacks.

Furthermore, the MITRE ATT&CK framework can be mapped to the NIST CSF to facilitate cybersecurity risk management in an organization. In [38], the authors proposed the Cyber Threat Dictionary (CTD), which links MITRE ATT&CK and NIST CSF and can be used to identify security gaps, map them to ATT&CK techniques, develop mitigation and detection techniques, prioritize vulnerabilities, and develop appropriate prevention solutions.

D. CYBER THREAT INTELLIGENCE SHARING

Rajamäki et al. refer to three main types of CTI – strategic, tactical and operational [39]. Strategic CTI is of high-level, which can provide organisations with an overview of the threat landscape; tactical CTI is aimed at technical audiences and focuses on indicators of compromise; operational CTI provides an overview of how different threat actors plan and execute their attacks and operations.

Janosek claims that the EU's approach to CTI sharing is built upon a triad of key regulations – NIS2 mandates a standard level of cybersecurity across critical sectors and facilitates voluntary threat information exchange, while DORA provides a more specific framework to ensure the operational continuity of the financial industry [40]. These frameworks operate under the strict data privacy requirements of the GDPR, which governs the lawful processing of any CTI that contains personal data.

Art. 29 of NIS2 directive establishes that EU Member States shall ensure that entities (in the scope of NIS2 and not) should be able to exchange on a voluntary basis relevant cybersecurity information [1]. Such sharing should aim to prevent, detect, etc. incidents and mitigate their impacts as well as enhance the level of cybersecurity, and should be done through arrangements which respect potentially sensitive nature of the information shared. According to NIS2, ENISA shall provide assistance for such information sharing.

The information sharing arrangements are also foreseen in Art. 45 of DORA [6]. DORA establishes that financial entities may exchange cyber threat information and intelligence among themselves. Such information sharing should aim to enhance the digital information resilience of financial entities, take place within trusted communities of financial entities, and be implemented through information-sharing arrangements that respect business confidentiality, protect personal data in accordance with the GDPR, and comply with competition policy. In other words, while DORA specifies which specific constraints should be taken into account (business confidentiality, data protection, competition), it can be assumed that at least the same approach should be taken under NIS2 considering the reference to 'potentially sensitive nature of information'.

In their paper Rajamäki et al. also focus on the GDPR's implications to CTI exchanges [39]. The authors establish that 'to conduct a CTI exchange involving GDPR-protected data, it is only legal in case data is necessary and the legal groundwork for sharing can be labelled as a legitimate interest.' They also claim that CTI sharing projects are recommended to prepare a data protection impact assessment (Art. 35 of the GDPR) and that CTI exchanges should anonymize identifiable data. As related to the GDPR, Janosek claims that CTI sharing should be structured to reduce or avoid the inclusion of personal data [40]. The suggested examples include, e.g., that reports can pseudonymize user identifiers by hashing emails or hostnames or by aggregating event details; instead of raw log lines detailing specific IPs, user identifiers, or exact timestamps, CTI reports might summarize activity per hour. Furthermore, MITRE ATT&CK threat classification can be considered as a ground-truth for CTI sharing among organizations.

CTI sharing is an integral part of NIST CSF 2.0 as well [7] and is implemented through its functions. As part of the "govern" function, policies for sharing threat intelligence with external partners, regulators, and industry groups to foster collaboration are established, in compliance with relevant regulations. Furthermore, in "identify" function, continuous threat data gathering is performed, using the threat information received from others, to identify new threat relevant to the organization and protect from them. Finally, once threats are detected ("detect" function), information is shared with other organizations ("respond" functions), in compliance with regulations ("govern" function).

Overall, while CTI sharing is an important requirement established in the EU legislation, it must be implemented in

a way that it does not undermine other applicable legislation and fundamental rights.

III. RELATED WORK ON AUTOMATED REGULATORY COMPLIANCE

Organizations face numerous challenges related to compliance with regulations, such as the abstract nature of regulations, conflicts with existing practices, the need for new expertise, lack of established principles and methods, regulatory complexity, resource demands, enforcement difficulties, evolving system dynamics, overlapping regulatory frameworks, organizational barriers, and regulatory gaps among others [41].

So far, the Regulatory Technologies (RegTech) that support organizations with regulatory compliance are primarily being developed for finance sector [42].

While Generative AI (GenAI) shows potential for compliance support, its current unreliability for standalone analysis, due to accountability issues and regulatory gaps, underscores the need for formal, structured methods like the one proposed here [43]. However, due to overlapping regulatory frameworks, existing regulatory gaps, and inconsistencies with current organizational practices, GenAI systems remain unreliable for standalone compliance analysis. Challenges related to liability and accountability also persist, particularly concerning responsibility for incorrect or incomplete outputs generated by AI. Moreover, frequent regulatory updates require continuous model retraining, and current standards are not yet fully aligned with GenAI capabilities. As a result, effective use of GenAI in compliance still requires substantial domain expertise [43].

The first step in automating regulatory compliance is to abstract and formally structure legal provisions into a machine-interpretable representation [44]. This involves extracting key concepts from legal texts to construct a model or ontology. These concepts then form the basis for defining compliance criteria. Once the legal knowledge is formalised, automated methods can support analysts in a range of compliance-related tasks.

Ontology-based Requirements Engineering (ObRE) represents a promising approach for advancing automation in regulatory compliance and automated requirements specification [45,46].

It has been recently applied for automating compliance with GDPR [47]; securing 5G network security ensuring compliance with EU cybersecurity requirements [48]; automating compliance with AI Act [49]; supporting security-by-design of industrial control systems by conforming with the IEC 62443 standard [50]; hybrid threat analysis [51,52].

A primary limitation of current ObRE implementations is their siloed nature: most existing frameworks focus exclusively on a single instrument (e.g., GDPR or IEC 62443) rather than on the intersectional requirements of critical infrastructure. In our previous work, we addressed this gap by proposing a methodology for specifying regulatory compliance requirements for dual-use AI systems [11]. The approach integrated legal and technical perspectives by structuring compliance obligations across deployment domains, system lifecycle stages, and requirement categories. As a result, an ontological framework was developed, capable of representing layered EU and defense governance structures within a unified semantic model.

The present work extends our previous research by integrating organization cybersecurity risk management frameworks (NIST CSF 2.0), cybersecurity standards (IEC 62443) and threat models (MITRE ATT&CK for ICS) into an ontological dual-use framework.

IV. METHODOLOGY

This study adopts an ontology-driven methodology to enable the formal integration and operationalization of regulatory compliance and cybersecurity requirements. The approach is grounded in semantic web technologies and proceeds through four main stages: knowledge acquisition, ontological modelling, semantic formalization, and instance-based validation.

A. KNOWLEDGE ACQUISITION AND INTEGRATION

The methodology adopts a four-domain integration approach, systematically identifying knowledge sources across: (A) cybersecurity risk management frameworks (e.g., NIST CSF 2.0); (B) regulatory frameworks (e.g., GDPR, NIS2, AI Act); (C) technical standards (e.g., IEC 62443-3-3); and (D) threat intelligence models (e.g., MITRE ATT&CK for ICS). As illustrated in Figure 1, these sources were selected to synthesize both organizational and technical dimensions of cybersecurity compliance. Key concepts and relationships were extracted and harmonized into a unified conceptual structure, with particular attention to linking regulatory obligations to operational cybersecurity constructs.

B. ONTOLOGICAL MODELLING

The extracted knowledge was formalized into an ontology using RDF and OWL. Core classes include Regulation, RegulatoryRequirement, CybersecurityFunction, SecurityControl, Asset, ThreatTechnique, and ThreatModel. Relationships between these classes were explicitly defined using object properties such as:

- imposesRequirement
- mapsToFunction
- implementedBy
- appliesTo
- mitigates

These relationships enable the propagation of regulatory requirements across governance, technical, and operational layers, forming a coherent semantic structure for compliance traceability.

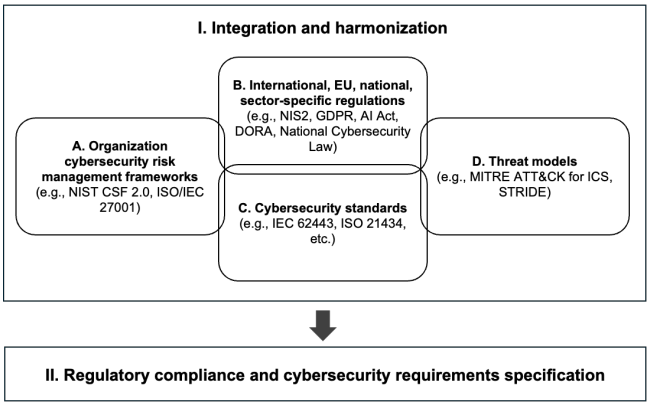

FIGURE 1. Ontological framework scope. Here, the integration of four domains is depicted: organizational cybersecurity risk management frameworks, regulations, cybersecurity standards, and threat models. These work together in support of regulatory compliance and the specification of cybersecurity requirements.

C. SEMANTIC FORMALIZATION AND IMPLEMENTATION

The ontology was encoded in RDF/Turtle and implemented within the Stardog knowledge graph platform (*https://cloud.stardog.com/*). Instance-level data were created to represent concrete linkages between regulations, requirements, controls, threat techniques, and assets.

SPARQL queries were used to retrieve and analyze traceability chains across the graph. The following query illustrates how a compliance-to-threat chain can be extracted:

```
PREFIX ircf: <https://purl.org/ircc-framework#>
SELECT ?regulation ?requirement ?function ?control ?threat ?asset
WHERE {
  ?regulation ircf:imposesRequirement ?requirement .
  OPTIONAL { ?requirement ircf:mapsToFunction ?function . }
  OPTIONAL { ?requirement ircf:implementedBy ?control . }
  OPTIONAL { ?control ircf:mitigates ?threat . }
  OPTIONAL { ?requirement ircf:appliesTo ?asset . }
}
LIMIT 20
```

This query retrieves linked entities across regulatory, functional, technical, and operational layers, demonstrating the ability to traverse the ontology in a structured, machine-interpretable manner.

1) REPRESENTATIVE RESULTS

Execution of the above query within the Stardog environment produced results consistent with the traceability structure illustrated in Figure 2. A representative result is shown in Table 1.

TABLE I
REPRESENTATIVE RESULTS

Regulation	Requirement	Function	Control	Threat	Asset
GDPR	Data Minimization	Protect	Network Monitoring Control	Remote Service Abuse	AI Based OT Sensor

This result demonstrates a complete traceability chain from a regulatory source to a specific threat context, with intermediate mappings to cybersecurity functions, technical controls, and operational assets.

2) INSTANCE-BASED VALIDATION

To validate the operationalization of the ontology, representative instances were constructed and queried to confirm the existence of coherent traceability chains. A typical instantiated chain follows the following structure, with additional mappings to cybersecurity functions and assets:

Regulation → *RegulatoryRequirement* → *SecurityControl* → *ThreatTechnique*

This structure is visualized in Figure 2, which presents a concrete example retrieved from the knowledge graph. The results confirm that the ontology supports machine-interpretable reasoning and enables consistent navigation across regulatory, technical, and threat intelligence domains.

V. INTEGRATED ONTOLOGICAL FRAMEWORK FOR AUTOMATING REGULATORY COMPLIANCE AND CYBERSECURITY REQUIREMENTS SPECIFICATION

The primary contribution of this work is an integrated ontological framework that bridges the gap between high-level regulatory compliance and low-level cybersecurity engineering in critical infrastructure. Unlike existing approaches that treat regulations, technical standards, and threat models in isolation, the proposed framework provides a unified semantic representation that links legal obligations (e.g., NIS2, GDPR, AI Act), organisational cybersecurity processes (NIST CSF 2.0), technical controls (IEC 62443), and adversarial behaviours (MITRE ATT&CK for ICS). By establishing a unified semantic model, the framework provides traceable, machine-interpretable links between legal obligations, operational controls, and specific adversarial behaviors, thereby supporting compliance-by-design and threat-informed requirements specification within a single coherent model.

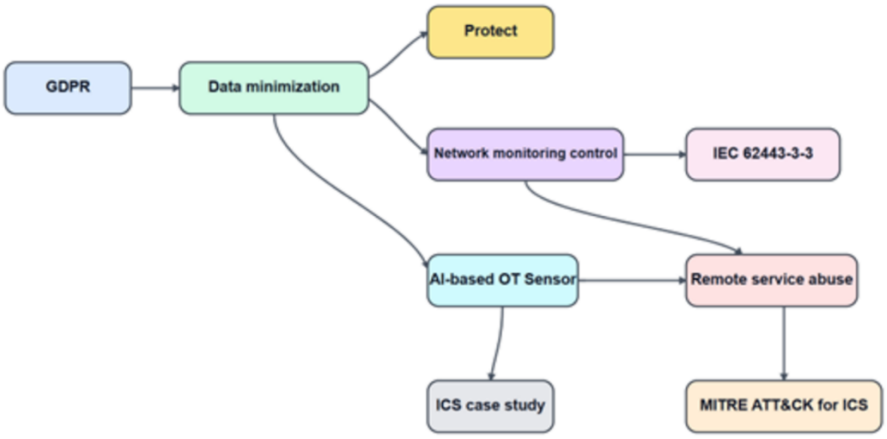

FIGURE 2. **Integrated regulatory compliance and cybersecurity framework: instance-level traceability chain.**

Figure 1 illustrates the high-level structure of the ontology, showing how regulatory sources, cybersecurity frameworks, technical standards, and threat models are represented as interconnected components within a unified semantic model. The figure highlights the role of the ontology as an integration layer that links abstract legal requirements to concrete technical controls and threat-informed security practices.

The proposed integrated ontological framework provides a machine-interpretable semantic layer that unifies regulatory requirements, cybersecurity frameworks, technical standards, and cyber-threat models relevant to critical infrastructure. Its primary purpose is to support automated regulatory compliance analysis and cybersecurity requirements specification by enabling traceability across legal, organizational, and technical domains.

The scope of the ontology includes selected EU regulatory instruments (notably NIS2, GDPR, and the AI Act), organizational cybersecurity risk-management frameworks (NIST CSF 2.0), technical cybersecurity standards (IEC 62443-3-3 [53], and threat classification models (MITRE ATT&CK for ICS). These sources are integrated into a single conceptual structure that allows requirements, controls, and threats to be analyzed in relation to one another rather than in isolation.

At the conceptual level, the ontology is structured around a set of core classes, including Regulation, RegulatoryRequirement, CybersecurityFramework, FrameworkFunction, TechnicalStandard, SecurityControl, Threat, Technique, Asset, Stakeholder, and ComplianceMeasure. These classes capture the principal entities required to represent regulatory obligations, organisational practices, technical safeguards, and threat scenarios in critical infrastructure environments.

The ontology further defines a set of semantic relations that enable cross-domain integration. These include relations such as imposesRequirement (linking regulations to specific obligations), appliesTo (linking requirements to systems or assets), mapsToFunction (aligning requirements and controls with NIST CSF functions), mitigates and detects (linking controls to threats), and supportsComplianceWith (linking technical and organizational measures to regulatory obligations). Together, these relations provide a structured basis for linking legal provisions to concrete cybersecurity measures and threat-informed contexts.

The ontology is designed to support formal representation and automated analysis, including query-based traceability and validation of compliance relationships. While the present work focuses on the conceptual integration, the model is structured to be compatible with semantic web technologies (e.g., RDF/OWL) and constraint-validation approaches, enabling future implementation of machine-assisted compliance checking and reasoning.

To illustrate the operationalization of the proposed ontology, Figure 2 presents a representative instance-level traceability chain retrieved from the Stardog knowledge graph, linking a regulatory requirement to cybersecurity functions, technical controls, threat techniques, and an operational asset. The figure illustrates a single end-to-end compliance-to-threat traceability chain instantiated within the proposed ontology. Starting from the General Data Protection Regulation (GDPR), a regulatory requirement such as data minimization is derived (*imposesRequirement*). This requirement is then propagated across multiple layers of the framework.

In the primary chain, the requirement is operationalised by a network monitoring control (*implementedBy*) aligned with the IEC 62443-3-3 standard, which in turn mitigates the threat technique "remote service abuse" as defined in the MITRE ATT&CK for ICS knowledge base (mitigates). This establishes a direct linkage from regulatory obligation to concrete threat mitigation.

In parallel, the same requirement is mapped to the "Protect" function of the NIST Cybersecurity Framework (CSF) 2.0 (*mapsToFunction*), situating it within a recognised governance structure. It is also applied to an AI-based OT sensor deployed within an ICS illustrative scenario in Section

6 (*appliesTo)*, demonstrating how regulatory requirements extend to operational assets and detection capabilities.

Together, these relationships instantiate a coherent semantic chain of the form, with additional mappings to cybersecurity functions and system assets:

Regulation → Requirement → Control → Threat Mitigation

These relationships are formally represented in RDF/Turtle and can be queried via SPARQL within the Stardog environment, enabling machine-interpretable traceability from legal obligations to technical implementation and threat context.

This integrated representation enables a shift from fragmented compliance analysis toward a unified, traceable model in which regulatory requirements, cybersecurity controls, and threat scenarios can be systematically aligned. As a result, the ontology provides a foundation for compliance-by-design approaches that incorporate threat-informed security considerations from the outset.

VI. FRAMEWORK APPLICATION EXAMPLE

This section presents an illustrative critical infrastructure scenario in which an AI-based Operational Technology (OT) sensor is deployed to monitor network activity and detect anomalous behavior in ICS. It demonstrates how regulatory requirements are propagated through the proposed ontology to cybersecurity functions, technical controls, and threat mitigation mechanisms, as illustrated in Figure 2.

A. INITIAL ONTOLOGICAL APPLICATION

Within the ontology, relevant regulatory frameworks such as the General Data Protection Regulation (GDPR) and the AI Act are instantiated as Regulation entities. These give rise to specific RegulatoryRequirement instances, including data minimization, human oversight, and security by design (imposesRequirement). These requirements are then associated with the monitored asset, represented as the AI-based OT sensor (appliesTo), reflecting the operational context in which compliance obligations must be satisfied.

Each requirement is mapped to one or more functions of the NIST CSF 2.0 (mapsToFunction), such as “Protect” and “Detect.” These functions provide a structured linkage between regulatory obligations and cybersecurity practices. The requirements are further connected to concrete SecurityControl instances (implementedBy), including network monitoring controls and anomaly detection controls, which operationalize the regulatory constraints within the ICS environment.

The security controls are, in turn, linked to relevant threat techniques derived from the MITRE ATT&CK framework for ICS (mitigates), such as remote service abuse and command manipulation. Together, these relationships form a coherent compliance-to-threat traceability chain spanning regulatory sources, requirements, functions, controls, and threats, as visually represented in Figure 2.

To examine how regulatory requirements propagate to the monitored asset, a targeted SPARQL query was formulated to retrieve requirements applied to the AI-based OT sensor, along with their associated cybersecurity functions, implementation controls, and mitigation techniques. An example query is shown below:

```
PREFIX irccf: <https://purl.org/ircc-framework#>
SELECT ?requirement ?function ?control ?threat
WHERE {
 ?requirement irccf:appliesTo irccf:OTSensor .
 OPTIONAL { ?requirement irccf:mapsToFunction ?function . }
 OPTIONAL { ?requirement irccf:implementedBy ?control . }
 OPTIONAL { ?control irccf:mitigates ?threat . }
}
ORDER BY ?requirement ?function ?control ?threat
```

The query results are summarized in Table 2 and correspond directly to the traceability structure depicted in Figure 2.

TABLE II
SPARQL QUERY RESULTS FOR OT SENSOR–CENTERED COMPLIANCE TRACEABILITY

Requirement	Function	Control	Threat
Data Minimization	Protect	Network Monitoring Control	Remote Service Abuse
Human Oversight	Detect	Anomaly Detection Control	Command Manipulation
Security By Design	Protect	Anomaly Detection Control	Command Manipulation

Execution of this query produced multiple traceability chains linking regulatory requirements to cybersecurity functions, technical controls, and associated threat techniques. The results show that the data minimization requirement is mapped to the “Protect” function and implemented through a network monitoring control, which mitigates the threat technique “remote service abuse.” In addition, the requirements of human oversight and security by design are associated with the cybersecurity functions (“Detect” and “Protect,” respectively) and are implemented through an anomaly-detection control that mitigates the threat technique “command manipulation.”

Notably, these results reveal convergence across regulatory requirements, where multiple requirements are operationalized through shared controls and mitigation strategies. This indicates that distinct regulatory obligations may be implemented through common technical mechanisms, reflecting practical constraints and design patterns within ICS environments. This convergence is also evident in Figure 2, where different requirement paths converge on shared control and threat mitigation nodes.

Such patterns are not explicitly defined within individual regulatory or cybersecurity frameworks but emerge through the integrated ontological representation and can be

systematically retrieved using SPARQL. This demonstrates the analytical value of the proposed approach in enabling structured, asset-centered analysis of compliance and cybersecurity relationships within ICS environments.

The preceding scenario discussion demonstrated the proposed traceability methodology using two representative threat techniques. However, a realistic ICS deployment faces the full breadth of the adversarial landscape documented in the MITRE ATT&CK for ICS knowledge base, which comprises 94 techniques organized across 12 tactics representing distinct phases of an industrial control system attack chain. To evaluate the scalability and analytical capacity of the proposed ontological framework, the ICS scenario was extended to incorporate the complete ATT&CK ICS matrix.

B. ONTOLOGICAL EXTENSION

To enable systematic integration of the ATT&CK ICS matrix, a new class – Tactic – was introduced into the ontology, together with a corresponding object property belongsToTactic linking individual threat techniques to their parent tactics. All 12 ICS tactics were instantiated using their canonical MITRE identifiers (TA0100–TA0111), and each was linked to the MITRE ATT&CK for ICS threat model via the existing belongsToThreatModel property.

Critically, each tactic was mapped to one or more NIST CSF 2.0 functions via the mapsToFunction property. This tactic-to-function mapping establishes the semantic bridge between the threat model and the regulatory compliance structure already represented in the ontology, enabling the propagation of regulatory requirements to threat techniques through shared cybersecurity governance functions rather than requiring individual technique-level mappings.

Figure 3 presents the extended class-level schema of the ontology as visualized within the Stardog knowledge graph environment. The schema illustrates the structural role of the Tactic class as an intermediary between ThreatTechnique and FrameworkFunction, enabling tactic-mediated regulatory traceability. The principal chain

Regulation → RegulatoryRequirement → SecurityControl → ThreatTechnique → Tactic

is visible as a connected path across the graph, with SecurityControl additionally linked to TechnicalStandard (IEC 62443-3-3) via belongsToStandard, and FrameworkFunction linked to CybersecurityFramework (NIST CSF 2.0) via belongsToFramework. The AIEnabledSystem subclass of Asset is linked to ThreatTechnique via the detects property, representing the operational detection capabilities of the AI-based OT sensor within the ICS scenario.

The ontology was further extended with six additional regulatory requirements – risk management, vulnerability handling, supply chain security, business continuity, access control, and transparency obligation – reflecting provisions from NIS2, the AI Act, GDPR, and the Cyber Resilience Act (CRA). Nine additional IEC 62443-3-3 security controls were introduced, including access control enforcement (SR 1.1), use control authorization (SR 2.1), system integrity (SR 3.4), data confidentiality (SR 4.1), network segmentation (SR 5.1), audit logging (SR 2.8), communication integrity (SR 3.1), resource availability (SR 7.1), backup and recovery (SR 7.3), and input validation (SR 3.5). These controls were linked to threat techniques via mitigates and to regulatory requirements via implementedBy, completing the control-mediated traceability paths.

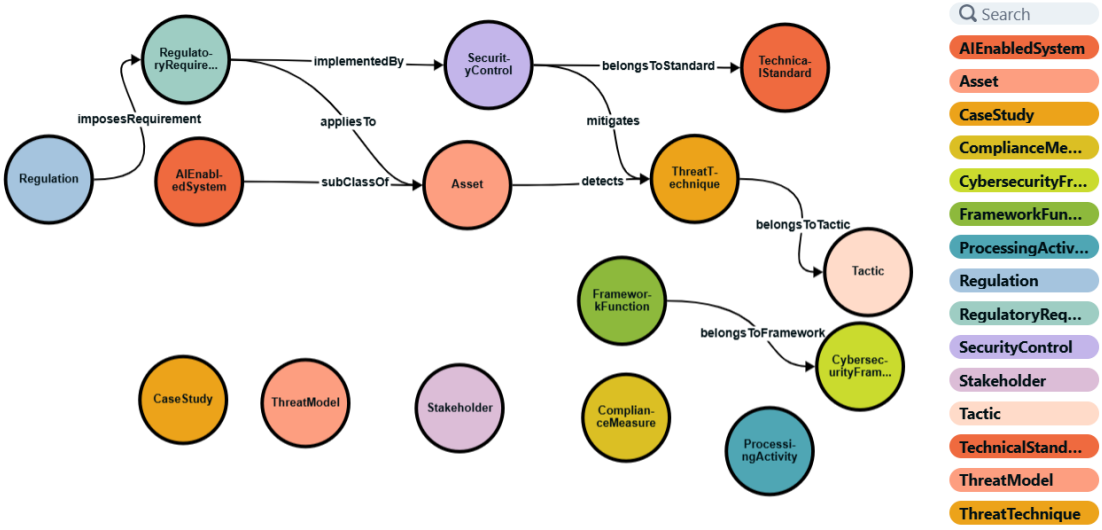

FIGURE 3. Extended class-level schema of the integrated ontological framework, retrieved from the Stardog knowledge graph. The Tactic class bridges ThreatTechnique instances from the MITRE ATT&CK for ICS matrix to FrameworkFunction instances from NIST CSF 2.0, enabling tactic-mediated regulatory traceability across the complete ICS attack chain. Fourteen core classes and their semantic relationships are shown, including the regulatory compliance chain (Regulation → RegulatoryRequirement → SecurityControl → ThreatTechnique) and the governance alignment chain (FrameworkFunction → CybersecurityFramework).

Table 3 presents the mapping between the 12 MITRE ATT&CK for ICS tactics and NIST CSF 2.0 functions. This mapping constitutes the primary integration surface through which regulatory requirements propagate to threat techniques.

TABLE III
TACTIC-TO-FUNCTION MAPPING

Tactic (MITRE ATT&CK ICS)	NIST CSF 2.0 Function(s)	Primary Regulatory Triggers
Initial Access (TA0108)	Protect, Detect	NIS2 Access Control; CRA Security by Design
Execution (TA0104)	Protect, Detect	AI Act Security by Design; NIS2 Access Control; AI Act/GDPR Human Oversight
Persistence (TA0110)	Protect, Detect	CRA Vulnerability Handling; AI Act Security by Design; NIS2 Access Control
Privilege Escalation (TA0111)	Protect	NIS2 Access Control
Evasion (TA0103)	Detect	AI Act/GDPR Human Oversight
Discovery (TA0102)	Detect, Identify	NIS2/AI Act Risk Management
Lateral Movement (TA0109)	Protect, Detect	NIS2 Access Control
Collection (TA0100)	Detect, Protect	GDPR Data Minimization; AI Act/GDPR Human Oversight
Command and Control (TA0101)	Detect, Protect	GDPR Data Minimization
Inhibit Response Function (TA0107)	Respond, Recover, Detect	AI Act/GDPR Human Oversight; NIS2 Business Continuity
Impair Process Control (TA0106)	Detect, Respond	AI Act/GDPR Human Oversight
Impact (TA0105)	Respond, Recover	NIS2 Business Continuity; NIS2 Incident Reporting; CRA Incident Reporting

C. EXTENDED SPARQL QUERY

Consider the following query:

```
PREFIX ircf: <https://purl.org/ircc-framework#>
SELECT ?regulation ?requirement ?function ?tactic
?technique ?control
WHERE {
 ?regulation ircf:imposesRequirement ?requirement .
 ?requirement ircf:mapsToFunction ?function .
 ?requirement ircf:implementedBy ?control .
 ?control ircf:mitigates ?technique .
 ?technique ircf:belongsToTactic ?tactic .
 ?tactic ircf:mapsToFunction ?function .
}
ORDER BY ?tactic ?regulation
```

To retrieve fully grounded traceability chains spanning from regulatory sources to specific threat mitigations, the SPARQL query was formulated. Unlike the asset-centered query presented in Section 6.1, this query exploits the tactic layer to join the regulatory and threat sides of the ontology through shared NIST CSF functions, requiring every link in the chain to be present.

Execution of this query within the Stardog environment produced 71 fully grounded traceability chains spanning all 12 tactics and all four regulatory instruments. Table 4 presents a curated subset of representative results, selected to illustrate distinct regulatory pathways, control mechanisms, and tactic phases.

D. REGULATORY DENSITY ANALYSIS

Table 5 summarizes the distribution of fully grounded traceability chains across tactics and regulations, revealing differential regulatory density across phases of the ICS attack chain.

Several analytical observations emerge from these results. First, the distribution of traceability chains across the attack chain is markedly uneven. Execution and Persistence account for 31 of the 71 chains (44%), reflecting the concentration of Protect-function requirements from multiple regulatory instruments (AI Act, CRA, NIS2) converging on these early- and mid-chain phases.

TABLE IV
REPRESENTATIVE FULLY GROUNDED TRACEABILITY CHAINS

Regulation	Requirement	Function	Tactic	Technique	Control
GDPR	Data Minimization	Protect	Collection	Screen Capture (T0852)	Data Confidentiality
GDPR	Data Minimization	Protect	Collection	Adversary-in-the-Middle (T0830)	Network Monitoring
GDPR	Data Minimization	Protect	Command and Control	Commonly Used Port (T0885)	Network Monitoring
NIS2	Risk Management	Identify	Discovery	Network Sniffing (T0842)	Network Monitoring
AI Act	Human Oversight	Detect	Evasion	Spoof Reporting Message (T0856)	Anomaly Detection
GDPR	Human Oversight	Detect	Evasion	Indicator Removal on Host (T0872)	Audit Logging
NIS2	Access Control	Protect	Execution	Command-Line Interface (T0807)	Use Control Authorization
CRA	Vulnerability Handling	Protect	Execution	Scripting (T0853)	Input Validation
AI Act	Security by Design	Protect	Execution	Modify Controller Tasking (T0821)	Anomaly Detection
NIS2	Access Control	Protect	Initial Access	External Remote Services (T0822)	Access Control Enforcement
AI Act	Human Oversight	Detect	Impair Process Control	Unauthorized Command Message (T0855)	Anomaly Detection
NIS2	Business Continuity	Recover	Inhibit Response Function	Denial of Service (T0814)	Resource Availability
GDPR	Human Oversight	Detect	Inhibit Response Function	Alarm Suppression (T0878)	Anomaly Detection
NIS2	Access Control	Protect	Lateral Movement	Default Credentials (T0812)	Access Control Enforcement
NIS2	Access Control	Protect	Persistence	Valid Accounts (T0859)	Access Control Enforcement
CRA	Security by Design	Protect	Persistence	Module Firmware (T0839)	System Integrity
NIS2	Business Continuity	Recover	Impact	Loss of Availability (T0826)	Backup and Recovery

By contrast, Impact – representing the phase at which physical consequences such as loss of safety, damage to property, and loss of availability materialize – is supported by only a single fully grounded chain. This asymmetry suggests that the current regulatory landscape provides denser prescriptive coverage for preventive measures than for recovery and response.

Second, regulatory convergence is observable at the technique level. Techniques such as Change Operating Mode (T0858) and Modify Controller Tasking (T0821) are each reached by multiple regulatory pathways – AI Act Security by Design, AI Act Human Oversight, CRA Security by Design, and GDPR Human Oversight – through distinct requirement-function combinations. This convergence, in which different regulatory instruments independently mandate controls addressing the same adversarial behavior, is not explicitly stated in any individual regulation but emerges through the integrated ontological representation.

Third, the Evasion tactic presents a noteworthy tension. Techniques such as Alarm Suppression (T0878), Spoof Reporting Message (T0856), and Indicator Removal on Host (T0872) specifically target an operator's ability to maintain situational awareness, which is precisely the capability that the AI Act's human oversight requirement (Article 14) is designed to preserve. The ontology captures this relationship through the Detect function, but the regulatory density for Evasion remains lower than for Execution or Persistence, suggesting a potential area for future regulatory refinement.

Fourth, the analysis reveals structural dependencies on specific controls. The Anomaly Detection Control carries the majority of Human Oversight chains across four tactics (Evasion, Execution, Impair Process Control, and Inhibit Response Function). A failure or compromise of this single control would simultaneously affect compliance obligations across GDPR and the AI Act for multiple attack phases, representing a concentrated compliance risk that is visible only through the integrated ontological analysis.

These findings demonstrate that the proposed ontological framework scales effectively from illustrative two-technique demonstrations to comprehensive matrix-level coverage, and that the tactic-mediated integration approach enables systematic, machine-interpretable regulatory analysis across the full ICS threat landscape.

VII. DISCUSSION

This section discusses the contributions, analytical findings, and limitations.

A. FRAMEWORK CONTRIBUTIONS

The central contribution of this work is methodological: the demonstration that regulatory requirements, organizational cybersecurity frameworks, technical standards, and threat models can be formally integrated within a single ontological representation, enabling machine-interpretable traceability across domains that are conventionally treated in isolation. While existing studies have applied ObRE to isolated instruments such as the GDPR, the AI Act, or IEC 62443, they typically lack formal linkages among them. This framework addresses that gap by providing a unified semantic layer where obligations from NIS2, GDPR, the AI Act, and the CRA are co-represented alongside NIST CSF 2.0 functions, IEC 62443-3-3 controls, and MITRE ATT&CK for ICS threat techniques. This enables a level of cross-regulatory traceability that no individual standard provides in isolation.

The introduction of the Tactic class as an intermediary between individual threat techniques and NIST CSF 2.0 functions proved to be a structurally significant design decision. Rather than requiring individual technique-to-requirement mappings – which would be both labour-intensive and brittle in the face of framework updates – the tactic layer provides a stable integration surface through which regulatory requirements propagate to techniques via shared cybersecurity governance functions. This tactic-mediated architecture enables the framework to absorb the full 94-technique, 12-tactic ATT&CK ICS matrix without requiring proportional growth in the number of explicit regulatory linkages.

TABLE V
DISTRIBUTION OF FULLY GROUNDED TRACEABILITY CHAINS BY TACTIC

Tactic	Total Chains	Regulations Involved
Execution	17	AI Act, CRA, GDPR, NIS2
Persistence	14	AI Act, CRA, NIS2
Evasion	8	AI Act, GDPR
Collection	7	GDPR
Inhibit Response Function	6	AI Act, GDPR, NIS2
Impair Process Control	6	AI Act, GDPR
Discovery	4	AI Act, NIS2
Initial Access	3	AI Act, CRA, NIS2
Command and Control	2	GDPR
Lateral Movement	1	NIS2
Privilege Escalation	1	NIS2
Impact	1	NIS2
Total	**71**	

The framework's implementation within the Stardog knowledge graph platform confirmed that the ontological structure supports practical SPARQL-based querying for compliance analysis. Queries ranging from simple asset-centred traceability (Section 6.1) to comprehensive tactic-mediated retrieval across the full threat matrix (Section 6.1.1) were executed successfully, producing structured, interpretable results that link regulatory provisions to specific threat mitigations through documented intermediary relationships.

B. ICS APPLICATION SCENARIO: ANALYTICAL FINDINGS

The ICS scenario progressed through two levels of analysis. At the initial level (Section 6.A), three fully grounded traceability chains were demonstrated, linking GDPR and AI Act requirements to two threat techniques via NIST CSF 2.0

functions and IEC 62443-3-3 controls. These results confirmed the basic viability of the ontological integration approach and illustrated the convergence of regulatory requirements through shared technical controls.

At the extended level (Section 6.B), the incorporation of the complete MITRE ATT&CK for ICS matrix yielded 71 fully grounded traceability chains spanning all 12 tactics, all four regulatory instruments, and 11 IEC 62443-3-3 security controls. This extension revealed several findings that would not be visible through analysis of any single framework or regulation in isolation.

1) REGULATORY ASYMMETRY ACROSS THE ATTACK CHAIN

The distribution of traceability chains is markedly uneven across attack phases. Execution and Persistence collectively account for 44% of all chains (31 of 71), reflecting the convergence of multiple Protect-function requirements from the AI Act, CRA, and NIS2. In contrast, Impact – the phase at which physical consequences such as loss of safety, damage to property, and denial of control materialise – is supported by only a single fully grounded chain:

NIS2 Business Continuity → Recover → Loss of Availability

This asymmetry indicates that the current EU regulatory landscape provides substantially denser prescriptive coverage for preventive and protective measures than for recovery and consequence management in ICS environments. While NIS2 Article 21 establishes incident-handling and business-continuity obligations, these are not supported by the same depth of control-to-threat specificity that characterises the prevention-oriented requirements. The CER Directive [5], which addresses the resilience of critical entities, may partially address this gap; however, its integration into the ontological framework remains a task for future work.

2) REGULATORY CONVERGENCE AT THE TECHNIQUE LEVEL

Several techniques are reached by multiple independent regulatory pathways. For example, Modify Controller Tasking (T0821) and Change Operating Mode (T0858) are each addressed by four distinct chains originating from three regulations (AI Act, CRA, GDPR) through two different requirement-function combinations:

Security by Design → Protect;
Human Oversight → Detect

This convergence – in which distinct legislative instruments independently mandate controls for the same adversarial behavior – is not codified within any individual regulation but emerges through the integrated ontological representation. From a compliance engineering perspective, such convergence provides natural reinforcement: organizations that implement controls addressing these techniques simultaneously satisfy obligations arising from multiple regulatory sources. The ontology makes this reinforcement explicit and queryable.

3) EVASION AND HUMAN OVERSIGHT

The Evasion tactic presents a notable tension within the regulatory structure. Techniques such as Alarm Suppression (T0878), Spoof Reporting Message (T0856), and Indicator Removal on Host (T0872) are specifically designed to undermine an operator's situational awareness, which is precisely the capability that the AI Act's human oversight requirement (Article 14) seeks to preserve. The ontology captures this adversarial relationship through the Detect function, linking Human Oversight requirements to evasion techniques via anomaly detection and audit logging controls. However, the regulatory density for Evasion (8 chains across two regulations) is substantially lower than that for Execution (17 chains across four regulations), despite the direct functional antagonism between evasion techniques and human oversight obligations. This suggests a potential area for future regulatory refinement, particularly as AI-enabled detection systems become more prevalent in critical infrastructure and the adversarial targeting of oversight capabilities becomes an increasingly relevant attack vector.

4) SINGLE-CONTROL DEPENDENCY RISK

The Anomaly Detection Control carries the majority of Human Oversight traceability chains across four tactics (Evasion, Execution, Impair Process Control, and Inhibit Response Function). If this control is compromised or degraded, the corresponding human oversight obligations under both GDPR and the AI Act would be simultaneously undermined across multiple attack phases. This concentration represents a structural compliance risk that is not apparent from examination of individual regulations or standards but becomes visible through the integrated ontological analysis. From a design perspective, this finding supports the principle that compliance architectures for ICS environments should avoid monoculture in control implementation – a recommendation consistent with the defence-in-depth philosophy underlying both IEC 62443 and NIST CSF 2.0, but here substantiated with specific, queryable evidence from the regulatory-threat integration.

C. LIMITATIONS

Several limitations of the current work should be acknowledged.

First, the framework provides a static snapshot of a highly dynamic landscape. As EU regulations and CJEU case law evolve the ontology currently requires manual revision to remain up to date.

Second, the scope of the threat model integration is limited to a single domain – MITRE ATT&CK for ICS. The Enterprise and Mobile matrices, which are relevant to the IT environments that typically interface with ICS networks and through which initial access is frequently obtained, are not

represented. The omission of cross-domain attack paths – for example, an adversary gaining initial access through an Enterprise technique before pivoting to an ICS environment – limits the framework's ability to model realistic multi-stage attack scenarios.

Third, the framework does not currently employ constraint validation mechanisms, such as SHACL (Shapes Constraint Language), to enforce structural or semantic integrity rules. While the SPARQL queries demonstrate successful retrieval of traceability chains, they do not verify that all required relationships are present for a given regulatory scenario or that the instantiated data conform to expected patterns. The absence of SHACL-based validation can lead to structural gaps or inconsistencies in the knowledge graph going undetected.

Fourth, the tactic-to-function mapping, while analytically productive, involves interpretive judgments. The assignment of tactics to NIST CSF functions is not formally standardised; although prior work on the Cyber Threat Dictionary [38] has established precedent for ATT&CK-to-CSF alignment, the specific mapping used in this work reflects the authors' assessment of functional correspondence and may be subject to alternative interpretations.

Fifth, the control-to-technique mitigation links are modelled at a general level, reflecting the system requirement categories of IEC 62443-3-3 rather than specific sub-requirements or implementation guidance. A more granular treatment would strengthen the prescriptive value of the traceability chains but would substantially increase the complexity and maintenance burden of the ontology.

Sixth, the illustrative scenario, provided in Section 6, while demonstrating the framework's structural capabilities, has not been validated in operational settings with critical infrastructure organisations. Field validation would be necessary to assess the approach's practical utility for compliance analysts and security engineers in real-world environments.

VIII. FUTURE WORK

The proposed framework will be further evaluated and enhanced. This section describes the possible application of the framework to support CTI sharing among critical infrastructure organizations and highlights future research directions.

A. APPLICATION OF PROPOSED FRAMEWORK TO SUPPORT CTI SHARING AMONG CRITICAL INFRASTRUCTURE ORGANIZATIONS

The application of the framework to Cyber Threat Intelligence (CTI) sharing demonstrates its versatility beyond the ICS domain. The ontology formally maps the inherent regulatory tension between NIS2 Article 29, which encourages broad information exchange, and GDPR Article 5, which mandates data protection principles including data minimization. By linking the CTI platform to both requirements, the framework provides compliance analysts with a structured tool to navigate these conflicting mandates during Data Protection Impact Assessments (DPIAs). Within the ontology, the NIS2 Directive and the General Data Protection Regulation (GDPR) are instantiated as Regulation entities. NIS2 gives rise to an incident reporting requirement (*imposesRequirement*), while GDPR similarly imposes data minimization and data breach reporting requirements. Together, these requirements form the basis for subsequent semantic propagation across the framework.

The incident reporting requirement is mapped to the "Respond" function of the NIST Cybersecurity Framework (CSF) 2.0 (*mapsToFunction*), situating it within an established cybersecurity governance structure. In parallel, the data minimization requirement is applied to a CTI sharing platform (appliesTo), reflecting constraints on the handling and dissemination of sensitive threat information.

The CTI sharing platform is further linked to the process of threat intelligence sharing, which is associated with a critical infrastructure organization. This establishes a chain connecting regulatory obligations to organizational participation in information-sharing activities. The platform is also contextualized within this CTI scenario, representing its deployment in an operational scenario.

Using SPARQL queries over the instantiated knowledge graph, these relationships can be retrieved as a coherent traceability structure linking regulations, requirements, functions, platforms, processes, and organizational entities.

To demonstrate the generality of the proposed ontology beyond the ICS monitoring scenario, described in Section 6, Figure 4 presents a representative instance-level traceability chain for a CTI sharing environment. In contrast to the compliance-to-threat chain illustrated in Figure 2, this example focuses on the propagation of regulatory requirements across governance, platform, and organizational layers within an information-sharing context.

The figure, derived from instantiated RDF data and retrieved via SPARQL queries in the Stardog environment, illustrates how requirements imposed by regulatory frameworks are mapped to cybersecurity functions and applied to operational platforms and processes.

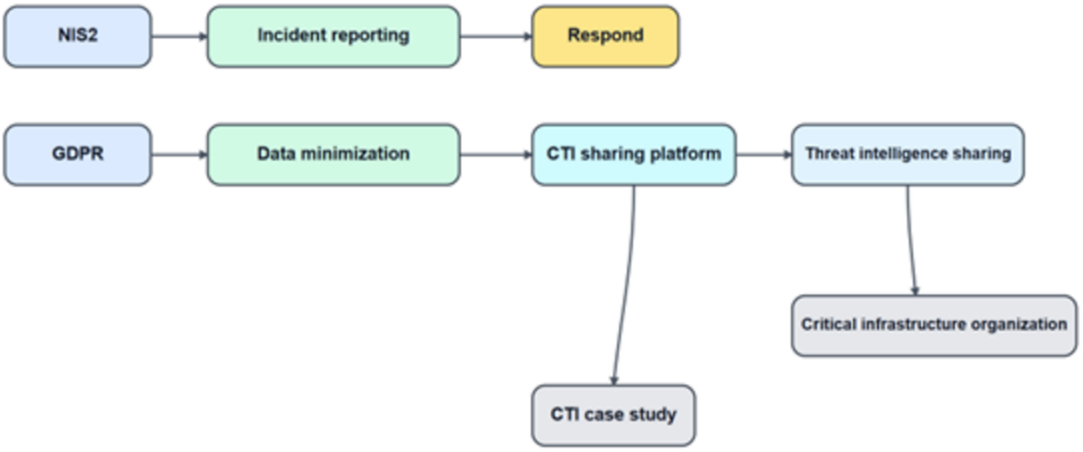

FIGURE 4. **Integrated regulatory compliance and cybersecurity framework: CTI-sharing traceability chain.**

Figure 4 presents an instance-level traceability chain for a CTI sharing scenario. The NIS2 Directive and GDPR are instantiated as regulatory sources that impose requirements (*imposesRequirement*), namely incident reporting and data minimization. The incident reporting requirement is aligned with the "Respond" function of the NIST Cybersecurity Framework (*mapsToFunction*), while the data minimization requirement is applied to a CTI sharing platform (*appliesTo*).

The inclusion of data minimization is critical here because CTI often contains information that could identify a natural person, such as IP addresses, hostnames, and metadata which, therefore, is considered personal data. While NIS2 Article 29 encourages the broad exchange of cybersecurity information to enhance collective resilience, GDPR Article 5 mandates that the processing of such personal data be limited to what is strictly necessary. By mapping this requirement directly to the CTI sharing platform node, the framework enables compliance analysts to verify that the platform's technical architecture supports the privacy-preserving measures during inter-organizational exchange.

The platform is linked to the process of threat intelligence sharing, which is associated with a critical infrastructure organization, representing the operational context in which information exchange occurs. The platform is further situated within a CTI case study, illustrating its deployment in a concrete scenario.

Together, these relationships demonstrate how regulatory obligations are propagated across governance, platform, processing, and organizational layers.

The application of the framework to CTI sharing illustrates its ability to make inherent regulatory tensions formally navigable. Specifically, it captures the conflict between NIS2 Article 29, which encourages broad, voluntary information exchange, and GDPR Article 5, which mandates that personal data be limited to what is strictly necessary. By linking the CTI platform to both requirements simultaneously, the framework enables compliance analysts to identify which constraints apply to a given operational context, thereby directly supporting the preparation of Data Protection Impact Assessments (DPIAs) as recommended by Rajamäki et al. (2024) and mandated under GDPR Article 35. Furthermore, as B. Al-Sada (2025) notes, the MITRE ATT&CK framework is an increasingly standard vocabulary for CTI exchange, and our proposed ontology provides the formal semantic foundation for sharing intelligence while maintaining strict traceability to the regulatory constraints governing such activities.

B. FUTURE RESEARCH DIRECTIONS

While the current framework establishes a robust semantic foundation for integrated requirements specification, its long-term operational efficacy depends on its ability to adapt to an increasingly volatile regulatory and adversarial landscape. To advance this research toward a fully automated, resilient compliance ecosystem, the following strategic directions are proposed:

- *SHACL Constraint Layers:* Introducing SHACL shapes to enforce ontological integrity and completeness of compliance is an immediate priority to verify that every regulatory requirement linked to an asset has at least one implementing control.
- *Automated Regulatory Update Ingestion:* We plan to develop semi-automated methods using Natural Language Processing (NLP) to incorporate regulatory updates, including new legislation, implementing acts, and CJEU rulings, to address the static nature of the current implementation.
- *Cross-Domain Threat Model Integration:* Extending the framework to incorporate MITRE ATT&CK Enterprise and Mobile matrices will enable the modelling of cross-domain attack paths that reflect

realistic adversarial campaigns targeting critical infrastructure through IT/OT convergence points.

- *Operational Validation:* Collaborative engagement with critical infrastructure operators will enable field validation of the framework's practical utility for compliance gap analysis, audit preparation, and threat-informed security architecture design.
- *Sector-Specific Instantiation:* We intend to explore domain-specific extensions for energy, transport, and health, incorporating unique regulations and threat profiles for each NIS2-defined critical sector.

IX. CONCLUSION

This paper has presented an integrated ontological framework that bridges the persistent gap between regulatory compliance and cybersecurity engineering in critical infrastructure environments. By formally unifying the selected EU regulatory instruments (NIS2, GDPR, the AI Act, and the CRA), organizational cybersecurity risk management (NIST CSF 2.0), sector-specific technical standards (IEC 62443-3-3), and threat classification (MITRE ATT&CK for ICS) within a single RDF/OWL ontology, the framework enables machine-interpretable traceability from legal obligations to concrete mitigations, a capability that no individual standard provides in isolation.

The introduction of a tactic-mediated integration architecture proved central to the framework's scalability, allowing regulatory requirements to be systematically propagated across the full 94-technique ICS threat matrix without requiring individual technique-level annotations. The resulting 71 fully grounded traceability chains revealed analytically significant patterns: a structural regulatory asymmetry in density across attack phases, the convergence of independent regulatory instruments on shared technical controls, and the concentrated compliance risk arising from single-control dependencies.

Beyond internal monitoring, applying the framework to support CTI sharing further demonstrated its versatility. The formal co-representation of NIS2 information-sharing provisions and GDPR data minimization constraints within a single semantic model provides a navigable structure for the regulatory tensions inherent in threat intelligence exchange, tensions that will intensify as CTI sharing matures across critical sectors.

The framework is designed for extensibility, with a modular structure that accommodates additional regulations (including the proposed Digital Omnibus), additional threat models, and constraint validation mechanisms such as SHACL. Ultimately, this work demonstrates that regulatory compliance in critical infrastructure can move beyond a manual, administrative burden. Ontology-based integration provides the formal semantic infrastructure to align legal requirements with operational reality, establishing compliance-by-design as a rigorous engineering discipline.

ACKNOWLEDGMENT

In preparing this manuscript, we acknowledge the limited use of a generative AI tool (*Microsoft Copilot – no version number provided by the tool*) solely to improve readability, grammar, and language clarity, and to troubleshoot citation manager formatting and bibliography consistency issues (e.g., Zotero). All AI-assisted use occurred under direct human oversight.

No generative AI tool was used to generate scientific content, perform conceptual analysis, interpret evidence, determine inclusion or exclusion decisions, or contribute to the theoretical, methodological, or empirical arguments of the manuscript.

All AI-assisted text was reviewed and edited using a human-in-the-loop approach, and the authors take full responsibility for the manuscript's content, reasoning, and conclusions.

REFERENCES

[1] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)," *Official Journal of the European Union*, L 333, Dec. 27, 2022, pp. 80–152. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[2] European Parliament and Council of the European Union, "*Regulation* (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)," *Official Journal of the European Union*, L 2024/2847, Nov. 20, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[3] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union*, L 119, May 4, 2016, pp. 1–88. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[4] European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," *Official Journal of the European Union*, L 2024/1689, Jul. 12, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[5] European Parliament and Council of the European Union, "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC," *Official Journal of the European Union*, L 333, Dec. 27, 2022, pp. 164–198. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[6] European Parliament and Council of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011," *Official Journal of the European Union*, L 333, Dec. 27, 2022, pp. 1–79. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[7] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 26, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[8] ISA/IEC, *Security for Industrial Automation and Control Systems*, ISA/IEC 62443, 2018.

[9] MITRE Corporation, "MITRE ATT&CK for ICS," [Online]. Available: https://attack.mitre.org/matrices/ics/

[10] T. V. Avdeenko and N. V. Pustovalova, "The ontology-based approach to support the requirements engineering process," *2016 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE)*, Novosibirsk, Russia, 2016, pp. 513-518, doi: 10.1109/APEIE.2016.7806406.

[11] G. Sabaliauskaite, R. A. Paskauskas, E. Bružė, R. Matulytė, and T. Lavišius, "Automated regulatory compliance for AI systems in the security domain: The case of dual-use deployment," *Open Res Europe*, vol. 6, p. 83, Mar. 2026, doi: 10.12688/openreseurope.23137.1.

[12] J. Ruohonen, "A Systematic Literature Review on the NIS2 Directive", 2024, *arXiv*. doi: 10.48550/ARXIV.2412.08084.

[13] European Parliament and Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)," *Official Journal of the European Union*, Nov. 19, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837

[14] R. Mikac, "Protection of the EU's Critical Infrastructures: Results and Challenges", *Applied Cybersecurity & Internet Governance*, vol. 2, no. 1, pp. 1–5, Dec. 2023, doi: 10.60097/ACIG/162868.

[15] D. Orlando and P. Dewitte, "The 'by Design' Turn in EU Cybersecurity Law: Emergence, Challenges and Ways Forward," in *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, A. Vedder, J. Schroers, C. Ducuing, and P. Valcke, Eds. Intersentia, 2019, pp. 239–252

[16] ENISA, "NIS2 Technical Implementation Guidance," Version 1.0, Jun. 2025. [Online]. Available: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

[17] European Parliament and Council of the European Union, "Union Rolling Work Programme for European cybersecurity certification," SWD(2024) 38 final, Feb. 7, 2024. [Online]. Available: file:///Users/giedre/Downloads/SWD_2024_38_F1_STAFF_WORKING_PAPER_EN_V3_P1_3268229_8D9PyZAu7Q8rfTyMp2OkTXgP4_102292.PDF

[18] European Parliament and Council of the European Union," Draft Commission guidance on the Cyber Resilience Act," 2026. [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en

[19] ENISA, "Single Reporting Platform (SRP)." [Online]. Available: https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp

[20] European Parliament and Council of the European Union, "Proposal for a Regulation for the EU Cybersecurity Act," Jan. 20, 2026. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

[21] European Parliament and Council of the European Union, "EU Cybersecurity Certification Scheme on Common Criteria (EUCC)," Jan. 31, 2024. [Online]. Available: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

[22] European Insurance and Occupational Pensions Authority, "Digital Operational Resilience Act (DORA): Oversight of critical third-party providers," JC 2025 29, July 15, 2025. [Online]. Available: https://www.eiopa.europa.eu/publications/dora-oversight-guide_en

[23] European Central Bank, "ECB Guide on outsourcing cloud services to cloud service providers," 2024. [Online]. Available: https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603_draftguide.en.pdf

[24] Communication from European Commission, "Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)," C(2025) 5052 final, July 29, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

[25] Communication from the Commission Artificial Intelligence for Europe, "Apply AI Strategy," COM(2025) 723 final, Oct. 8, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0723

[26] European Data Protection Board, "One-Stop-Shop case digest on Security of Processing and Data Breach Notification," Jan. 2024. [Online]. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-security_en

[27] Court of Justice of the European Union, "C-634/21 - SCHUFA Holding," 2023. [Online]. Available: https://curia.europa.eu/juris/liste.jsf?num=C-634/21

[28] Court of Justice of the European Union, "C-511/18 - La Quadrature du Net and Others," 2020. [Online]. Available: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

[29] Court of Justice of the European Union, "C-203/22 - Dun & Bradstreet Austria GmbH," 2025. [Online]. Available: https://curia.europa.eu/juris/liste.jsf?num=C-203/22

[30] North American Electric Reliability Corporation, "CIP - Critical Infrastructure Protection." [Online]. Available: https://www.nerc.com/standards/reliability-standards/cip

[31] ISO/SAE, *Road vehicles - Cybersecurity engineering*, ISO/SAE 21434:2021, International Organization for Standardization (ISO), 2021.

[32] ISO/IEC, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements,* ISO/IEC 27001:2022, International Organization for Standardization (ISO), 2022.

[33] Center for Internet Security, "CIS Critical Security Controls," Version 8.1, 2024. [Online]. Available: https://www.cisecurity.org/controls/v8-1

[34] A. Shostack, *Threat Modeling: Designing for Security*. Indianapolis, USA: Wiley, 2014.

[35] H. Michael, D. LeBlanc, *Writing secure code*. Washington, USA: Microsoft Press, 2003.

[36] National Institute of Standards and Technology, "Guide to Data-Centric System Threat Modeling," NIST SP 800-154, Mar. 2016. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/154/ipd

[37] B. Al-Sada, A. Sadighian, and G. Oligeri, "MITRE ATT&CK: State of the Art and Way Forward," *ACM Comput. Surv.*, vol. 57, no. 1, pp. 1–37, Jan. 2025, doi: 10.1145/3687300

[38] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," *2020 Resilience Week (RWS)*, Salt Lake City, UT, USA, 2020, pp. 106-112, doi: 10.1109/RWS50334.2020.9241271

[39] J. Rajamäki et al., "Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals," *WSEAS Transactions on Computers*, vol. 23, pp. 1–11, Apr. 2024, doi: 10.37394/23205.2024.23.1

[40] D. Janosek, "Toward a Global Framework for Cyber Threat Intelligence Sharing," *CDR*, vol. 10, no. 2, pp. 99–114, Dec. 2025, doi: 10.55682/cdr/sgyw-5r5p.

[41] O. Kosenkov et al., "Systematic mapping study on requirements engineering for regulatory compliance of software systems," *Information and Software Technology*, vol. 178, p. 107622, Feb. 2025, doi: 10.1016/j.infsof.2024.107622

[42] R. El Khoury, M. M. Alshater, and M. Joshipura, "RegTech advancements-a comprehensive review of its evolution, challenges, and implications for financial regulation and compliance," *Journal of Financial Reporting and Accounting*, vol. 23, no. 4, pp. 1450–1485, Sep. 2025, doi: 10.1108/JFRA-05-2024-0286.

[43] J. M. Imperial, M. D. Jones, and H. Tayyar Madabushi, "Standardizing Intelligence: Aligning Generative AI for Regulatory and Operational Compliance," 2025, SSRN. doi: 10.2139/ssrn.5146161

[44] S. Abualhaija, M. Ceci, and L. Briand, "'Legal Requirements Analysis: A Regulatory Compliance Perspective," *in Handbook on Natural Language Processing for Requirements Engineering*, A. Ferrari and G. Ginde, Eds, Cham: Springer Nature Switzerland, 2025, pp. 209–242. doi: 10.1007/978-3-031-73143-3_8

[45] G. Amaral, R. Guizzardi, G. Guizzardi, and J. Mylopoulos, 'Trustworthiness Requirements: The Pix Case Study', in *Conceptual Modeling*, vol. 13011, A. Ghose, J. Horkoff, V. E. Silva Souza, J. Parsons, and J. Evermann, Eds, in Lecture Notes in Computer Science, vol. 13011. , Cham: Springer International Publishing, 2021, pp. 257–267. doi: 10.1007/978-3-030-89022-3_21

[46] R. Guizzardi, G. Amaral, G. Guizzardi, and J. Mylopoulos, "An ontology-based approach to engineering ethicality requirements," *Softw Syst Model*, vol. 22, no. 6, pp. 1897–1923, Dec. 2023, doi: 10.1007/s10270-023-01115-3

[47] A. Orlando and M. Santoro, "A semantic approach to understanding GDPR fines: From text to compliance insights," *Computer Law & Security Review*, vol. 59, p. 106187, Nov. 2025, doi: 10.1016/j.clsr.2025.106187

[48] R. A. Paskauskas, "A Preliminary Ontology for 5G Network Resilience: Hybrid Threats, Risk Reduction, Compliance", in *2025 IEEE International Conference on Cyber Security and Resilience* (CSR), Chania, Crete, Greece: IEEE, Aug. 2025, pp. 490–497. doi: 10.1109/CSR64739.2025.11129990

[49] J. Hernandez, D. Golpayegani, and D. Lewis, "Ontology-Based Approach for Mapping Concepts and Requirements from Regulations and Standards: The Case of the EU AI Act and International Standards," in *Frontiers in Artificial Intelligence and Applications*, J. Savelka, J. Harasta, T. Novotna, and J. Misek, Eds, IOS Press, 2024. doi: 10.3233/FAIA241258

[50] A. M. Hosseini, W. Kastner, and T. Sauter, "Ontology Framework Supporting Security-By-Design of Industrial Control Systems," *IEEE Trans. Ind. Inf.*, vol. 21, no. 9, pp. 7188–7197, Sep. 2025, doi: 10.1109/TII.2025.3574694

[51] R. A. Paskauskas, E. Bružė, G. Sabaliauskaitė, R. Matulytė, and T. Lavišius, "Hybrid-Threat Intelligence: A Critical Review of Semantic Integration Challenges and the Role of the HIPSTer Ontological Framework," *J. Intell. Commun.*, in press, April 2026.

[52] E. Bružė, R. A. Paskauskas, R. Matulytė, G. Sabaliauskaitė, and T. Lavišius, "Integration of Hybrid Threat Intelligence: The HiPSTer Ontological Method for Cross-Domain Correlation in Influence Operations," *Open Res. Europe*, in press, April 2026.

[53] ISA/IEC, *System Security Requirements and Security Levels*, ISA/IEC 62443-3-3:2013, International Society of Automation (ISA), 2013.

E. BRUŽĖ is Research Projects' Manager and Deputy Head of Security Research Lab at Mykolas Romeris University, Lithuania. He is interested in interdisciplinary research with focus on emerging technologies in security, enforcement and defense domains. Evaldas has received BsC in Complex Software Engineering from the Vilnius University, Lithuania in 2001, MsC in Economy and Business Administration from Vytautas Magnus University, Lithuania in 2013, International Executive MBA from Baltic Management Institute, EU/India/China in 2013, also 2014-2020 studied Gestalt Psychotherapy post-graduate programme in Vilnius Gestalt Institute and Minsk Gestalt Institute. Throughout this period and until now, he worked in academia, applied research and industry, as well as independent consultant in various countries, including different MS of EU, UK, Near East, Africa, Australia and natively Lithuania. Last decade leads R&I&D teams in the EU international innovation and research projects under EU Horizon and other flagship EU research programmes. Overtime, he has acquired integrated, multi-disciplinary knowledge and skills especially related to transformative and disruptive innovations in security, enforcement and defense domains.

G. SABALIAUSKAITE is a Professor of Cyber Security at Mykolas Romeris University, Lithuania. Her work focuses on interdisciplinary research addressing the safety, security, and resilience of complex systems. She received the Ph.D. degree in Software Engineering from Osaka University, Japan, in 2004. Since then, she has worked across academia, industry, and applied research institutions in Germany, Portugal, Sweden, Singapore, the UK, and Lithuania. Over time, she has developed cross-disciplinary expertise in diverse cultural and organizational settings, leading multiple research teams and conducting research on cybersecurity and the resilience of critical infrastructure systems.

R. A. PASKAUSKAS is a Senior Research Associate with the Security Research Laboratory, Mykolas Romeris University, Vilnius, Lithuania. He received the Ph.D. degree in Science and Technology from the University of Toronto, and the M.Sc. degree in Bioinformatics from the University of Oxford. His current research focuses on cybersecurity, cybercrime, hybrid threats, critical infrastructure resilience, and ontology-driven approaches to regulatory compliance, semantic integration, and threat intelligence.

R. MATULYTĖ is a Ph.D. candidate at Mykolas Romeris University, Vilnius, Lithuania. She holds a Magna Cum Laude Master's degree from Vilnius University, where her thesis conducted an economic analysis of law by comparing EU and U.S. data protection models. Her primary research interests concern privacy and data protection. She is a member of the Security Research Laboratory at Mykolas Romeris University. For several years, she also worked as an associate at a top-tier Baltic law firm, where her practice focused on data and technology matters, including data protection, cybersecurity, AI governance, and related domains.

T. LAVIŠIUS received the B.S. and M.S. degrees in law from Vilnius University, Vilnius, Lithuania, and the Ph.D. degree in law from Mykolas Romeris University, Vilnius, Lithuania. Since 2008, he has held various positions in the governmental sector. Since 2019, he has served as a researcher and adviser in the Research Department of the Seimas of the Republic of Lithuania, while also engaging in scientific and pedagogical activities. He has published articles in the fields of business law, sustainability, social responsibility, and the legal environment of cybersecurity. He is a member of the Security Research Laboratory and the Justice Research Laboratory at Mykolas Romeris University.