Towards Automated Certification Framework of Composite Systems: A SWRL-Based Approach

Jasmin Cosic
Department for Information and Cyber Security
DEKRA SE
Stuttgart, Germany
jasmin.cosic@dekra.com

Chatzopoulou Argyro
Department for R&D
APIROPLUS
Solutions Ltd
Limassol, Cyprus
ac@apiroplus.solutions

Marga Martín Sánchez
Department for Growth Management
DEKRA TC SAU
Málaga, Spain
marga.martin@dekra.com

Antonio David Vizcaino Gomez
Cybersecurity Division
DEKRA TC SAU
Málaga, Spain
antoniodavid.vizcaino@dekra.com

Drazen Morog
Department for Information and Cyber Security
DEKRA SE
Stuttgart, Germany
drazen.morog@dekra.com

***Abstract*— This paper presents an ontological approach to the cyber-security certification of composite systems, leveraging the Common Criteria (CC) framework. We introduce an ontology that models key elements of the common criteria, such as Target of Evaluation (TOE), Security Assurance Requirements (SARs), Security Functional Requirements (SFRs), Evaluation Assurance Level (EAL), etc. and components like IoT Devices, Edge Gateways, AI Engine, etc. Some specific components, which were used in project pilots, are also presented. The ontology facilitates automated reasoning through Semantic Web Rule Language (SWRL) rules to assess certification status. This methodology enhances explainability, efficiency, transparency, consistency, and automation in certification processes, especially for systems integrating complex components like IoTs, AIs, etc.**

Keywords*— *cyber security certification, common criteria, ontologies, SWRL, composite systems

I. INTRODUCTION

Certification of composite systems, which are made up of at least two individual components, presents unique difficulties due to their complexity and the linked security needs of the separate parts (components). [1],[2] The Common Criteria (CC) framework [2] gives a methodical way to assess the security features of IT products but using it for composite systems necessitates detailed, not only techniques, but the adoption of a holistic approach for such a certification.

A composite product consists of at least two different components. These components could also be independent products that are combined in order to create the composite system. For example, a hardware device, operating with a specific operating system and specialized software. For a certificate to be awarded to a composite system, the security objectives (the concise statements of the intended solution to the security problem [2] posed by the composite system) have to be evaluated and validated within a predefined assurance level. The composite TOE (Target of Evaluation) comprises the whole composite product, (a component of which may already have been certified), and the evaluation of the composite TOE is a composite evaluation [3].

As defined in Common Criteria [2] there are three types of compositional model:

a) *Layered compositional model* where one component is built on top of another component. One of the most common examples of layered compositional model comes from the smartcard domain where hardware (a hardware integrated circuit (IC)) is presented as the base component, and the software part is on top of it (dependent component).

b) *Network or bi-directional compositional model* where one component uses the specific functionality of another component communicating via some channel. One of the most common examples of the network or bi-directional compositional model where one application (component A) uses the authentication functionality of an external LDAP server (component B).

c) *Embedded compositional model* where a component is used as part of larger component or product. One of the most common examples of the Embedded compositional model is that of a product (Major component A) utilizes a library or a subsystem of another component (Minor component C). [2] Figure 1 depicts the three variations of the compositional models presented here.

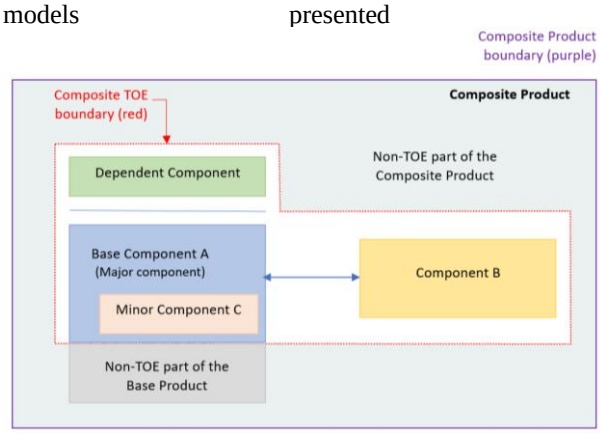

Figure 1 A view of the components of a composite product

Figure1, depicts a composite product which consists of four components interconnected in all three compositional models presented above. The Target of Evaluation (ToE) can be a part of a composite product, meaning that the rest of the product will be within the scope of the evaluation (non-TOE part of the composite product). Figure1, cannot capture

though, the more real-life cases where the composite ToE is created by multiple components, following more than one compositional model. In such real, practical examples of composite products, we expect to see larger complex systems, consisting of a large and varied (in type) number of components. Such an example of a composite product could be that of a drone or of a monitoring system utilized within a 5G network. These products would be expected to consist of hardware, software, and information, interconnected in order to fulfil their operational objectives, making the identification and control of these components and their relationships a key process in the evaluation of composite ToE.

Using ontologies in engineering provides us a formal method to describe the domain and model the domain knowledge, as well as allow for automated reasoning. [4] By using ontological modelling in the cyber-security certification process, we can illustrate the connections and dependencies among components (parts of the composite ToE under evaluation), simplify certification choices, and make sure we meet security standards. This paper intends to connect traditional certification methods with new ontological approaches, presenting a fresh method to support cybersecurity assurance.

The Common Criteria (CC) standard, established under ISO/IEC 15408, serves as a widely accepted framework for the security evaluation of IT products. The CC framework articulates the concept of a Target of Evaluation (TOE), delineating the system components and security functions that necessitate evaluation. However, the application of the CC framework to composite systems, which involve multiple interconnected components contributing to the overarching security posture, presents substantial challenges encompassing scalability, dependency management, and concerns related to AI security. [1], [2]

The questions raised regarding composite ToE evaluation and subsequent certification are the following:

- How can the completeness and control of the identification and documentation of the components of a composite ToE be ensured?
- How can the relationships between the components be depicted in a way that is useful to the evaluation process according to common criteria standards?
- How can the results of previous evaluations of one or more components of the composite ToE be standardized and utilized to expedite the evaluation process?

Ontology-based approaches have gained prominence to address aa lot off challenges, providing a formalized representation of system components and their interdependencies. Ontologies facilitate the modelling of certification requirements, dependencies, and security controls in a machine-readable format, thus enabling automated reasoning and compliance verification. Notably, the Protégé ontology editor, developed at Stanford University [5], offers a robust platform for crafting OWL-based ontologies that support both logical inference and rule-based reasoning using the Semantic Web Rule Language (SWRL). [6]

The framework, which is introduces in this paper, is validated through a practical use case from CUSTODES Project [7], involving a smart home/building scenario, evaluating its efficacy in ensuring adherence to requirements pertaining to AI transparency, GDPR, and security. The proposed solution effectively addresses critical challenges of composite ToE, including real-time testing, component dependency inventory and tracking, and scalability in complex systems.

II. RELATED WORK

The processes that must be used for cybersecurity certification are described in specific standards and certification schemes. ISO/IEC 17065 [8] contains requirements for the competence, consistent operation and impartiality of product, process and service certification bodies. Whereas the ISO/IEC 15408 series [9] of standards establish the general concepts and principles of IT security evaluation and specify the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products. The Common Criteria framework has been widely adopted internationally, providing a baseline for cybersecurity evaluations [2]. However, integrating ontologies with CC for composite systems remains an underexplored area, highlighting the novelty and relevance of our approach. Finally, from the part of cybersecurity for ICT products, the EU Cybersecurity Certification Scheme on Common Criteria (EUCC) [10] was published in January 2024, allowing 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.

Prior research has explored various methods for modelling of aspects related with cybersecurity. Some of these methods are described in [11] including Infosec-Tree, Reference Model of Information Assurance & Security and others. Also, [11] presents the concepts of composition in a simplified manner. Ontological approaches have been applied in the research [12], where the contribution was on the research on quantitative Secure Assurance Evaluation by proposing an ontology-based assurance metrics computation solution, which consists of quantitative Secure Assurance Evaluation approach, an ontology for modelling the security assurance components and metrics, and a metrics calculation engine for automatically generating metrics values. The feasibility and effectiveness of the proposed ontology are examined through a preliminary ontology evaluation as well as a practical application-based evaluation. Authors in [13] were engaged with Industrial IoT and provided comprehensive analysis through a systematic review of ontologies and key security attributes essential for modelling the security of IoT environments. This review includes an extensive analysis of research articles, semantic security ontologies, and cybersecurity standards.

With the topic of AI-enabled systems dealt authors in [14], where was emphasized role of the ontologies in cyber-security domain and knowledge representation. The accent of the research was on “documenting prevalent machine learning (ML) threats and countermeasures, including the mechanisms by which emerging attacks circumvent existing defences as well as the arms race between them”. The goal of the research was to systematically formalize a body of knowledge intended to complement existing taxonomies and threat-modelling approaches of applications empowered by AI.

Ontology is also used in the domain of digital forensic field and the field of dealing with digital evidence [15]. This study highlights the potential of ontologies to improve transparency and automate compliance verification and support digital investigation process. The European Cyber Security Organization (ECSO) published the paper "Product Certification Composition" whit the aim to be high-level guideline for product certification composition. Generic IoT device was used as a reference Case Study to explain how document can be used in practice. [1] The ontologies, as methodologies are also used in risk assessment procedures, where authors [16] tried to propose a extended cyber-security ontology which may be used to assist in the process. A good systematic review of Cyber-security Ontologies was provided by authors in [17]. The research shows us that most of the developed and presented ontology are coming from infrastructure and networking, software, and human factor.

The CUSTODES Project [7] aims to develop an innovative system for the cybersecurity certification of composite ICT products and services. A notable contribution from this project is the paper [25] which explores the development of an ontology tailored for cybersecurity certifications, enhancing the clarity and efficiency of the certification process. The presented ontology was in early phasis of deployment, due the lack of information about future pilots and use-cases. This, proposed ontology differs from previous research bringing the reasoning and logic (from SWRL) which could support process of evaluation and short the time of evaluation.

III. ONTOLOGICAL APPROACH FOR CERTIFICATION

The methodology employed in this study is structured to ensure a comprehensive and systematic approach to the certification of composite systems in Ambient Intelligence Environments, in compliance with the Common Criteria (CC) standards. The approach for development was following methodology published in [19], [22] The process involves several key phases, including requirement analysis, ontology design, rule definition, and evaluation against specific requirements. Within the context of this document, the word validation is used. Validation means confirmation that the contents of data objects meet the needs of identified stakeholders (e.g., healthcare providers, patients), often involving acceptance and suitability; verify correctness (to reflect the true situation) [20]. On the other hand, verification means the rigorous review in detail with an independent determination of sufficiency [21].

A. *Requirement Analysis:*

- Definition of the composite Target of Evaluation (TOE).
- Identification of security assurance and functional requirements based on the Common Criteria standards [2].
- Identification and classification of the components of the composite system (e.g., hardware, software, AI modules, etc.) and their contribution to solving the problem posed by the composite system.

B. *Ontology Design:*

- Development of an OWL-based ontology to represent processes supporting testing and certification, components, and security requirements.
- Definition of classes such as *TOE, Components, HardwareComponent, SoftwareComponent, and AIComponent*.
- Establishment of object properties to link components with security requirements.

C. *SWRL Rule Definition:*

- Creation of SWRL rules to automate reasoning (supporting testing and certification processes).
- Design and implementation of rules that would allow the identification of existing certification information of the components of the composite ToE.
- Verification of AI-specific requirements, such as explainability and security impact analysis.

D. *System Validation:*

- Deployment of the ontology within the Protégé framework.
- Execution of reasoning processes using HermiT and/or Pellet reasoners to validate rule effectiveness.
- Performance evaluation to ensure the ontology's ability to dynamically infer testing and evaluation results.

IV. ONTOLOGY DESIGN

This chapter details the ontology developed to support the certification processes of composite systems. The ontology, developed in Protégé, using methodology described in [19], [22], captures key entities and relationships in the certification process. It is structured to reflect the hierarchical and relational nature of composite systems, ensuring that each component's security attributes are accurately represented. On Phase 1 – Initiation defined initial systems and components and identification of the scenarios and in Phase 2 – Ontology Modelling were described activities in regards of Knowledge acquisition, Conceptualization, Formalization and Partial Validation. Phase 3,4 and 5 (Deployment, Validation and Life-Cycle Re-Engineering) were followed through provision of the application, consistency check with Protégé reasoner, Review of the requirements fulfilment and Knowledge Review [22] The starting point for this ontology was work delivered in CUSTODES WP2 and published on the project repository. [7] The described ontology is a more mature and enriched version of previous work implemented at the beginning of the CUSTODES project. That first initial version was further enriched with most common classes, object/data properties and new set of the rules.

On Figure 2 we can see some statistics about Core Concept of proposed ontology.

A. Core Concepts

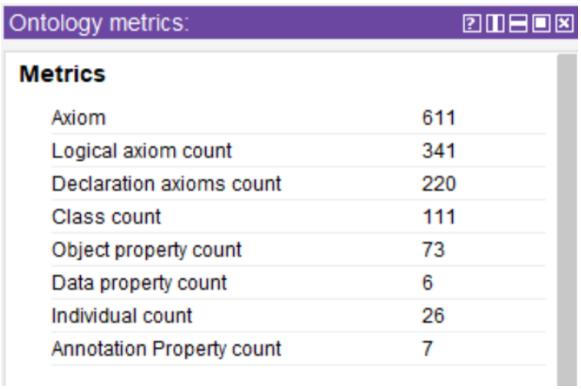

Figure 2 Metric of the proposed Ontology

We can see that proposed ontology consists of huge number of axioms, but pilot is centred around the following few core concepts:

CompositeSystem: Represents a system composed of multiple interacting components. This class serves as the Target of Evaluation.

Component: Represents an individual hardware or software part that comprises a composite system. Each individual component could already be certified against specific requirements at various assurance levels.

HardwareBoard: A specialized type of component that often forms the foundation of a composite system.

CertificationLevel: Represents a well-formed package of security assurance requirements representing a point on the predefined assurance scale [1] . This class allows for the representation of different certification schemes (e.g., Common Criteria EAL levels).

SecurityRequirement: Represents a specific security requirement that a ToE must fulfil. This class encompasses security assurance and security functional requirements.

Interaction: Represents the interaction between two components. The resilience of these interactions is crucial for the overall security of the composite system.

B. Class Hierarchy

The ontology defines a class hierarchy to organize the concepts and capture specialization. Key aspects of the hierarchy include:

Component is a superclass for all types of components. *HardwareBoard* is a subclass of *Component. SecurityRequirement* is a superclass for various specific security requirements (e.g., *AIActConsideration, SR1, SR2, SR3, SR4*). *CertificationLevel* can be further specialized if needed to represent specific certification schemes or levels within those schemes, etc.

C. Properties

The proposed ontology is enriched with more than 70 object properties. Here a few key properties are presented to demonstrate the relationships between the concepts:

hasComponent: An ObjectProperty relating a CompositeSystem to its constituent Components. The domain is CompositeSystem and the range is Component.

hasCertificationLevel: An ObjectProperty relating a Component or HardwareBoard to a CertificationLevel. The domain is Component and the range is CertificationLevel.

requires: An ObjectProperty relating a Component or CompositeSystem to a SecurityRequirement. The domain is Component and the range is SecurityRequirement.

fulfills: An ObjectProperty relating a Component to a SecurityRequirement, indicating that the component fulfills that requirement. The domain is Component and the range is SecurityRequirement.

interactsSecure: An ObjectProperty relating two Components, indicating that their interaction is safe and does not introduce vulnerabilities. The domain and range are both Component.

D. Instances

The ontology includes instances of the defined classes to represent specific composite systems, components, certification levels, and security requirements. These instances form the knowledge base for the SWRL rules used for certification. For example, those are:

- *ais1* as Composite system,
- *AI_Module1* as AI Component,
- *ais1, ais4* as Ambient Intelligence Service,
- *ai1 and ai1* as AI Engine,
- *gw1 and gw3* as Edge Gateway,
- *hb1 and hb4* as Hardware Board, specific hardware boards,
- *dev1 and dev4* as a IoT Devices,
- software modules, and security requirements (*sr1, sr2, sr3 and sr4*) relevant to the target domain are instantiated within the ontology.

E. Ontology Design Rationale

The design of this ontology is driven by the need to capture the essential information required for composite system certification. The focus on components, their certification information, their security requirements, and their interactions provides a structured and formal way to support evaluation and certification processes of composite ToEs. The use of OWL allows for rich expressiveness and enables automated reasoning using SWRL rules, which are detailed in the next chapter. This ontology serves as the foundation for the automated certification framework, enabling efficient and consistent evaluation of composite systems.

On Figure 3, 4 and 5 are presented some of the classes from this ontology.

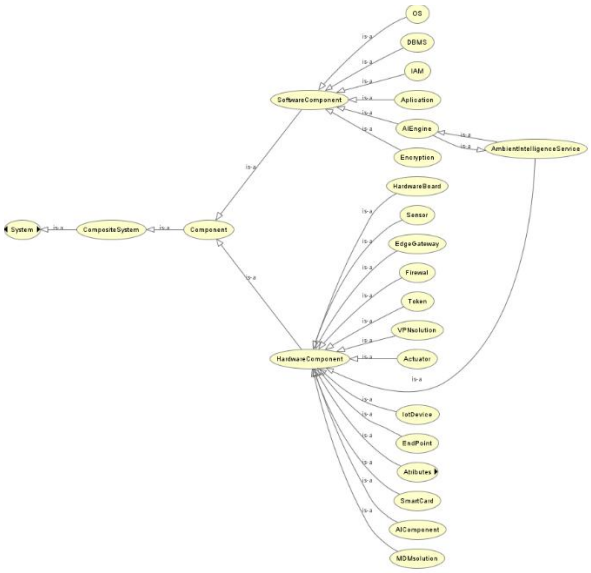

Figure 3 Class: Component

Figure 4 Class: Requirement

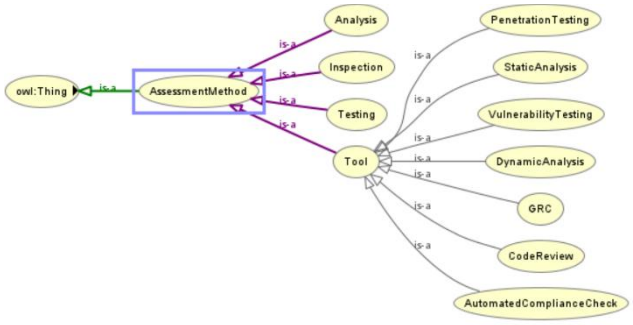

Figure 5 Class: Assessment Method

SWRL Rules for Certification: SWRL rules (Figure 6) automate the reasoning process in order to automate the identification of information regarding the certification status of the components of the composite ToE.

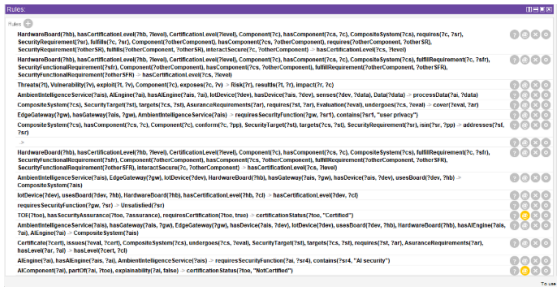

Figure 6 Portion of the proposed rules

V. USE CASE (PROJECT PILOT)

A. *System Description*

For this Use-Case, focus will be on the cyber security certification based on Common Criteria standard, of an Ambient Intelligence Service which is composed by the following architecture elements:

- *Edge gateway*. This device incorporates enhanced computing capabilities and allows local processing/actuation for user privacy and security concerns.
- *Enhanced IoT devices* equipped with heterogeneous sensors (i.e. instances can be - temperature, noise, presence, CO2, cameras, microphones) and with embedded AI capabilities.

These devices have the capability to take intelligent decisions/actions in an individual or cooperative manner. The collaborative approach allows to improve the efficiency/resiliency of single sensor solutions, which might fail. These devices can programmed to address different application scenarios in a smart home/building use case.

We also will consider that *Hardware Board* (hardware) as a component is already certified (Market Product), and *Enhanced IoT*, *Edge Gateway* (Software) and *Ambient Intelligence engine* (Software) are not certified.

Our model is based on the following key concepts:

1. *Components*: Individual hardware or software entities that make up the composite system. Each component may have its own certification level.
2. *Composite System*: A system composed of multiple interacting components. The certification level of the composite system depends on the certification levels of its components and the safety of their interactions.
3. *Certification Level*: A level of assurance granted to a component or system after evaluation against a set of criteria. Examples include EAL levels from Common Criteria.
4. *Security Requirements*: Specific requirements that a component must fulfil to be considered secure. These requirements can be functional (e.g., authentication, access control) or non-functional (e.g., performance, reliability).
5. *Secure Interaction*: The guarantee that the interaction between two components does not introduce new vulnerabilities or compromise existing security requirements.

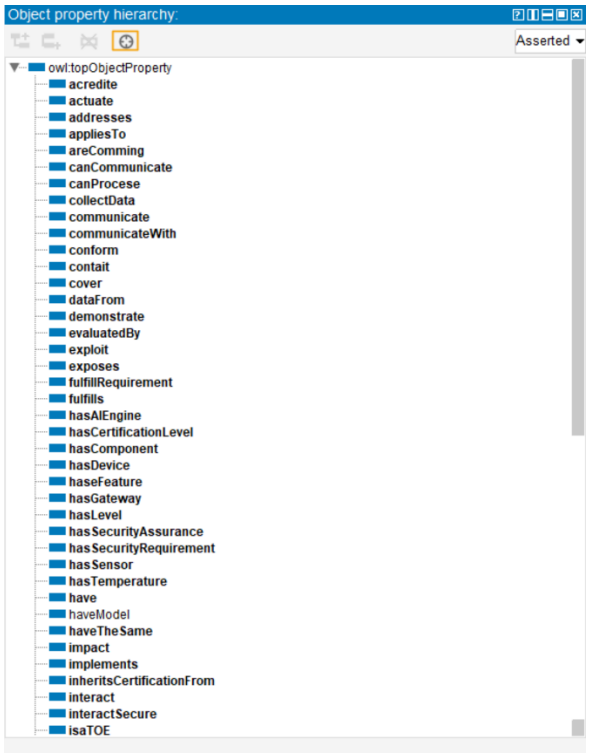

Figure 7 Some of Object properties defined for this ontology (part 1)

Figure 8 Some of object properties defined for this ontology (Part II)

B. *The Rules*

Let's define the rules which will be used for this Use-Case:

1. Composite System Definition:

AmbientIntelligenceService(?ais), hasGateway(?ais, ?gw), EdgeGateway(?gw), hasDevice(?ais, ?dev), IoTDevice(?dev), usesBoard(?dev, ?hb), HardwareBoard(?hb), hasAIEngine(?ais, ?ai), AIEngine(?ai) -> compositeSystem(?ais)

2. Hardware Board Certification: The hardware board's certification level is inherited by the IoT device (partially).

IoTDevice(?dev), usesBoard(?dev, ?hb), HardwareBoard(?hb), hasCertificationLevel(?hb, ?cl) -> hasCertificationLevel(?dev, ?cl) // The IoT device's hardware is at least as certified as the board.

3. IoT Device Security Requirements: IoT devices must implement security functions addressing data privacy and secure communication, considering the hardware board's existing certification.

IoTDevice(?dev), usesBoard(?dev, ?hb), HardwareBoard(?hb), hasCertificationLevel(?hb, ?cl), conformsTo(?dev, ?pp), ProtectionProfile(?pp), SecurityRequirement(?sr), isIn(?sr, ?pp), (contains(?sr, "data privacy") OR contains(?sr, "secure communication")) -> needsSecurityFunction(?dev, ?sr)

IoTDevice(?dev), needsSecurityFunction(?dev, ?sr), Component(?c), hasComponent(?ais, ?c), implements(?c, ?sf), SecurityFunction(?sf), addresses(?sf, ?sr) -> satisfiedBy(?sr, ?c) // A component of the AIS satisfies the requirement.

IoTDevice(?dev), needsSecurityFunction(?dev, ?sr), \neg satisfiedBy(?sr, ?c) -> iotDeviceNotCompliant(?dev, ?sr) // If no component satisfies it, the IoT device is not compliant.

4. Edge Gateway Security Requirements: The gateway must implement security functions for user privacy, secure communication, and access control.

EdgeGateway(?gw), hasGateway(?ais, ?gw), AmbientIntelligenceService(?ais) -> requiresSecurityFunction(?gw, ?sr1), contains(?sr1, "user privacy")

EdgeGateway(?gw), requiresSecurityFunction(?gw, ?sr1), Component(?c), hasComponent(?ais, ?c), implements(?c, ?sf), SecurityFunction(?sf), addresses(?sf, ?sr1) -> satisfiedBy(?sr1, ?c)

EdgeGateway(?gw), requiresSecurityFunction(?gw, ?sr1), \neg satisfiedBy(?sr1, ?c) -> gatewayNotCompliant(?gw, ?sr1)

EdgeGateway(?gw), hasGateway(?ais, ?gw), AmbientIntelligenceService(?ais) -> requiresSecurityFunction(?gw, ?sr2), contains(?sr2, "secure communication")

EdgeGateway(?gw), requiresSecurityFunction(?gw, ?sr2), Component(?c), hasComponent(?ais, ?c), implements(?c, ?sf), SecurityFunction(?sf), addresses(?sf, ?sr2) -> satisfiedBy(?sr2, ?c)

EdgeGateway(?gw), requiresSecurityFunction(?gw, ?sr2), \neg satisfiedBy(?sr2, ?c) -> gatewayNotCompliant(?gw, ?sr2)

EdgeGateway(?gw), hasGateway(?ais, ?gw), AmbientIntelligenceService(?ais) -> requiresSecurityFunction(?gw, ?sr3), contains(?sr3, "access control")

EdgeGateway(?gw), requiresSecurityFunction(?gw, ?sr3), Component(?c), hasComponent(?ais, ?c), implements(?c, ?sf), SecurityFunction(?sf), addresses(?sf, ?sr3) -> satisfiedBy(?sr3, ?c)

EdgeGateway(?gw), requiresSecurityFunction(?gw, ?sr3), \neg satisfiedBy(?sr3, ?c) -> gatewayNotCompliant(?gw, ?sr3)

5. Ambient Intelligence Engine Requirements: The AI engine must meet security and privacy requirements, especially regarding data processing. This is a simplified representation and will need significant refinement based on the AI Act and relevant standards.

AIEngine(?ai), hasAIEngine(?ais, ?ai), AmbientIntelligenceService(?ais) -> requiresSecurityFunction(?ai, ?sr4), contains(?sr4, "AI security")

AIEngine(?ai), requiresSecurityFunction(?ai, ?sr4), Component(?c), hasComponent(?ais, ?c), implements(?c, ?sf), SecurityFunction(?sf), addresses(?sf, ?sr4) -> satisfiedBy(?sr4, ?c)

AIEngine(?ai), requiresSecurityFunction(?ai, ?sr4), \neg satisfiedBy(?sr4, ?c) -> aiEngineNotCompliant(?ai, ?sr4)

6. Composite Certification: The Ambient Intelligence Service's certification depends on the compliance of its components.

AmbientIntelligenceService(?ais), \neg (iotDeviceNotCompliant(?dev, ?sr1)), \neg (gatewayNotCompliant(?gw, ?sr2)), \neg (aiEngineNotCompliant(?ai, ?sr3)) -> hasCertificationLevel(?ais, ?level) // Simplified for the proof of concept. A real certification would be much more detailed.

C. Proof of Concept (Protégé):

The ontology is implemented in Protege, with individuals representing system components. The following steps were taken to model the system and apply the certification rules:

1. Ontology Creation: Classes and properties were defined to represent system components and their relationships.
2. Instance Creation: Instances like cs1, ai1, hw1, etc. were created.
3. Property Assertions: Relationships such as *fulfil*(Component, SFR), *CommunicateWith* (Component, Component), *hasAIEngine* (AmbientIntelligenceService, AIEngine), hasComponent (CompositeSystem, Component), *meetsRequiremement* (Component, Requirement), and *hasSecurityAssurance*(SoftwareComponent1, true), etc. were established.
4. SWRL Rule Application: The defined rules were applied to the ontology.
5. Reasoning: The HermiT reasoner was used to infer the certification status of TOE_Example.

Let's assume: If a *CompositeSystem* has a *HardwareBoard* certified to "Level X", and all other components meet specific functional and security requirements (defined in other rules or properties), and the interaction between components does not introduce vulnerabilities, then the *CompositeSystem* can be considered for certification at a Level no higher than "LevelX".

HardwareBoard(?hb) ^ hasCertificationLevel(?hb, ?level) ^ CertificationLevel(?level) ^ CompositeSystem(?cs) ^ hasComponent(?cs, ?c) ^ Component(?c) ^ requires(?c, ?sr) ^ SecurityRequirement(?sr) ^ fulfills(?c, ?sr) ^ Component(?otherComponent) ^ hasComponent(?cs, ?otherComponent) ^ requires(?otherComponent, ?otherSR) ^ SecurityRequirement(?otherSR) ^ fulfills(?otherComponent, ?otherSR) ^ interactsSafelyWith(?c, ?otherComponent) -> hasCertificationLevel(?cs, ?level)

VI. RESULTS AND DISCUSSION

Following the information presented above, let's assume that *hb1* (Hardware Board) has certification level EAL4, *cs1* (Composite System) has components *comp1* and *comp2*, *comp1* requires and fulfils AIActConsideration, *comp2* requires and fulfils SR1 and *comp1* interactsSecure with comp2.

With this new, corrected rule, Protégé (using a SWRL reasoner) will correctly infer that *cs1* has assurance level EAL4 (or lower) only if *comp1* fulfils AIActConsideration and *comp2* fulfils SR1. If either of these conditions is not met, the rule will not be activated. The automated reasoning process correctly identified certification statuses based on the defined rules. For example, *AI_Module1* lacking explainability resulted in the entire system (TOE_Example) being marked as "*NotCompliant.*" Conversely, when all components met their respective assurance requirements, the TOE was certified.

The results demonstrate the effectiveness of the ontology in automating evaluation decisions and highlight the potential for scaling this approach to more complex systems.

The ontology effectively modelled the certification process, highlighting interdependencies among components. This approach offers several advantages:

- Explainability: With this approach knowledge from the domain is simple presented and structured,
- Transparency: The ontology provides a clear and structured representation of the certification process, making it easier to understand and audit.
- Consistency: Automated reasoning ensures consistent application of certification criteria, reducing the likelihood of human error.
- Scalability: The model can be easily extended to accommodate new components and certification criteria.

Conclusion: This study shows a conceptual way to evaluate composite systems, combining SWRL rules with the Common Criteria framework. The approach use ontology for knowledge modelling and reusability, enables automated reasoning, increasing the effectiveness and dependability of certification processes. By using ontological modelling, we can improve the clarity, uniformity, and scalability of security certification, especially for intricate systems that include AI

parts. To bridge the gap between theory and practice, we simulated a deployment in a project pilots, where the framework's efficiency allowed use for Smart Home scenario. The ontology can be simple modified and used as a framework for similar pilots and use-cases, i.e. in large-scale production environment, where a key challenge would be ensuring consistent performance under varying data distributions. Given its ability to enhance interpretability, improve robustness, and streamline data processing, proposed framework could also support compliance with emerging regulations such as the EU Cyber Resilience Act. [23], [24] However, some limitations were noted, such as the need for comprehensive rule definitions to cover all possible certification scenarios, because this paper dealt with specific Use-Case from the project. Future work will focus on expanding the ontology to include more detailed security requirements and integrating it with dynamic system monitoring tools. The proposed ontology (OntoCCS.owl) can be downloaded from the project repository - https://custodes-project.eu/custodes-repo/

ACKNOWLEDGMENT

The research leading to these results received funding from the European Union's HORIZON Innovation Action program under grant agreement No. 101120684 - project CUSTODES, as well as DIGITAL-ECCC-2024-DEPLOY-CYBER-06 under proposal number 101190372 . Jasmin Cosic and Drazen Morog (DEKRA SE), Marga Martin Sanchez and Antionio David Vizcaino Gomez (DEKRA TC), are participants as CUSTODES project partners and Chatzopoulou Argyro (APIRO Plus) as CURIUM and CUSTODES project partner. We want to thank to all project partners from both of sides for constructive suggestions and research activities in the projects.

MATCH & CONTRIBUTION

This contribution aligns well with the theme of the ICE IEEE 2025 conference on "AI-driven Industrial Transformation: Digital Leadership in Technology, Engineering, Innovation & Entrepreneurship". The paper presents an ontological approach to the cyber-security certification of composite systems, leveraging the Common Criteria (CC) framework. This framework forms the basis for the automation of evaluation and testing tasks supporting the cybersecurity and AI certification of ICT products. This contribution addresses the conference's focus on utilizing data-driven approaches to foster innovation and entrepreneurship, making it a relevant and valuable addition to the conference proceedings.

REFERENCES

[1] [1] European Cyber Security Organization, ECSO, Product Certification Composition, WG 1, 2020

[2] [2] "Common Criteria for Information Technology Evaluation", Publication, [Online]. Available: https://commoncriteriaportal.org/index.cfm

[3] [3] I. Furgel and V. Schenk, Composite Evaluation: General Approach and Practical Integration of Security Policies, The 7th ICC Conference, Lanzarote

[4] [4] J.Cosic, Z.Cosic, M.Baca, An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence, JIOS, 2011

[5] [5] Protégé, A free, open-source ontology editor and framework for building intelligent systems, [Online]. Available: https://protege.stanford.edu/

[6] [6] SWRL – Semantic Web Rule Language, W3C Member, [Online]. Available: https://www.w3.org/submissions/SWRL/

[7] CUSTODES Project, [Online]. Available: https://custodes-project.eu/

[8] ISO/IEC 17065:2012. Conformity assessment — Requirements for bodies certifying products, processes and services. [Online]. Available: https://www.iso.org/standard/46568.html

[9] ISO/IEC 15408-1:2022. Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. Part 1: Introduction and general model. [Online]. Available: https://www.iso.org/standard/72891.html

[10] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), January 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02024R0482-20250108.

[11] R. Villalón-Fonseca, "The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity", Computers & Security, Volume 120, 2022, 102805, https://doi.org/10.1016/j.cose.2022.102805.

[12] S-F. Wen, B. Katt, "Ontology-Based Metrics Computation for System Security Assurance Evaluation, Journal of Applied Security Research, Vol.19,2024.

[13] J.M. Aslam, J. Watson, A. Sajjad, "Modelling Industrial IoT Security Using Ontologies: A Systematic Review", DOI: 10.1109/OJCOMS.2024.011100

[14] D. Preuveneers, W. Josen, "An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Application, Future Internet, 2024

[15] J.Cosic, Z.Cosic, M.Baca, An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence, JIOS, 2011

[16] C. Grigoriadis, A.M. Berzovitis, I. Stellios, P. Kotzanikolaou, "A Cybersecurity Ontology to Supprot Risk Information Gathering in Cyber- Physical Systems", Lecture Notes in Computer Science, 2022.

[17] W.F. Borja Rivadeneira, O.S. Gomez, "Cybersecurity Ontologies: A Systematic Literature Review", Computacione Informatioca, 2021

[18] J. Doe, "Applying Common Criteria to Composite Systems," Proc. IEEE Intl. Conf. on Security Evaluation, pp. 123-130, 2019

[19] F. Noy Natalya and L. McGuinness Deborah, Ontology Development 101: A Guide to Creating Your First Ontology, https://protege.stanford.edu/publications/ontology_development/ontology101.pdf

[20] ISO/IEC TR 20004:2015. Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045. Available: https://www.iso.org/standard/68837.html

[21] ISO/TS 21089:2018. Health informatics — Trusted end-to-end information flows. [Online]. Available: https://www.iso.org/standard/66936.html.

[22] S. Weber, T. Dannen, et all., Methodology for agile and iterative ontology development for toolmaking, 6th CIRP Conference on Manufacturing Systems, CIRP CMS '23, South Africa

[23] Cyber Resilience Act, Shaping Europe's digital future, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[24] CURIUM Project, [Online]. Available: www.curium-project.eu

[25] J. Cosic and A. Jukan, "Deciphering Cyber-Security Certifications: An Ontological Journey through Composite Systems and their certification," 2024 IEEE International Conference on Engineering, Technology, and Innovation (ICE/ITMC), Funchal, Portugal, 2024, pp. 1-6, doi: 10.1109/ICE/ITMC61926.2024.10794255.