Concepts and relationships in safety and security ontologies: A comparative study

1st Malina Adach, 2nd Kaj Hänninen, 3rd Kristina Lundqvist
School of Innovation, Design and Engineering
Mälardalen University
Västerås, Sweden
{malina.adach, kaj.hanninen, kristina.lundqvist}@mdu.se

***Abstract*— Safety and security ontologies quickly become essential support for integrating heterogeneous knowledge from various sources. Today, there is little standardization of ontologies and almost no discussion of how to compare concepts and their relationships, establish a general approach to create relationships or model them in general. However, concepts with similar names are not semantically similar or compatible in some cases. In this case, the problem of correspondence arises among the concepts and relationships found in the ontologies. To solve this problem, a comparison between the Hazard Ontology (HO) and the Combined Security Ontology (CSO) is proposed, in which the value of equivalence between their concepts and their relationships was extracted and analyzed. Although the HO covers the concepts related to the safety domain and the CSO includes security-related concepts, both are based on the Unified Foundational Ontology (UFO). For this study, HO and CSO were compared, and the results were summarized in the form of comparison tables. Our main contribution involves the comparisons among the concepts in HO and CSO to identify equivalences and differences between the two. Due to the increasing number of ontologies, their mapping, merging, and alignment are primary challenges in bridging the gaps that exist between the safety and security domains.**

***Index Terms*—Hazard Ontology, safety, Combined Security Ontology, concepts, relationships, comparison, security.**

I. Introduction

System-of-systems (SoS) are increasingly used across various domains (e.g., industrial processes, power grids, air, and road transportation). These systems include heterogeneous structures at different levels of abstraction. Due to this diversity, models and sets of spatial data are constructed with different structural characteristics and basic semantics to represent the systems. For example, ontologies can be used to represent, in a formal manner, the characteristics of an SoS.

An ontology presents knowledge in a structured way and supports communication, organization, and knowledge reusability [1]. It includes a description of the concepts and the relationships among them. The main goals of an ontology are to describe reality, share vocabulary, and provide a formal description of terms to decrease language ambiguity. Many ontologies have been proposed over the past decade, but they have only covered some aspects of specific domains.

Many authors have indicated that the safety and security domains complement each other, and as such, there is a need for a universal ontology [2], which is considered a significant challenge [3]. Therefore, the ontologies from the safety and security domains would benefit from having formally defined common and shared concepts and relationships among them.

Ontology creators may also use different meanings to explain concepts and different hierarchies in an ontology, which may not always provide heterogeneity. Therefore, the task of identifying differences between ontologies becomes necessary to prevent the overlapping of information when more than one ontology is used for the same domain or when ontologies from different domains are merged [1]. When two different ontologies are combined, there may be confusion because some concepts may be syntactically equal but have different semantic properties depending on their domain. These issues are addressed in this paper, which examines two ontologies from two different domains.

Further, in recent years, the importance of interoperability at both the syntactic and semantic levels has grown and has become an integral part of ontologies. Ontology technologies enable the unambiguous identification of concepts and provide formal descriptions of relationships between concepts. However, developers continue to face the problem of semantic interoperability, which hinders the full potential of an ontology. Semantic interoperability refers to the ability of systems to exchange data (information) in a way that the exact meaning of the data (information) can be determined and the data itself can be understood by all systems. Therefore, comparing and aligning ontologies is a fundamental aspect of interoperability and data integration problems. Due to the current state of ontologies, we enhance interoperability by contributing to ontology comparing (matching).

For this study, a comparison was carried out between a Hazard Ontology (HO) proposed by Zhou et al. [4] and a Combined Security Ontology (CSO) presented in our earlier work [5]. The compared ontologies have different terminologies and have been developed in different domains, however, both can be utilized for SoS analysis. Both ontologies are grounded in the Unified Foundational Ontology (UFO) [6] and are written in Unified Modeling Language (UML). We employ UFO as the starting point for comparing ontologies from different domains. Using UFOs as a basis, we constructed a CSO that is comparable to the HO. The literature on ontological engineering applied to security was considered to perform this comparison. In addition, this study identifies the concepts in the CSO that are equivalent to those in the HO.

Our contribution in this paper is to maintain specific concepts and relationships for each domain to reflect the comparison accurately. By comparing the two disciplines, we will be able to identify the similarities and differences between them to facilitate their integration. This paper proposes a promising solution that enables the reader to see both similarities and differences. Moreover, this comparison may lead to the expansion of the compared ontologies or the construction of an ontology that can be applied to both safety and security domains.

Comparing two ontologies can be justified for several reasons, but we will focus primarily on two:

- Often, it is easier to construct a new ontology than to find similarities and differences between existing ontologies and attempt to combine them.
- A combined ontology dictating structure from multiple domains is often needed, rather than having a domain-specific ontology.

As a result of the lack of comparisons of ontologies from different domains, we will have to compare and match knowledge that is represented in different ways. Therefore, we must deal with the challenge of comparing knowledge from different sources as well as dealing with the issue of dealing with different knowledge representations. This issue is addressed by ontology matching, and the critical aspect is establishing a comparison of concepts and relationships between two ontologies. A comparison of two ontologies reveals the following four issues related to ontology matching:

1) Different labels can be applied to concepts.
2) Certain concepts can appear in only one or both ontologies
3) Though concepts can be similar, they are not identical
4) Though concepts can have similar notations, they can have different meanings (semantics)

Alternatively, the issue of comparing and matching ontologies from different domains could be avoided or reduced by utilizing common ontologies, as we did in our case, taking UFO as the fundamental basis.

The remainder of this paper is structured as follows. In Section 2, comparison planning is introduced, and Section 3 presents the related works. In Section 4, HO and CSO are compared, and the results are discussed. Finally, in Section 5, conclusions and future work are included.

II. Research Questions

In this section, the following research questions (RQs) are defined:

RQ1: How do the Hazard Ontology and Combined Security Ontology concepts relate to each other?

RQ2: How do the Hazard Ontology and Combined Security Ontology relationships relate to each other?

In the context of the planned comparison, the HO presented by Zhou et al. [4] and the CSO proposed in our earlier work [5] were compared. The expected results at the end of the comparison provide the answers to the RQs.

III. Related Work

In the security domain, various aspects of ontologies are mainly studied and compared to improve the identification of vulnerabilities, attacks, and intrusions into the system, and assess information security and various threats. Some comparisons between security ontologies can be found in Blanco et al. [7], and Maedche and Staab [8]. A systematic review method was used to identify, select, and analyze the main security ontology proposals in Blanco et al. [7]. Selected ontologies were compared using a formal framework, and it was found that existing ontologies were not prepared for reuse and extension. Attempts to combine the identified ontologies were made, but problems arose related to the use of expressions in natural language to describe the concepts. However, a methodology for measuring the extent to which the ontologies overlapped and matched each other at different semiotic levels was proposed by Maedche and Staab [8]. Based on a comparative study of five ontologies in the same domain, a multi-phase cross-evaluation was conducted to determine the adequacy of proposed measures and the agreement between subjects in the domain ontology [8].

A comparison of five major security ontologies related to cloud computing was presented by Singh and Pandey [9], who pointed out their strengths, weaknesses, and future research directions.

Meriah and Rabai [10] identified relevant concepts in the information security management standard ISO 27001 [11] to gain insights into its structure. Qualitative data analysis was applied to enhance the traceability and transparency of the meta-modeling procedure. It was shown that meta-models could assist in analyzing and comparing multiple ontologies.

With the various comparisons conducted among security ontologies, the works mentioned above were primarily focused on literature reviews, identifying the strengths and weaknesses of security ontologies, and using different methods and frameworks for comparing ontologies with specific meta-models. In contrast to those works, in this study, the HO is compared to the CSO, focusing on identifying differences among concepts and their relationships.

IV. Comparing the Hazard Ontology with the Combined Security Ontology

A comparison between the HO [4] and the CSO [5], as presented in our earlier work [5], is performed in this section. First, the concepts and their relationships are introduced in Unified Modeling Language (UML) diagrams are introduced; and their meanings are briefly described.

As mentioned in Section I, the comparison contributes to the identification of concepts in the CSO that are equivalent to those in the HO. The criterion for comparing concepts is associated with the synonymy of their meanings and their equivalence in the safety and security domains.

The meaning of a concept in an ontology can be defined in various ways, and the use of different concepts can express the same meaning. When an ontology has rich relationships among concepts, the meanings of the concepts are more precise; and

the misinterpretation of vocabulary is reduced. Moreover, a change to the meaning of a concept can result in the addition or removal of a concept in an ontology. Relationships among concepts are also taken into account because they describe the properties or interactions among them.

Figure 1 presents the concepts and relationships of the HO [4]. As shown in Fig. 1, the HO includes 11 concepts and 14 relationships among them.

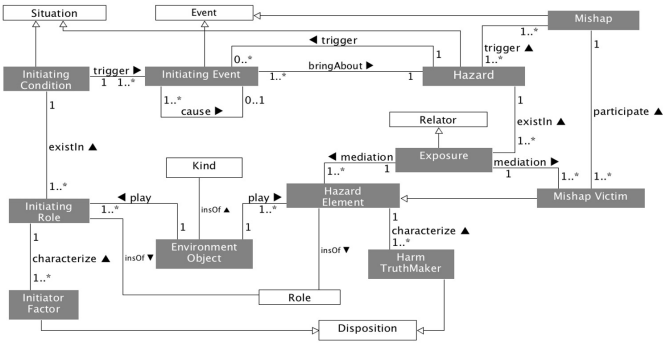

Figure 1. The Hazard Ontology with concepts and relationships [4]

The HO concepts, as defined in [4], have the following meanings:

- **Environment Object** - represents a specific thing or a set of things, such as living beings, objects, and places that '*can play different roles in a hazard or initiating condition*' [4].
- **Mishap Victim** - represents '*a role object that is not supposed to but has the potential to encounter with damages or injuries*' [4].
- **Hazard Element** - represents an active or passive role that can be played by various environment objects and '*can bear harm truthmaker*' [4].
- **Harm Truthmaker** - represents '*the harmful or critical dispositions in a hazard*' [4].
- **Exposure** - represents '*the relations through which victim(s) will be exposed to harms posed by hazard elements*' [4].
- **Initiating Role** - represents a role that '*is necessary constituent parts of an initiating condition to trigger initiating events*' [4].
- **Initiator Factor** - represents a property of the initiating role. It represents the weakness [12] of the initiating role that makes it to contribute to the initiating condition.
- **Initiating Condition** - represents '*a situation that comprises the necessary constituent parts to trigger initiating events*' [4].
- **Initiating Event** - represents '*an undesirable or unexpected event that can bring about a hazard situation*' [4].
- **Hazard** - represents '*a situation whose instances are situations that comprise a set of essential endurants as well as other possible endurants, in order to trigger severe mishaps. An endurant is an entity that exists in time while possessing a unique identity and keeping its identity.*' [4].
- **Mishap** - represents '*an accidental event that will consequently cause injuries to people, damage to the environment or significant financial losses*' [4].

Figure 2 presents the concepts and relationships of the CSO [5]. As shown in Fig. 2, the CSO includes 12 concepts and 37 relationships among them.

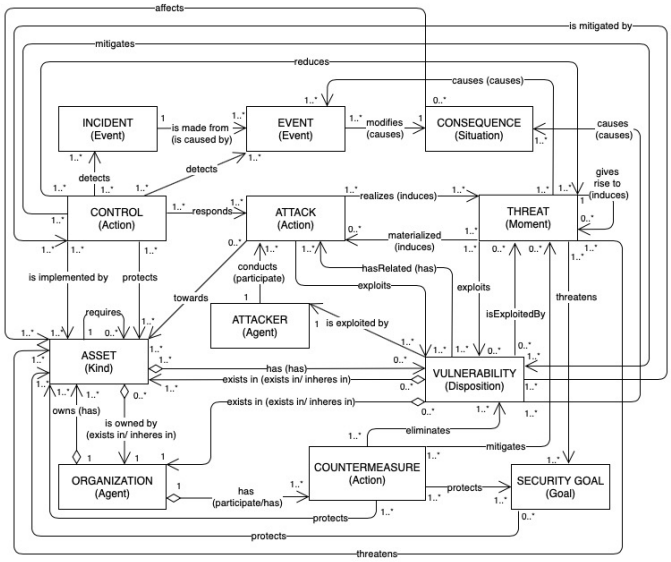

Figure 2. Fundamental concepts and relationships of the Combined Security Ontology [5]

The CSO concepts, as defined in [13], have the following meanings:

- **Asset** - represents '*any resource that has importance and value to the owner and may be the target of a security incident. It can exhibit some weakness that makes it susceptible to exploitation*' [13]. It can be divided into tangible or intangible assets an organization can have. The intangible assets include data, software reputation, or role. The tangible assets include movable (e.g., furniture, IT components, detectors) and immovable assets (e.g., location, buildings, and their elements).
- **Attack** - represents '*unauthorized access to or use of an asset, or a malicious attempt to alter, destroy, disable, expose, gain or steal an asset that an attacker can take by exploiting any vulnerability and producing security events*' [13].
- **Attacker** - represents '*anyone or anything that attempts to alter, destroy, disable, expose, gain or steal an asset by exploiting any vulnerability and producing some security events*' [13].
- **Consequence** - represents '*the possible outcome of an attack or an event (e.g., denial of services), affecting the properties (CIA) of an asset or a security incident caused by an attacker*' [13].
- **Control** - represents '*a mean of managing risk (e.g., policies), which can be administrative, technical, managerial,*

or legal. An attribute assigned to an asset reflects its relative importance or necessity in achieving or contributing to stated goals' [13].

- **Countermeasure** - represents '*a prevention mechanism that detects an incident/event reduces or avoids a threat/an incident's effects, and/or protects an asset and its properties. It can be an action/approach that mitigates or prevents the risk and impacts of an attack or a measure that modifies risk and mitigates defined vulnerabilities by implementing physical (e.g., fire extinguisher) or organizational (e.g., non-smoking policy)*' [13]. It includes cryptography, secure network communication, encryption, access control, backup, intrusion detection system.
- **Event** - represents '*an occurrence or change of a particular set of circumstances*' [13].
- **Incident** - represents '*an anomalous or unexpected event, set of events, a condition, or situation at any time during the life-cycle of a project, product, service, or system*' [13].
- **Organization** - represents '*a group of people and facilities with responsibilities, authorities, and relationships.*' [13].
- **Security Goal** - represents' *confidentiality, availability, integrity, accountability, assurance, anonymity, authentication, authorization, correctness, identification, non-repudiation, policy compliance, privacy, secrecy, and trust.*' [13].
- **Threat** - represents '*a potential cause of an unwanted incident which can harm a system/organization/asset. It includes the types of dangers against a given set of security properties (CIA)*' [13] and can be classified as passive (non-human threat, e.g., system mapping, eavesdropping, statistical attacks on databases), active (human threat, e.g., unauthorized system modification or denial of service attacks), natural (e.g., monsoon, lightning, earthquake), accidental (e.g., hardware failure, liquid leakage), and intentional (e.g., theft or software alternation). It threatens a security goal and an asset, and sometimes a countermeasure can also be a threat.
- **Vulnerability** - represents '*any weakness of an asset or the system that can be exploited by a threat (e.g., security flaws, defects, mistakes in software). It can be influenced directly (intentionally malicious) or indirectly (an unintentional mistake) by human behavior*' [13].

Table I present all unique concepts and relationships of the HO [4] and the CSO [5] ontologies.

Table I
THE UNIQUE CONCEPTS AND RELATIONSHIPS OF THE HO AND A CSO ONTOLOGIES

Concepts	
Hazard Ontology	***Combined Security Ontology***
Environment Object	Asset
Exposure	Attack
Harm Truthmaker	Attacker
Hazard	Consequence
Hazard Element	Control
Initiating Condition	Countermeasure
Initiating Event	Event
Initiating Role	Incident
Initiator Factor	Organization
Mishap	Security Goal
Mishap Victim	Threat
	Vulnerability
Relationships	
bringAbout	affects
causes	cause
characterize	conducts
existIn	detects
mediation	exists in
play	exploits
trigger	eliminates
	gives rise to
	has
	is exploited by
	is implemented by
	is made from
	is owned by
	materialized
	mitigates
	modifies
	owns
	produces
	protects
	realizes
	reduces
	responds
	towards
	threatens

A. Method and Evaluation of Equivalence

To simplify the comparison between HO and CSO concepts and their relationships, the research questions formulated in Section II have been answered in the following subsections. The results of this comparison are presented in Tables II - V, which show the results of the comparisons between HO and CSO concepts and relationships. The method we used to compare the HO and CSO concepts and relationships had three steps [14]:

1) **Label Matching** - comparing the names (syntax) of two concepts or two relationships to determine if they are equal.
2) **Description Matching** - comparing the definitions (semantics) of two concepts to determine if they are equal.
3) **Property Matching** - comparing the properties of two concepts or two relationships related to UFO Ontology types to determine if they are equal.

Due to the lack of an automatic tool that allows comparing ontologies from different domains, the comparison was carried out manually by the authors of this study. All the steps are described in the following subsections.

B. Label Matching

This process includes determining the similarity of the labels, a given surface word for a concept. To compare the similarity of the labels, three types of comparable concepts and relationships were defined:

1) exact sameness,
2) partial sameness, and
3) no sameness.

Although the labels of the two concepts may differ in form, they can function like synonyms.

In comparing the HO and CSO concept labels, we did not find the exact sameness. However, the HO concept **Initiating Event** and the CSO concept **Event** exhibit partial sameness. Therefore, it is trivial to present it in a table.

The results of the comparisons between the HO and CSO relationship labels are presented in Table II.

Table II
LABEL MATCHING OF HO AND CSO RELATIONSHIPS

HO relationships	*CSO relationships*	*Equivalence*
bringAbout	gives rise to, realizes	partial sameness
cause	causes	exact sameness
cause	modifies	partial sameness
existIn	exists in	exact sameness
existIn	is owned by	partial sameness
trigger	causes, gives rise to	partial sameness
characterize		no sameness
mediation		no sameness
play		no sameness

Table II shows that four HO relationships and six CSO relationships had exact or partial sameness when compared. However, HO relationships, including *characterize*, *mediation*, and *play* had no sameness to any of the CSO relationships they were compared to.

C. Description Matching

Description matching is intended to be an optional matching step when a description is attached to a concept. For example, security and safety have different terminology and concept descriptions, but one concept can have the same meaning in both. The description of a concept is created by ontology developers and is selected from the well-known literature [15], reducing the possibility of considering synonymous meanings to identify the equivalent concepts. However, if two concepts refer to the same meaning reference, they can be considered synonymous with each other.

Table III describes the results of the description matching of HO and CSO concepts.

Table III
DESCRIPTION MATCHING OF HO AND CSO CONCEPTS

HO concepts	*CSO concepts*	*Equivalence*
Environment Object	Asset	exact sameness
Environment Object	Organization	exact sameness
Harm Truthmaker	Vulnerability	partial sameness
Hazard	Consequence	partial sameness
Hazard	Event	partial sameness
Hazard	Incident	partial sameness
Initiating Condition	Event	partial sameness
Initiating Condition	Incident	partial sameness
Initiating Condition	Threat	partial sameness
Initiating Event	Event	partial sameness
Initiating Event	Incident	exact sameness
Initiating Event	Attack	partial sameness
Initiator Factor	Vulnerability	exact sameness
Mishap	Event	partial sameness
Mishap	Incident	partial sameness
Exposure		no sameness
Hazard Element		no sameness
Initiating Role		no sameness
Mishap Victim		no sameness

The descriptions of seven HO concepts and eight CSO concepts show exact or partial sameness. However, the descriptions of HO concepts such as **Exposure**, **Hazard Element**, **Initiating Role**, **Mishap Victim** have no sameness when compared with the descriptions of concepts in CSO.

D. Property Matching

Property matching includes the likeliness of properties related to concepts and relationships between ontologies. We assume that the concepts and relationships that contain equivalent property types are likely to be synonymous with each other. Moreover, the properties related to the UFO Ontology types inherited by the concepts and relationships in HO and CSO are also considered attached properties.

The results of comparing the concept properties of HO and CSO ontologies are included in Table IV, which shows that seven HO concepts and five CSO concepts are equivalent.

Table IV
PROPERTY MATCHING OF HO AND CSO CONCEPTS

HO concepts	*UFO Ontology type*	*CSO concepts*	*Equivalence*
Environment Object	Kind	Organization, Asset	exact sameness
Harm Truthmaker, Initiator Factor	Disposition	Vulnerability	exact sameness
Hazard, Initiating Condition	Situation	Consequence	exact sameness
Initiating Event	Event	Event, Incident	exact sameness
Mishap	Event	Event, Incident	exact sameness
Initiating Role	Role		no sameness
Mishap Victim	Kind		no sameness
Exposure	Relator		no sameness
Hazard Element	Role		no sameness

The properties of HO concepts such as **Exposure**, **Hazard Element**, **Initiating Role**, **Mishap Victim** show no sameness with properties of any CSO concept. UFO types, including **Role** and **Relator** in HO, have no equivalents in CSO.

Table V presents the results of property matching HO and CSO relationships.

Table V
PROPERTY MATCHING OF HO AND CSO RELATIONSHIPS

HO relationships	*UFO Ontology type*	*CSO relationships*	*Equivalence*
cause	causes	causes	exact sameness
existIn	exist in	exists in	exact sameness
bringAbout	bringAbout		no sameness
mediation	mediates		no sameness
play			no sameness
trigger	trigger		no sameness

Only two HO relationships, *cause* and *existIn*, have exact sameness with CSO relationships.

The following section discusses the comparisons between HO and CSO concepts and relationships based on the three matching steps.

E. Semantic comparison of HO and CSO

The semantic comparison allows for the consideration of not only the structure of an ontology; but also the sense of

the information contained within it. As a set of fundamental terms in a domain, we use UFO terminology, represented by foundational (top-level) ontology. To understand the relationship between concepts in two ontologies belonging to different domains, it is necessary to examine semantic correspondences (semantic conflict), which can be classified into four categories:

- Semantic equivalence (similarity) – This indicates a 1:1 match between the description of concept C1 in Ontology O1 and the description of concept C2 in Ontology O2. This category was checked during the description matching step of the HO and CSO concepts, as shown in Table III.
- Semantic dissimilarity – This indicates that there is no match between the labels of concept C1 (with name C1) from Ontology O1, and concept C2 (with name C2) from Ontology O2, and Name (C1) = Name (C2). This category was assessed during the label matching step of the HO and CSO concepts.
- Semantic intersection – This refers to the 1:1 match between some part values in concept C1 from the domain of the Ontology O1 and some part values in concept C2 from the domain of the Ontology O2.
- Semantic containment – This indicates that for the concepts C2 from Ontology O2, every value within its domain has a 1:1 match to the value within the concept C1 from Ontology O1 domain, but not vice versa.

However, it may be challenging to define semantic intersection or semantic containment. To perform semantic matching, experts must establish semantic relationships between two sets of ontologies from different domains. Therefore, it is evident that it may be difficult to provide explicit matches between concepts from different ontologies. However, it is necessary to define the relationships between the general concepts derived from a top-level ontology (UFO) and the specific concepts derived from different ontologies (HO and CSO).

Since both ontologies — HO and CSO — contain the UFO taxonomy, we can draw the following summaries:

- Based on UFO-A [6], we can assume that ”Environment Object” (HO) corresponds to "Asset" and "Organization".
- Based on UFO-A [6], we can assume that "Environment object" (Kind) can play the ”Role” (HO) – of ”Attacker” (CSO).
- Based on UFO-B [6], we can assume that ”Complex Event”(Event) corresponds to ”Initiating Event” (HO) and ”Incident” (CSO).
- Based on UFO-C [16], we can also assume that ”Agent” corresponds to ”Attacker” (CSO).
- Based on UFO-C [16], we can assume that ”Action” corresponds to ”Attack” (CSO).
- Based on UFO-C [16], we can assume that ”Intentional Moment” corresponds to ”Threat” (CSO).

However, other CSO concepts, such as ”Countermeasure” (Action), ”Control” (Action), ”Security Goal” (Goal), and ”Threat” (Moment)” have no semantic equivalence to the HO concepts.

V. Discussion

Interoperability between ontologies can only be achieved through matching. Furthermore, comparing ontologies that are not hierarchical and do not belong to the same domain, semantic matching is a laborious and error-prone process.

Our results revealed that the concepts and relationships in HO and CSO are not all comparable. We performed a detailed comparison of 11 concepts and 14 relationships in HO with 12 concepts and 37 relationships in CSO using the three matching steps and found that some of them are equivalent or partially equivalent.

We found that label matching does not primarily capture equivalent concepts and/or relationships in ontologies. As an example, there was only one equivalency identified in label matching for HO and CSO concepts, and there were equivalencies within four HO relationships and six CSO relationships. Many descriptions are attached to the concepts in each of the given ontologies. Description matching revealed equivalencies in seven HO concepts and eight CSO concepts. We found that properties can be successfully used capture synonymous terms. For example, using property matching, seven HO concepts with eight CSO concepts and two HO relationships with two CSO relationships were declared equivalent.

A summary of the results of comparing both ontologies is presented in Table VI.

Table VI
Matching of HO and CSO concepts and relationships

Feature	***HO concepts***	***CSO concepts***
Label	1	1
Description	7	8
Properties	7	5
Label + description	7	8
Label + properties	7	5
Properties + description	7	8
Label + properties + description	7	8
All matches	7	8
Feature	***HO relationships***	***CSO relationships***
Label	4	6
Description	x	x
Properties	2	2
Label + description	4	6
Label + properties	4	6
Properties + description	2	2
Label + properties + description	4	6
All matches	4	6

Focusing on the total sum of equivalents, we found that seven HO concepts are equivalent to eight CSO concepts, and four HO relationships are equivalent to six CSO relationships. Both ontologies are based on UFOs, however, the HO is designed for the safety domain, and the CSO is designed for the security domain.

Furthermore, our study found that current methods of ontology matching are insufficient to capture the context of concepts

and relationships when comparing ontologies from different domains.

As shown above, the concepts of HO and CSO are presented through a UFO-based ontology. The primary distinctions provided by UFO made it easier to compare the contexts of both analyzed ontologies, which belong to two separate domains. Thus, both ontologies employ a UFO-based approach in which the more specific types create groups of a more general type, facilitating, for example, correlations based only on a comparison of their common characteristics.

VI. Conclusion and Future Work

This paper presented a comparison between HO and CSO ontologies using a three-step method to capture equivalent concepts and relationships. This method exploits information within ontological concepts and relationships, including labels, descriptions, and properties. The comparison presented in this paper contributes to identifying equivalent or non-equivalent concepts and relationships in the HO and CSO ontologies. The results of the comparison between the HO and CSO ontologies answer RQ1 and RQ2 as follows:

- Regarding RQ1, the study shows that it is possible to compare the concepts and relationships of the HO and CSO by applying the structured method outlined in Section IV.
- Regarding RQ2, the comparison results allow for the determination of equivalent concepts in CSO and HO. CSO concepts and relationships not equivalent to those in HO can be useful in modifying HO.

Furthermore, the result of this comparison can be caused by the fact that HO is based on concepts derived from UFO-A [6] and UFO-B [6]. However, CSO includes concepts from all three parts: UFO-A [6], UFO-B [6], and UFO-C [16].

Likewise, comparing the HO and CSO ontologies enabled us to observe two situations:

1) when comparing safety and security terminologies and their concept descriptions, some concepts can have the same meaning in both domains, and
2) when comparing the properties of concepts/relationships in both ontologies, some concepts can have exact sameness, especially since both ontologies were created from the same foundational basis (UFO).

The results of this study may have implications for future research by modifying the HO to incorporate the CSO concepts and relationships that were considered in this paper.

We can conclude that our comparison contributes to pointing out the similarities and differences in two ontologies built on the same basis, therefore ensuring seamless interoperability of ontologies from different domains. As a result, in our comparison, we maintain awareness of the relationship between matching and ontologies across domains, contributing to data interoperability. Initially, this is a first step towards comparing and matching ontologies from different domains to address the issues of heterogeneity in the matching process.

Moreover, in terms of various aspects of both safety and security, it may also be possible to propose a modified ontology to address these issues. Therefore, a potential extension of HO is necessary and may enhance the analysis of safety hazards and security threats in cyber-physical systems or systems-of-systems.

Lessons learned from our comparison will facilitate the matching and alignment of ontologies from different domains, allowing researchers to work more effectively. Therefore, our comparison represents a step forward in knowledge interoperability solutions for demanding systems, such as SoS.

Due to the results of this study, some research directions have been suggested:

- How could the HO be extended to incorporate CSO concepts and relationships for the analysis of safety hazards and security threats?
- To what extent do extensions to security cover the needs and concepts of system-of-systems?

Acknowledgment

This work is supported by the projects: Serendipity - Secure and dependable platforms for autonomy, grant nr: RIT17-0009, funded by the Swedish Foundation for Strategic Research (SSF) and by the DPAC - Dependable Platform for Autonomous Systems and Control, grant nr: 20150022, funded by the Knowledge foundation (KKS).

References

[1] B. Tsoumas, D. Gritzalis, "Towards an ontology-based security management," 20th Int. Conference on Advanced Information Networking and Applications, vol. 1, pp. 985–992, 2006.

[2] H. Mouratidis, P. Giorgini, "Integrating security and software engineering: advances and future visions," Idea Group Publishing, 2006.

[3] G. Dobson, P. Sawyer, "Revisiting ontology-based requirements engineering in the age of the semantic web," International Seminar on Dependable Requirements Engineering of Computerised Systems at NPPs, Institute for Energy Technology (IFE), Halden, 2006.

[4] J. Zhou, K. Hänninen, K. Lundqvist, and L. Provenzano, "An ontological interpretation of the hazard concept for safety-critical systems," 27th European Safety and Reliability Conference (ESREL), Portoroz, Slovenia, 2017, pp. 183–185.

[5] M. Adach, K. Hänninen, and K. Lundqvist, "A Combined Security Ontology based on the UFO ontology," 16th IEEE International Conference on Semantic Computing (ICSC), Laguna Hills, CA, USA, 2022, pp. 187–194.

[6] G. Guizzardi, "Ontological foundations for structural conceptual models," PhD thesis, University of Twente, The Netherlands, 2005.

[7] C. Blanco, J. Lasheras, R. Valencia-García, E. Fernández-Medina, A. Toval, and M. Piattini, "A systematic review and comparison of security ontologies," 3rd International Conference on Availability, Reliability and Security, Barcelona, Spain, 2018, pp. 813–820.

[8] A. Maedche, S. Staab, "Comparing ontologies - similarity measures and a comparison study," Institute AIFB, University of Karlsruhe, Internal Report No.408, 2001.

[9] V. Singh, S.K. Pandey, "A comparative study of cloud security ontologies. In: 3rd International Conference on Reliability," Infocom Technologies and Optimization, Noida, India, pp. 1–6, 2014.

[10] I. Meriah, LBA. Rabai, "Comparative study of ontologies based ISO 27001 series security standards," Procedia Comput. Sci., 160, pp. 85–92, 2019.

[11] Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27001:2005, information technology - security techniques - information security management systems - requirements, 2005. [Online]. Available: https://www.iso.org/standard/42103.html

[12] L. Provenzano, K. Hänninen, J. Zhou, and K. Lundqvist, "An ontological approach to elicit safety requirements," 24th Asia-Pacific Software Engineering Conference (APSEC), 2017, pp. 713–718.

[13] M., Adach, K., Hänninen, and K. Lundqvist, "Security Ontologies: A Systematic Literature Review," In: Enterprise Design, Operations, and Computing: 26th International Enterprise Design, Operations and Computing Conference 2022 (EDOC), Bozen-Bolzano, Italy, Springer-Verlag, Berlin, Heidelberg, pp. 36 – 53, 2022.

[14] W. Na Chai, T. Ruangrajitpakorn, M. Buranarach, and T.A., Supnithi, "A framework to generate carrier path using semantic similarity of competencies in job position," Pacific Rim International Conference on Artificial Intelligence (PRICAI), Phuket, Thailand, 2016, pp. 89–97.

[15] S. Pavel, J. Euzenat, "Ontology matching: state of the art and future challenges," IEEE Trans. Knowl. Data Eng. 25(1), pp. 158–176, 2013.

[16] G. Guizzardi, R. Falbo, and G. Guizzardi, "Grounding software domain ontologies in the Unified Foundational Ontology (UFO): the case of the ODE software process ontology," CIbSE, Recife, Pernambuco, Brasil, 2008, pp. 244–251.