# A Combined Security Ontology based on the Unified Foundational Ontology

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}@mdh.se

***Abstract*—While ontology comparison and alignment have been extensively researched in the last decade, there are still some challenges to these disciplines, such as incomplete ontologies, those that cover only a portion of a domain, and differences in domain modeling due to varying viewpoints. Although the literature has compared ontological concepts from the same domain, comparisons of concepts from different domains (e.g., security and safety) remain unexplored. To compare the concepts of security and safety domains, a security ontology must first be created to bridge the gap between these domains. Therefore, this paper presents a Combined Security Ontology (CSO) based on the Unified Foundational Ontology (UFO) that could be compared to or aligned with other ontologies. This CSO includes the core ontological concepts and their respective relationships that had been extracted through a previous systematic literature review. The CSO concepts and their relationships were mapped to the UFO to get a common terminology that facilitates to bridge the gap between the security and safety domains. Since the proposed CSO is based on the UFO, it could be compared to or aligned with other ontologies from different domains.**

***Index Terms*—security ontology, UFO ontology, security concepts, security relationships**

## I. Introduction

The last few years have seen an increase in the number of autonomous vehicles that exchange information. These vehicle's cyber-physical systems must function safely and securely. Therefore, the various issues related to the safety (e.g., malfunction of a vehicle) or security (e.g., unauthorized access) of these autonomous vehicles must be considered.

Although security and safety have historically been considered separately, these domains are closely related [1], [2]. The growing complexity of modern systems and the increasing dependence on information and communication technologies that foster interconnection have intertwined these two domains. In certain contexts (e.g., autonomous vehicles), security and safety issues now concern the same systems and should therefore be considered together. Thus, adopting a common approach to security and safety is important (e.g., for preventing intentional attacks and/or accidental failures). However, overlapping safety and security countermeasures have not yet been mastered, which can lead to undesirable consequences (e.g., loss of critical data).

Ontologies have been independently developed for both domains. In the security domain, however, the high-level concepts such as "asset", "threat", or "vulnerability" cover only a portion of the domain or model the domain from different perspectives. Various ontologies cover the fundamental aspects of the domain and overlap to a limited extent. Therefore, an efficient technique for combining multiple ontologies needs to be developed for the creation and use of ontologies. However, this has proven to be a challenging activity.

Domain ontologies, which introduce concepts in a given domain and their relationships, as well as activities, theories, and basic principles related to the security domain, are reusable in that specific domain [3]. Many ontologies that are devoted to the domains of safety or security, and specific ontology comparison criteria are needed in these domains. A comparison of these ontologies determines which of them has a complete and consistent domain conceptualization. However, the selection process of ontologies depends on linguistic criteria and usability, and other criteria (e.g., completeness). Therefore, before the security and safety ontologies are compared, a security ontology that facilitates the comparison to a safety ontology, must be created.

In our previous research, a systematic literature review was performed and the core concepts and relationships of security ontologies [4] were extracted. Our paper concluded that the identified core concepts and relationships provided a good framework for the creation of a new security ontology. The quality of the resulting security ontology would depend on quality of the security ontologies (e.g., content, presentation, usage) from which it was created. Therefore, to ensure the quality of the resulting security ontology, this paper proposed a Combined Security Ontology (CSO) based on the UFO Ontology (UFO) [5] and the security ontologies [6]–[13]. The CSO also contains relationships extracted from additional security ontologies that were not included in our previous paper [4], (e.g., those by Vorobiev and Bekmamedova [14], and by Massacci et al. [15]).

This paper addressed the following general research question: *"How can we create a security ontology based on the UFO Ontology that can be compared to or aligned with other ontologies?"*

To resolve this question and to create the CSO, the two methods proposed by Fernandez et al. [16] and Jones et al. [17] were combined. Additionally, the CSO concepts and their relationships were mapped to the UFO to close the gap between the security and safety domains. The UFO was chosen as the

2022 IEEE 16th International Conference on Semantic Computing (ICSC) | 978-1-6654-3418-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICSC52841.2022.00039

978-1-6654-3418-8/22/$31.00 ©2022 IEEE
DOI 10.1109/ICSC52841.2022.00039

basis for creating a new security ontology because it proposes a complete set of foundational concepts and relationships that cover important aspects of the safety policy development; the foundational concepts of the UFO include aspects of safety and were thus suitable for this work. The goal of the CSO is to provide a meta-model that included knowledge related to security concepts and various aspects thereof, such as "attacks" and "threats". To bridge the gap between the safety and security domains, the CSO concepts and their relationships were mapped to the Unified Foundational Ontology (UFO) [5], and their properties were consolidated. The aim was also for the CSO to be comparable to the Hazard Ontology (HO) [18], an ontology that has successfully incorporated well-established concepts from the UFO and is used in the safety domain. Therefore, the contribution of this paper was three-fold:

1) We propose a Combined Security Ontology (CSO) that included core concepts and relationships extracted from the systematic literature review that was presented in our earlier paper [4].
2) The completeness, validity, and applicability of the proposed ontology is shown, as it identified vulnerabilities of an autonomous quarry site, such as assets and technologies that were susceptible to threats or attacks.
3) The CSO concepts and relationships were mapped to the UFO, and their properties were consolidated to bridge the gap between the security and safety domains.

The remainder of this paper is organized as follows: In section 2, a background on UFO Ontology is presented. In section 3, the CSO creation process is explained, and a practical application of the proposed ontology is demonstrated on an autonomous quarry site. In section 4, the validation process of the CSO is presented. In section 5, the mapping process for the CSO and UFO ontologies is described. In section 6, the related work on ontology development methodologies and the ways in which they relate to the proposed paper is described. Finally, in section 7 the conclusions and suggestions for future work are presented.

## II. Background

The UFO [5] was adopted as the basis for this paper because it has been successfully used in many areas of research, including the analysis, integration, and re-engineering of various modeling languages (e.g., Unified Modeling Language (UML), Reference Model of Open Distributed Processing (RM-ODP)) [19]–[21] Furthermore, the UFO reuses basic concepts and relationships to represent a given subject domain, facilitates the operability of ontologies developed according to the same foundational ontology, and provides guidelines for the correct application of its concepts. Additionally, various studies have provided details about the different layers and ontological concepts of the UFO [5], [22], [23].

Based on the formal theory of the part-whole relationships, the UFO is a recent and successfully employed foundational ontology for conceptual modeling [24]. Furthermore, this ontology deals with universals and particulars and is used to formulate theories in areas including the philosophy of language [25], [26] and cognitive psychology (e.g., kinds, roles, states) [5]. The UFO consists of three primary layers that allow for a detailed and accurate representation of many domains for different applications. These are as follows: UFO-A, or the endurant ontology, which defines terms like "universal", "role", "relator", and "intrinsic moment" [5]; UFO-B, or the event ontology, which defines terms like "event", "state", "atomic event", and "complex event" [27]; UFO-C, or social agent's ontology, which defines terms like "social object", "social role", "social agent", "normative description" [27].

The UFO considers many of the structural aspects of conceptual modeling that have not been considered by other ontologies such as various types of entities and their relationships, their parts and properties [28]. Many other foundational ontologies (e.g., a Hazard Ontology (HO) [18]) have successfully incorporated well-established concepts from the UFO. The OntoUML language, which was based on the Unified Modeling Language (UML), was created by UFO researchers to facilitate the use of UFO concepts and address various language problems (e.g., ambiguities, semantic interoperability, different level of abstractions, possible contradictions in concept descriptions) [5].

## III. Creation of a Combined Security Ontology (CSO)

The main contribution of this paper is the proposed CSO based on the UFO [5]. The method used to create the CSO was adapted from a combination of two methods proposed by Fernandez et al. [16] and Jones et al. [17]. The creation process included six steps: goal, scope, knowledge acquisition, conceptualization, implementation, and validation. The security concepts and relationships among them were obtained through a systematic literature review presented in our earlier work [4]. After the creation process was complete, the concepts and relationships of the CSO and UFO were mapped [5].

In the knowledge acquisition step, the information needed to create the CSO was collected from various sources, such as ontologies provided by Herzog et al. [6], by Fenz and Ekelhart [7], by Agrawal [8], by Schumacher [9], by Pereira and Santos [10], by Wang and Guo [11], by Ramanauskaite et al. [12], by Dritsas et al. [13], by Vorobiev and Bekmamedova [14], by Massacci et al. [15]. The information was then organized into a conceptual model (along with the concepts and their relationships) during the conceptualization step. The created conceptual model of the CSO was then extended to include concepts mapped from the UFO [5]. In the implementation step, the CSO was described using unified modeling language (UML) diagrams. Then, in the validation step, the use case is presented to ensure that the resulting ontology corresponded to what it was supposed to represent. The first five steps of ontology creation are detailed in the following subsections, while the validation step is presented in Section IV.

### A. Goal of the CSO

The main goal of the security ontology is to provide a meta-model that included knowledge of security concepts

and relationships, such as ”threats”, ”vulnerabilities”, ”attacks”, ”countermeasures”, etc. The ontology is created from the reviewed security ontologies [6]–[13] by integrating the standard-compliant security concepts and their relationships. The CSO is created to bridge the gap between the safety and security domains for future work and to draw comparisons with the HO, proposed by Zhou et al. [18]. Some of the challenges caused by the lack of such a CSO are undefined, complex threats and vulnerabilities in modern systems that can impact safety aspects.

### *B. Scope of the CSO*

Based on our systematic literature review, presented in [4], a CSO that included core concepts and relationships from the security domain and allowed the identification of security issues is needed. Further details on the security concepts covered by the ontology are provided in Section III-D.

### *C. Knowledge Acquisition*

The goal of knowledge acquisition is identifying and collecting the knowledge needed to create a new security ontology. For this paper, knowledge acquisition began with the existing security ontologies in the literature. The core concepts and relationships extracted from the eight security ontologies were analyzed which were extracted in our previous systematic literature review [4]. Through the literature review process, a gap between the safety and security domains (e.g., lack of concepts and relationships that cover safety aspects) was identified. The following is a summary of the eight security ontologies and their analyses:

1) Schumacher [9] provided an ontology with nine concepts and 12 relationships to maintain the security pattern repositories with a general security pattern search engine.
2) Dritsas et al. [13] provided a specialized ontology with seven core concepts and nine relationships for the e-poll domain and described the usefulness of the ontology for dealing with security issues in software projects.
3) Fenz and Ekelhart [7] provided a ontology with 11 concepts and 15 relationships to propose a unified and formal body of knowledge for the information security domain.
4) Herzog et al. [6] provided an overview of information security ontologies based on the Web Ontology Language and proposed an ontology that contained six concepts and seven relationships.
5) Wang and Guo [11] provided the ontology for vulnerability management (OVM) with six concepts and 10 relationships that focused on software vulnerabilities and captured the core concepts of information security.
6) Pereira et al. [10] provided an ontology with eight concepts and 16 relationships that aimed to unify the concepts and terminology of information security in accordance with the ISO/IEC_JTC1 [29] to support the implementation of management to facilitate decision-making related to security information issues.
7) Ramanauskaite et al. [12] provided an ontology with five concepts and seven relationships that was mapped with the security standards (e.g., ISO/IEC 27001 [30], ISSA 5173 [31], NISTIR 7621 [32], and PCI DSS [33]) to decrease the complexity of mapping and increase the usability of multiple security standards in organizations.
8) Agrawal [8] provided an ontology with 11 concepts and 16 relationships that specified the concepts of ISO 27005 [34] and included risk management standards and relationships.

More detailed summaries of these ontologies can be found in our earlier work [4].

### *D. Conceptualization*

The goal of conceptualization is to structure the acquired knowledge into a conceptual model that captures the core concepts of the knowledge and their relationships [16]. In [4], the core concepts were organized and mapped to the following security standards: NIST SP 800-160 [35], NIST SP 800-30 rev.1 [36], NIST SP 800-27 rev.A [37], ISO/IEC 27001 [30] and NISTIR 8053 [38]. As a result of this mapping, 12 core concepts and their relationships were identified and then combined in a conceptual model of the ontology, as shown in Fig. 1.

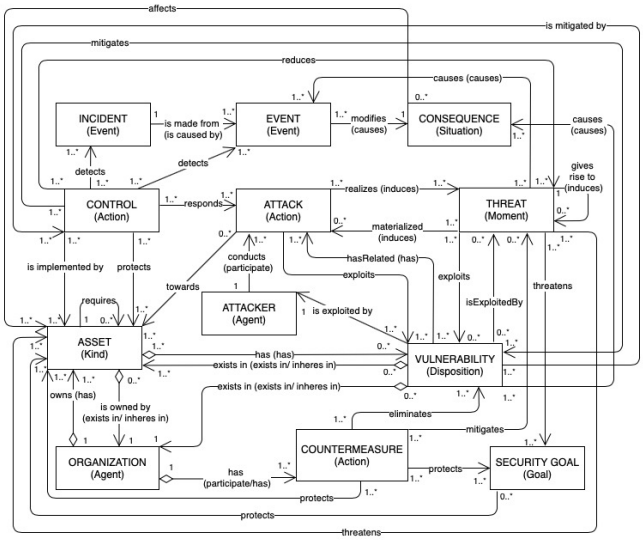


Fig. 1. The proposed Combined Security Ontology based on Unified Foundational Ontology [5]

The names of the core concepts and their relationships in the CSO were selected based on their relevance for capturing security issues, the frequency of their appearance in the selected papers, and their limitations to a high-level of abstractions (e.g., high-level domain concepts). When a concept had a different name in the analyzed ontologies [6]–[10], [23] (e.g., ”an attacker” or ”an agent”), the general name consistent with the security standard was selected (in this case, ”an attacker”).

The definitions of the 12 core concepts mapped to the security standards are described in our earlier work [4]. The standard-compliant concepts were divided into three dimensions – organizational, risk, and treatment – which are con-

sidered modules in ontology engineering. The organization dimension includes concepts that capture the system´s social and technical components in terms of their objectives, capabilities, and dependencies (e.g., assets). The risk dimension contains concepts that capture risks at the social and organizational levels (e.g., attacks). Finally, the treatment dimension relates to concepts that capture countermeasure techniques to mitigate threats and attacks (e.g., controls) [39].

The ontology proposed by Fenz and Ekelhart [7] divided the concepts into three groups: enterprise (e.g., "asset"), location (e.g., "location"), and security (e.g., "threat"). However, the classification of the concepts proposed in this paper improved the understanding and organization of security knowledge and was based on the security meta-model presented in Mayer [40]. The classification and descriptions of concepts and relationships are described in the following subsections.

Among 12 core concept, 35 relationships were identified. To complete the CSO, the two following relationships "affects" [14], "protects" [15] were added.

All core concepts and relationships of the CSO are presented in Table I and II, and descriptions of all aforementioned concepts are presented in our earlier paper [4].

TABLE I
THE CORE CONCEPTS AND RELATIONSHIPS OF OUR PROPOSED COMBINED SECURITY ONTOLOGY

| **Author** | ***Concepts*** | ***Relationships*** |
|---|---|---|
| Herzog et al. [6] | asset, countermeasure, security goal, threat, vulnerability | *has, protects, protects, threatens, threatens* |
| Fenz and Ekelhart [7] | asset, control, organization, threat, vulnerability | *is exploited by, is implemented by, is mitigated by, is owned by, gives rise to, requires* |
| Agrawal [8] | asset, consequence, control, event, organization, threat, vulnerability | *causes, mitigates, modifies, owns* |
| Schumacher [9] | attack, threat, vulnerability | *exploits, realizes* |
| Pereira and Santos [10] | asset, attack, control, event, incident, threat | *detects, detects, is made from, materialized, protects, reduces, responds, towards* |
| Wang and Guo [11] | attack, attacker, consequence, vulnerability | *is exploited by, attackConsequence, causes, conducts, hasRelated* |
| Ramanauskaite et al. [12] | asset, countermeasure, organization, threat, vulnerability | *eliminates, existsIn, existsIn, exploits, has, mitigates* |
| Dritsas et al. [13] | asset, attacker, countermeasure, threat | |
| Vorobiev and Bekmamedova [14] | asset, consequence | *affects* |
| Massacci et al. [15] | asset, security goal | *protects* |

Descriptions of all aforementioned concepts are presented in detail in our earlier paper [4].

### E. Implementation of the CSO

The goal of this step was to implement the CSO in a formal language. UML diagrams have been chosen for this step because has a good support for expressing ontologies (e.g., class diagram) and provide a way to check the consistency of the ontology. Furthermore, because UML has a large set of notations (e.g., activities, components), it could clearly present the ontology, allowing the CSO to provide the necessary security knowledge in a formalized and explicit form. Following the guidelines for ontology creation [16], [17] and coding the UML diagrams, the CSO with well-defined concepts and relationships was created.

TABLE II
DIMENSIONS OF OUR PROPOSED COMBINED SECURITY ONTOLOGY

| **Dimension** | ***Concepts*** | ***Relationships*** |
|---|---|---|
| Organizational | asset, organization | protects, has, exists in, requires, is implemented by, towards, affects, threatens, owns, is owned by |
| Risk | attack, attacker, consequence, event, incident, threat, vulnerability | conducts, is exploited by, exploits, causes, produces, realizes, exploits, gives rise to, is made from, modifies |
| Treatment | security goal, control, countermeasure | protects, threatens, prevents, detects, mitigates, reduces, protects, eliminates |

Fig. 1 presents the CSO with its related concepts and their relationships. The rectangles represent the core concepts, and the lines and arrows represent their relationships with a reading direction. Cardinality constraints are labeled on each end of the relationships. The 12 core concepts related to the security domain (written with capital letters) were grounded in eight foundational concepts in the UFO (written in parentheses), such as "action", "agent", "disposition", "event", "goal", "kind", "moment", "situation". Of the 37 relationships related to the security domain, only 15 with the UFO relationships (written in parentheses) could be mapped, as shown in Fig. 1.

## IV. VALIDATION OF THE CSO

Validation aims to ensure that the created ontology meets the needs of its use (e.g., the ontology corresponds to the represented system) [16]. Since our goal was to create a CSO that included core concepts and their relationships, the following criteria such as **completeness, validity** and **applicability** were considered. These criteria are discussed in greater detail in the following sections:

### A. Completeness

Completeness was evaluated by mapping the created ontology and some other ontologies extracted from the literature (mainly on the security ontologies that were used in our systematic literature review) [4]. The completeness criterion was used to verify the integrity of the existing knowledge in other security ontologies that were included in the CSO. By this criterion, we tried to prove that the created ontology was more complete than the security ontologies in the literature. The ontology alignment (shown in Table III) contained our ontology concepts on the left side and the concepts of the security ontologies used in our earlier work [4] on the right side.

The concepts of "asset" and "threat" were used in all compared ontologies, expect that proposed by Wang and Guo

TABLE III
THE ALIGNMENT OF THE CSO AND THE SECURITY ONTOLOGIES THAT WERE USED IN OUR SYSTEMATIC LITERATURE REVIEW

| | Security ontologies | | | |
|---|---|---|---|---|
| **CSO** | **Agrawal [8]** | **Herzog et al. [6]** | **Schumacher [9]** | **Fenz and Ekelhart [7]** |
| Asset | Asset | Asset | Asset | Asset |
| Attack | | | Attack | |
| Attacker | | | Attacker | |
| Consequence | Consequence | | | |
| Control | Control | | | Control |
| Countermeasure | | Countermeasure | Countermeasure | |
| Event | Event | | | |
| Incident | | | | |
| Organization | Organization | | | Organization |
| Security Goal | | Security Goal | | |
| Threat | Threat | Threat | Threat | Threat |
| Vulnerability | Vulnerability | Vulnerability | Vulnerability | Vulnerability |
| **CSO** | **Ramanauskaite et al. [12]** | **Pereira and Santos [10]** | **Wang and Guo [11]** | **Dritsas et al. [13]** |
| Asset | Asset | Asset | | Asset |
| Attack | | Attack | Attack | |
| Attacker | | | Attacker | Attacker |
| Consequence | | | Consequence | |
| Control | | Control | | |
| Countermeasure | Countermeasure | | Countermeasure | Countermeasure |
| Event | | Event | | |
| Incident | | Incident | | |
| Organization | Organization | | | |
| Security Goal | | | | |
| Threat | Threat | Threat | | Threat |
| Vulnerability | Vulnerability | Vulnerability | Vulnerability | |
| **CSO** | **Vorobiev and Bekmamedova [14]** | **Massacci et al. [15]** | | |
| Asset | Asset | Asset | | |
| Consequence | Consequence | | | |
| Security Goal | | Security Goal | | |

[11]. Furthermore, the ontologies proposed by Schumacher [9], Wang and Guo [11], and Pereira and Santos [10] used the concept of "attack". The concept of "attacker" was used by Schumacher [9], Wang and Guo [11], and Dritsas et al. [13], and the concept of "consequence" was used by Agrawal [8], Wang and Guo [11] and Vorobiev and Bekmamedova [14]. The ontologies proposed by Agrawal [8], Fenz and Ekelhart [7], and Pereira and Santos [10] included the concept of "control". The concept of "countermeasure" was used by Herzog et al. [6], Schumacher [9], Ramanauskaite et al. [12], Wang and Guo [11], and Dritsas et al. [13]. Only the ontologies used by Pereira and Santos [10], and Agrawal [8], included the concept of "event". The concept of "incident" was used by Pereira and Santos [10], while the concept of "security goal" was used by Herzog et al. [6] and Massacci et al. [15]. The concept of "organization" was used by Fenz and Ekelhart [7], Agrawal [8], and Ramanauskaite et al. [12]. All the ontologies included the concept of "vulnerability", expect the ontology proposed by Dritsas et al. [13]. Thus, because of the integration of all other security ontologies, the CSO was more complete than those described in our systematic literature review [4]; every concept found in those ontologies was included in the CSO.

### B. Validity

Validity was checked to ensure that the ontology could provide reliable answers to a set of questions using its terminology. Conforming to Uschold [41], informal and formal questions can be used to validate an ontology. Following the work of Fox et al. [42], the CSO by applying competency questions (CQs) was validated and then the correctness of the results for the questions was checked. The ontology was applied to the security domain, as shown in Fig. 2.

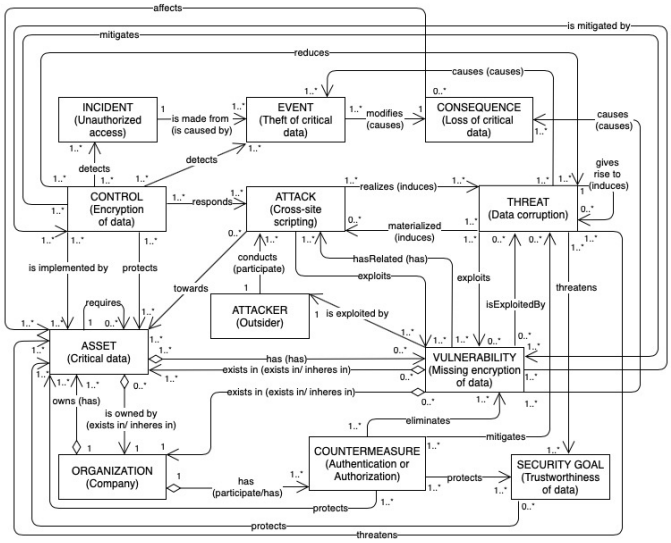

Fig. 2. An application of our proposed Combined Security Ontology

Questions were used that were likely to arise when analyzing the security of a cyber-physical system. Thus, the questions were indicative of how the proposed ontology could be applied. The formulation of the CQs was an iterative process (as shown in Table IV) that ended when all CQs were answered.

TABLE IV
VALIDATION OF OUR COMBINED SECURITY ONTOLOGY WITH RESPECT TO DIMENSIONS

| **Dimension** | ***Competency Questions*** | ***Answers*** |
|---|---|---|
| Organizational | Who owns the assets? | Organization |
| | What are the assets to be protected in an organization? | Critical data |
| Risk | What is the threat that threaten an asset? | Data corruption |
| | Who is responsible for an attack? | Outsider |
| | Which are the existing vulnerabilities? | Missing encryption of data |
| | Which are the existing attacks? | Cross-site scripting |
| | What is the consequence that causes an attack? | Loss of critical data |
| | What incident can be detected by a control? | Unauthorized access |
| | What is an event caused by a threat? | Theft of critical data |
| Treatment | Which Security Goal can mitigate a vulnerability? | Confidentiality of critical data |
| | What is the method used by an organization to mitigate a threat? | Intrusion detection |
| | What is the security action to prevent an attack? | Authentication of data |

The dimensions that correspond to the CQs are presented in the first column of the table. Each of the CQs is expressed informally in natural language in the second column. The answers to the CQs are presented in the last column and in Fig. 2. The goal of validation step was to verify if the CSO was following set of CQs. This step has demonstrated how the CSO could be exploited in the security of cyber-physical system.

### C. Applicability

Applicability was demonstrated with an industrial scenario to show that the proposed CSO can be applied in a real-life application context to identify security issues.

Fig. 3 presents an autonomous quarry site use case that included autonomous and remote-controlled vehicles.

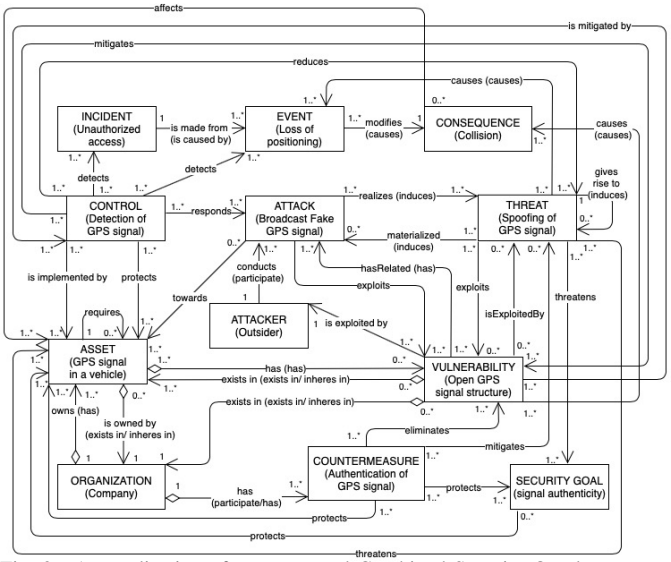

Fig. 3. An application of our proposed Combined Security Ontology on an autonomous quarry site

The quarry site uses smart devices for information-gathering and data transmission among vehicles and devices. The smart devices are used to control the autonomous vehicles and detect their needs and to monitor the arrival and usage of materials from the quarry site. Different technologies are also used for data transmissions inside and outside of the quarry site. The quarry site has some security concerns (e.g., unauthorized access) that could affect the autonomous vehicles, communication, and production, and could therefore lead to potential critical problems (e.g., loss of positioning or collision).

Applying the CSO in this autonomous quarry site helped secure the data communication and transmission among the autonomous vehicles, smart devices, and cloud infrastructure. The CSO identified the quarry site assets and technologies´ vulnerabilities (e.g., open GPS signal structure) that were vulnerable to attacks or threats, as well as possible paths that could be used by an attacker to exploit the GPS signal of the autonomous vehicles to achieve target.

The rationale behind the CSO example is structured as follows: ”An organization has a countermeasure protective security goal that protects an asset. An asset has a vulnerability that can be exploited by an attacker, who conducts an attack. An attack produces a threat that is reduced by a control. A control detects an incident that is made from an event. An event modifies a consequence that affects an asset that is owned by an organization”.

In the use case, an autonomous vehicle used GPS signal to track and report its position; thus, an attacker could use GPS spoofing to transmit inaccurate coordinates or hide the location of the vehicle. Thus, the CSO enabled the identification of quarry site asset and technologies´ vulnerabilities that were vulnerable to attacks or threats.

## V. Mapping of the Concepts and Relationships of the CSO and UFO

The concepts and relationships of the CSO and UFO [5] were mapped using the following five steps (as shown in Tab V).

TABLE V
CRITERIA FOR CSO AND UFO CONCEPTS AND RELATIONSHIPS MAPPING

| ***Criteria*** | ***CSO concepts*** | ***UFO concepts*** |
|---|---|---|
| 1. name | event | event |
| 2. meaning | vulnerability | disposition |
| 3. property | asset | kind |
| ***Criteria*** | ***CSO relationships*** | ***UFO relationships*** |
| 4. name | has | has |
| 5. property | materialized | induces |

The concepts or relationships could be identical to each other in terms of name, meaning, or property. The definitions of UFO concepts can be found in [5], [22], [43]. The results of mapping the concepts and relationships of the CSO and UFO are presented in Table VI.

To bridge the gap between the created CSO and UFO, a set of mapping was performed, as described below. A given concept in the CSO was mapped to a concept in the UFO. For example, the rule ”Asset (CSO) corresponds to Kind (UFO)” means that the concept of ”asset” in the CSO was mapped to the concept of ”kind” in the UFO. The results showed that all concepts of the CSO could to be mapped to the UFO concepts.

The mapping of relationships of both ontologies, was as follows: ”has”/”owns” (CSO) corresponds to ”has” (UFO) meant that the relationships ”has”/”owns”/”hasRelated” in the CSO were mapped to the relationship ”has” in the UFO. The relationship ”is made from” in the CSO was mapped to the relationship ”is caused by” in the UFO. The relationships ”causes”/”modifies” in the CSO were mapped to the relationship ”causes” in the UFO. The relationships ”conducts”/”has” in the CSO were mapped to the relationship ”participate” in the UFO. The relationships ”gives rise to/materialized”/”realizes” in the CSO were mapped to the relationship ”induces” in the UFO. The relationships ”exists in”/”is owned by” in the CSO were mapped to the relationships ”exists in”/”inheres in” in the UFO. However, the relationships ”exploits”, ”detects”, ”threatens”, ”protects”, ”reduces”, ”mitigates”, ”eliminates”, ”responds”, ”towards”, ”is exploited by”, ”is implemented by” in the CSO could not be mapped to the relationships in the UFO. The results showed that only 15 of 37 relationships (e.g., ”has”, ”hasRelated”, ”owns”, ”exists in”, ”exists in”, ”is owned by”, ”conducts”, ”is made from”, ”has”, ”causes”, ”causes”, ”modifies”, ”gives rise to”, ”materialized”, ”realized”) of

the CSO could be mapped to the seven relationships (e.g., ”has”, ”exists in”, ”inheres in”, ”participate”, ”is caused by”, ”causes”, ”induces”) in the UFO, as shown in Table VI.

TABLE VI
MAPPING OF CONCEPTS AND RELATIONSHIPS BETWEEN THE CSO AND UFO ONTOLOGIES

| *CSO concepts* | *UFO concepts* | *CSO relationships* | *UFO relationships* |
|---|---|---|---|
| Asset | Kind | has, owns | has |
| Vulnerability | Disposition | hasRelated | has |
| Consequence | Situation | conducts | participate |
| Security Goal | Goal | is made from | is caused by |
| Event | Event | has | participate/has |
| Incident | Event | causes, modifies | causes |
| Attack | Action | gives rise to | causes |
| Countermeasure | Action | exists in | exists in/inheres in |
| Control | Action | is owned by | exists in/inheres in |
| Threat | Moment | materialized | induces |
| Attacker | Agent | realizes | induces |
| Organization | Agent | | |

This mapping of concepts and their relationships between the CSO and UFO, as well as the consolidation of their properties, is the preliminary step to bridging the gap between the safety and security domains. The results showed that all CSO concepts can be mapped to UFO concepts. However, only 15 of the 37 CSO relationships can be identical with the UFO relationships. These results can simplify future comparisons of finding similarities and differences between them.

## VI. RELATED WORK

In this section, the related work concerning ontology development are presented. Although some ontology development methodologies exist, none of them are viewed as the gold standard.

Dutta et al. [44] introduced Yet Another Methodology for Ontology (YAMO) and illustrated the creation of a food ontology.

Jones et al. [17] provided an overview of existing ontology methodologies and proposed guidelines for developing a complete and consistent conceptual model from scratch or adapting existing ontologies for other uses. While Vorobiev and Bekmamedova [14] devised the IDEF5 procedure for the development, modification, and maintenance of ontologies. This procedure introduced a set of guidelines for organizing and scoping, data collection and analysis, initial ontology development, and refinement and validation [45].

The CommonKADs methodology, which was presented by Blanco et al. [46] and Pereira and Santos [10] is an approach to creating an ontology for engineering knowledge-based systems that includes adopting and stressing modular design, redesign, and reuse. In this methodology, an ontology is selected from a library of small-scale ontologies by defining the type of task and domain and the problem-solving method required. It is further developed by mapping the vocabularies of different ontologies. A representative selection of appropriate ontologies from the literature and the refinement thereof was presented by Schreiber et al. [47]

Fernandez et al. [16] proposed **Methontology**, an ontology development method that emphasizes reengineering and/or reusing existing ontologies. This methodology consists of specification, conceptualization, formalization, integration, and implementation stages, which can be applied in seven steps. The purpose of the ontology is defined, the requisite knowledge is acquired, the domain terms are identified, the ontology of the Ontolingua standard-unit is incorporated, and knowledge acquisition, evaluation, and documentation are conducted. While a significant proportion of ontology development methodologies, including the first two approaches described above, seeks to develop low-level, domain-specific ontologies, **Methontology** [16] enables the development of ontologies at the knowledge level and provides detailed instruction for the activities that must be performed when building an ontology. **Methontology** was combined with the method proposed by Jones et al. [17]. These methods were combined to create the CSO because they allowed easy modification and implementation after ontology development and improved the complexity of the conceptual model.

## VII. CONCLUSIONS AND FUTURE WORK

In this paper, the core concepts and relationships extracted from our previous systematic literature review [4] were used to create a CSO based on the UFO [5] and other security ontologies [6]–[13]. The definitions of 12 CSO concepts to the relevant UFO concepts [5] were mapped, and the relationships of the CSO and UFO were mapped. The CSO with a simplified example of an autonomous quarry site was validated and the ontology's applicability in a real-life context was demonstrated.

The primary goal of the CSO was to provide a meta-model that included knowledge about security concepts (”asset”, ”attack”, ”attacker”, ”consequence”, ”control”, ”countermeasure”, ”event”, ”incident”, ”organization”, ”security goal”, ”threat”, and ”vulnerability”) and the relationships thereof. The completeness of this CSO as it related to existing security ontologies was evaluated, and a use case demonstrated that it could be applied to identify security issues. Thus, this work showed that the proposed ontology was useful for security analysis and improved the identification of potential security vulnerabilities and threats.

This paper can be considered as the first step in proposing a well-defined ontology to address the causes and consequences of safety risks and security threats. The CSO was created and mapped to the UFO to bridge the gap between the safety and security domains for future work. As part of future work we intend to compare the CSO with the HO [18] to identify additional security concepts and relationships that can be added to the HO. Then we will evaluate the effectiveness of the complete safety-security ontology.

## ACKNOWLEDGMENT

This work is supported by the Serendipity project funded by the Swedish Foundation for Strategic Research (SSF) and by the DPAC project funded by the Knowledge foundation (KK-Stiftelsen).

## REFERENCES


[1] M. B. Line, O. Nordland, L. Røstad, and I. Tøndel, "Safety vs. security?" in *PSAM*, New Orleans, USA, 2006.

[2] E. Schoitsch, "Design for safety and security of complex embedded systems: a unified approach," in *NATO Advanced Research Workshop on Cyberspace Security And Defence: Research Issues*, Gdansk, Poland, 2005, pp. 161–174.

[3] G. van Heijst, G. Schreiber, and B. J. Wielinga, "Using explicit ontologies in KBS development," *Int. J. Hum. Comput. Stud.*, vol. 46, no. 2, pp. 183–292, 1997.

[4] M. Adach, K. Hänninen, and K. Lundqvist, "Structured information retrieval of security ontologies," MDH, Tech. Rep., (2021), Accessed on October 1, 2021. [Online]. Available: http://www.es.mdh.se/publications/6218-

[5] G. Guizzardi, "Ontological foundations for structural conceptual models," Ph.D. dissertation, Univ. of Twente, Netherlands, 2005.

[6] A. Herzog, N. Shahmehri, and C. Duma, "An ontology of information security," *Int. J. Inf. Secur. Priv.*, vol. 1, no. 4, pp. 1–23, 2007.

[7] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *ASIACCS*, Sydney, Australia, 2009, pp. 183–194.

[8] V. Agrawal, "Towards the ontology of ISO/IEC 27005: 2011 risk management standard," in *HAISA*, Frankfurt, Germany, 2016, pp. 101–111.

[9] M. Schumacher, *8. A theoretical model for security patterns*. Berlin Heidelberg: Springer, 2003, vol. 2754, pp. 121–140.

[10] T. Pereira and H. Santos, "An ontology approach in designing security information systems to support organizational security risk knowledge," in *KEOD*, Barcelona, Spain, 2012, pp. 461–466.

[11] J. Wang and M. Guo, "Ovm: an ontology for vulnerability management," in *CSIIRW*, Oak Ridge Tennessee, USA, 2009, pp. 34:1–34:4.

[12] S. Ramanauskaite, D. Olifer, N. Goranin, and A. Cenys, "Security ontology for adaptive mapping of security standards," *Int. J. Comput. Commun. Control*, vol. 8, no. 6, pp. 878–890, 2013.

[13] S. Dritsas, L. Gymnopoulos, M. Karyda, T. Balopoulos, S. Kokolakis, C. Lambrinoudakis, and S. Gritzalis, "Employing ontologies for the development of security critical applications," in *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government*. Boston, MA: Springer, 2005, pp. 187–201.

[14] A. Vorobiev and N. Bekmamedova, "An ontology-driven approach applied to information security," *J. Res. Pract. Inf. Technol.*, vol. 42, no. 1, pp. 61–76, 2010.

[15] F. Massacci, J. Mylopoulos, F. Paci, T. Tun, and Y. Yu, "An extended ontology for security requirements," in *Advanced Information Systems Engineering Workshops*. Berlin, Heidelberg: Springer, 2011, pp. 622–636.

[16] M. Fernández-López, A. Gómez-Pérez, and N. Juristo, "Methontology: from ontological art towards ontological engineering," in *AAAI Spring Symposium*, Stanford, USA, 1997, pp. 33–40.

[17] D. Jones, T. Bench-Capon, and P. Visser, "Methodologies for ontology development," in *IT and KNOWS Conference of the 15th IFIP World Computer Congress*, Vienna/Budapest, 1998, pp. 62–75.

[18] J. Zhou, K. Hänninen, K. Lundqvist, and L. Provenzano, "An ontological interpretation of the hazard concept for safety-critical systems," in *ESREL*, Portoroz, Slovenia, 2017, pp. 183–185.

[19] J. P. Almeida, E. C. S. Cardoso, and G. Guizzardi, "On the goal domain in the RM-ODP enterprise language: An initial appraisal based on a foundational ontology," *EDOCW*, pp. 382–390, 2010.

[20] A. Bringuente, R. Falbo, and G. Guizzardi, "Using a foundational ontology for reengineering a software process ontology," *J. Inf. Data Manag.*, vol. 2, no. 3, pp. 511–526, 2011.

[21] E. Eessaar and R. Sgirka, "An ontological analysis of metamodeling languages," in *ISD*. New York: Springer, 2011, pp. 381–392.

[22] G. Guizzardi, G. R. Wagner, R. Falbo, R. Guizzardi, and J. Almeida, "Towards ontological foundations for the conceptual modeling of events," in *ER*, vol. 8217. Berlin Heidelberg: Springer, 2013, pp. 327–341.

[23] R. Guizzardi, G. Guizzardi, A. Perini, and J. Mylopoulos, "Towards an ontological account of agent-oriented goals," in *SELMAS*, vol. 4408. Berlin Heidelberg: Springer, 2006, pp. 148–164.

[24] M. Verdonck and F. Gailly, "Insights on the use and application of ontology and conceptual modeling languages in ontology-driven conceptual modeling," in *ER*, vol. 9974. Cham: Springer, 2016, pp. 83–97.

[25] J. MacNamara, *A Border Dispute, the Place of Logic in Psychology*. Cambridge, Mass.: MIT Press, 1986.

[26] J. Leeuwen, "Individuals and sortal concepts: an essay in logical descriptive metaphysics," Ph.D. dissertation, Univ. of Amsterdam, Netherlands, 1991.

[27] G. Guizzardi, R. Falbo, and R. Guizzardi, "Grounding software domain ontologies in the unified foundational ontology (UFO): the case of the ode software process ontology," in *CIbSE*, Recife, Pernambuco, Brasil, 2008, pp. 244–251.

[28] A. Lalis, R. Patriarca, J. Ahmad, G. Gravio, and B. Kostov, "Functional modeling in safety by means of foundational ontologies," *Transportation research procedia*, vol. 43, pp. 290–299, 2019.

[29] ISO/IEC_JTC1, "ISO/IEC FDIS 27005: information technology - security techniques - information security risk management," International Organization for Standardization, Tech. Rep., 2008.

[30] ISO, "ISO 27001:2013: information security management system-requirements," International Organization for Standardization, Tech. Rep., October 2013.

[31] ISSA-UK, "Information security for small and medium–sized enterprises," Information System Security Association, Tech. Rep., 2011.

[32] C. Paulsen and P. Toth, "NISTIR 7621 small business information security: The fundamentals," *National Institute of Standards and Technology (NIST), US Department of Commerce. Retrieved January*, 2016.

[33] Payment Card and Industry, "Payment card industry data security standard (PCIDSS)," PCI-Security Standard Council, Tech. Rep., 2006. [Online]. Available: https://www.commerce.uwo.ca/pdf/PCI_DSS_v3-2-1.pdf

[34] ISO/IEC, "ISO 27005:2011: information technology — security techniques — information security risk management," International Organization for Standardization, Tech. Rep., 2011.

[35] R. Ross, M. McEvilley, and J. Oren, "NIST SP 800-160, systems security engineering considerations for a multidisciplinary approach in the engineering of trustworthy secure systems," *National Institute of Standards Technology, US Department of Commerce, Gaithersburg, MD, USA, Tech Report NIST SP*, pp. 800–160, 2016.

[36] R. Ross, "NIST SP 800-30 REV. 1: guide for conducting risk assessments," *National Institute of Standards Technology*, 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[37] G. Stoneburner, C. Hayden, and A. Feringa, "NIST SP 800-27 REV. A. engineering principles for information technology security (a baseline for achieving security), revision a," *National Institute of Standards and Technology (NIST)*, 2004.

[38] S. L. Garfinkel, "NISTIR 8053: de-identification of personal information," *National Institute of Standards and Technology (NIST)*, 2015.

[39] M. Gharib, P. Giorgini, and J. Mylopoulos, "Towards an ontology for privacy requirements via a systematic literature review," in *ER*, vol. 10650, Valencia, Spain, 2017, pp. 193–208.

[40] N. Mayer, "Model-based management of information system security risk," Ph.D. dissertation, University of Namur, Belgium, 2009.

[41] M. Uschold, "Building ontologies: Towards a unified methodology," in *16th Annual Conf. of the British Computer Society Specialist Group on Expert Systems*, Cambridge, UK, 1996, pp. 1–18.

[42] M. S. Fox, J. F. Chionglo, and F. G. Fadel, "A common-sense model of the enterprise," in *Industrial and Engineering Applications of Artificial Intelligence and Expert Systems*. Norcross GA: Institute for Industrial Engineers, 1993, pp. 425–429.

[43] G. Guizzardi and G. R. Wagner, "Using the unified foundational ontology (UFO) as a foundation for general conceptual modeling languages," in *Theory and Applications of Ontology: Computer Applications*. Dordrecht: Springer, 2010, pp. 175–196.

[44] B. Dutta, U. Chatterjee, and D. P. Madalli, "Yamo: Yet another methodology for large-scale faceted ontology construction," *J. Knowl. Manag.*, vol. 19, pp. 6–24, 2015.

[45] B. Perakath, "The idef5 ontology description capture method overview," *Texas, USA: Knowledge Based Systems Inc.*, 1994.

[46] C. Blanco, J. Lasheras, R. Valencia-García, E. Fernández-Medina, J. Álvarez, and M. Piattini, "A systematic review and comparison of security ontologies," in *ARES*, Barcelona, Spain, 2008, pp. 813–820.

[47] A. T. Schreiber, B. J. Wielinga, W. N. H. Jansweijer, A. Anjewierden, and F. van Harmelen, "The kactus view on the 'o' word," in *IJCAI*, vol. 20, Montreal, Quebec, Canada, 1995, pp. 15.1–15.10.