

An Ontological Approach for Hazard Analysis Representation Aligned with IEC61508: A Hydrogen Case Study

Thorvaldur Jochumsson^{1,*}, Mehrdad Saadatmand², Kaj Hänninen¹ and Kristina Lundqvist¹

¹Department of Computer Science and Engineering, Mälardalen University, Sweden

²RISE Research Institutes of Sweden, Sweden

Abstract

Safety-critical systems require continuous hazard analysis throughout their lifecycle. This requires establishing and maintaining an accurate representation of hazard knowledge based on safety terminology defined in relevant standards. Such representation becomes difficult when the terminology lacks conceptual clarity, giving rise to ambiguities, alternative interpretations, and inconsistencies.

This paper presents an ontological approach to hazard-analysis representation based on applying conceptual safety and domain ontologies derived from safety standardisation to specify an application ontology and a corresponding knowledge base.

The approach is demonstrated within the hydrogen domain through the development of an application ontology and a knowledge base representing hazard scenarios for a hydrogen energy facility. The evaluation assesses whether information required by selected IEC61508 requirements can be represented in the knowledge base and retrieved through querying.

While the evaluation indicates that hazard knowledge associated with the selected IEC61508 requirements can be represented using the proposed ontological structure, the paper also discusses practical implications of the approach. These include how the conceptual ontologies are further specialised in the application ontology, the construction of a knowledge base through interpretation of a hazard analysis, and the role of abstract safety concepts in knowledge-base queries.

Keywords

ontology engineering, hazard analysis, functional safety, IEC61508, hydrogen safety

1. Introduction

The functional safety standard IEC61508 [1] serves as a foundation for many domain-specific standards, including those for the process industry [2], the automotive industry [3], and the railway sector [4]. As such, IEC61508 provides domain-independent normative requirements for establishing safety across entire system lifecycles. These requirements represent safety knowledge through generic abstract concepts introduced by the standard. Together, these concepts constitute a conceptual framework for communication and interoperability across safety-critical sectors.

The IEC61508 safety terminology is introduced through natural language in the form of definitions and descriptions. However, natural language is subject to interpretation, leading to ambiguities and inconsistencies that have emerged within and across domain-specific standards derived from IEC61508 [5, 6, 7]. As the same safety terminology is used when representing hazard knowledge and hazard analyses at the application level, similar interpretative challenges may arise in safety applications and development activities.

This work presents a representation of hazard analysis through an ontological structure spanning safety, domain, and application ontologies. The scope of the representation is limited to the hazard-

Proceedings of the Joint Ontology Workshops (JOWO) - Episode XII: The Tropical Spring of Ontology, co-located with the 16th International Conference on Formal Ontology in Information Systems (FOIS 2026), September 21-22, 2026, Vitória (ES), Brazil

*Corresponding author.

✉ thorvaldur.jochumsson@mdu.se (T. Jochumsson); mehrdad.saadatmand@mdu.se (M. Saadatmand); kaj.hanninen@mdu.se (K. Hänninen); kristina.lundqvist@mdu.se (K. Lundqvist)

ORCID 0009-0004-9898-9386 (T. Jochumsson); 0000-0002-1512-0844 (M. Saadatmand); 0000-0003-0757-822X (K. Hänninen); 0000-0003-0904-3712 (K. Lundqvist)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

analysis objectives as defined in IEC61508, including potential hazards associated with a control system, their causal sequences, and their consequences. The approach is modular, intended to support reuse of ontological representations of hazard knowledge across domains and applications while maintaining consistent conceptual interpretations of IEC61508 safety terminology.

The approach is demonstrated within the hydrogen domain through the development of an application-level hazard-analysis ontology and the instantiation of a knowledge base representing hazard scenarios from a hydrogen energy facility. The main implications observed during development, instantiation, and evaluation are identified and discussed. These include how conceptual safety and domain ontologies can be specialised toward hazard-analysis representation, how knowledge-base construction remains an interpretative process when formalising hazard analyses expressed in natural language, and how abstract safety concepts can be used to formulate generic queries over application-level hazard knowledge.

Overall, the evaluation indicates that the conceptual structures provided by the safety and domain ontologies can be preserved through application-level specialisation and knowledge-base instantiation. Information associated with selected IEC61508 requirements can be represented and retrieved through queries based on abstract safety concepts, illustrating how generic safety concepts remain applicable at the application level. While the evaluation indicates a structured and consistent representation of the selected hazard-analysis knowledge, further work is required to assess its applicability across different domains and applications.

The remainder of this paper is structured as follows. Section 2 presents background and previous work. Section 3 introduces the ontological approach investigated in this work. Section 4 outlines the applied safety and domain ontologies. Section 5 presents the application ontology. Section 6 describes the knowledge base. Section 7 discusses and concludes the paper.

2. Background

Ambiguities and inconsistencies in safety terminology have been addressed in several previous works. Schnieder et al. discuss inconsistencies in railway safety and security terminology [7], while Hogganvik et al. demonstrate that risk-related terminology is interpreted inconsistently across contexts of use [5]. Several ontological approaches have been proposed to provide explicit conceptual representations of safety knowledge. Kaindl et al. [6] developed a core ontology of safety-risk concepts based on terminology from several safety standards, providing conceptual clarification across domains. Zhou et al. [8] proposed a generic hazard ontology for safety-critical systems based on an ontological interpretation of hazard-related concepts. Jochumsson et al. proposed HO61508, a modular hazard ontology based on IEC61508 [9], where HO61508 focuses on conceptual representation of IEC61508 terminology, providing a generic foundation for domain-specific standardisation. Through the hydrogen domain ontology H2HO, Jochumsson et al. further demonstrated how domain-specific hazard concepts can be explicitly situated within the conceptual framework of HO61508 and the generic safety concepts of IEC61508.

Although previous work has focused on conceptual representation and domain-level extension of safety terminology, less attention has been given to how such conceptual structures can support representation of application-level safety activities, such as hazard analyses. To the best of our knowledge, it remains unclear how hazard knowledge derived from engineering activities can be represented while preserving the conceptual structure established at the standard and domain levels. This challenge motivates the investigation presented in this paper.

3. Ontological Representation

The overall ontological approach is based on separating safety, domain, and application ontologies, where the distinction between domain and application ontologies is adopted from Guarino [10], illustrated in Figure 1.

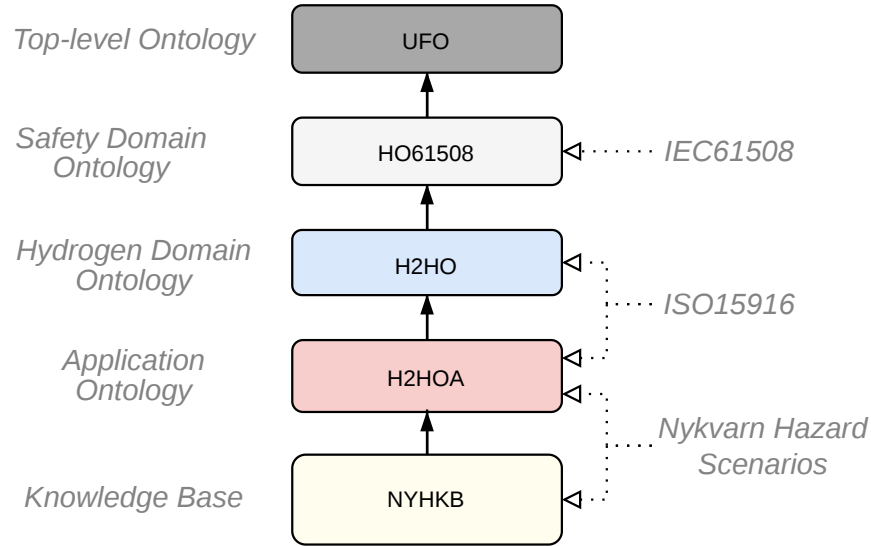


Figure 1: Hazard analysis ontological representations, distinguished according to their level of generality.

The top-level ontology, Unified Foundational Ontology (UFO) [11], describes general and domain-independent concepts, such as *Event* that refers to an occurrence that unfolds in time. The safety domain ontology HO61508 describes generic hazard concepts in IEC61508, such as *HarmfulEvent*, representing an *Event* leading to harm. The hydrogen domain ontology H2HO describes hydrogen-specific hazard concepts by specialising concepts in HO61508, such as *Combustion* as a specialisation of *HarmfulEvent*. The application ontology, called H2HOA¹, further specialises concepts in H2HO and introduces application-specific concepts, such as *Fireball* as a specialisation of *Combustion*. Finally, the knowledge base, called NYHKB², instantiates H2HOA by representing hazard-related phenomena identified in hazard scenarios for the hydrogen energy facility Nykvarn.

HO61508 and H2HO were chosen as the conceptual foundation for the application ontology because they provide explicit ontological representations of IEC61508 safety concepts. UFO was maintained as the top-level ontology to support direct reuse and further specialisation of these ontological structures.

This work applies classical ontology engineering practices [12, 13] for the development of the application ontology H2HOA and the knowledge base NYHKB, including the activities of *capture*, *coding*, and *evaluation*. The *capture* activity concerns identification and interpretation of hazard concepts from relevant standards, domain knowledge, and hazard analyses. The *coding* activity concerns the formal representation of these concepts through ontological specialisation, extending the conceptual structures of HO61508 and H2HO toward the application ontology H2HOA and the knowledge base NYHKB. The *evaluation* activity concerns whether information associated with the selected IEC61508 requirements can be represented and retrieved through the resulting ontological structures.

Positioned within the broader ontology engineering framework LOT [14], this work corresponds to the ontology implementation phase, while selected normative requirements from IEC61508 constitute functional ontology requirements defined as competency questions. The implementation activities of *capture* and *coding* are further guided by hazard definitions and descriptions from IEC61508, ISO15916, and the Nykvarn hazard analysis, with the competency questions subsequently formalised as SPARQL queries for the *evaluation* activity.

¹The H2HOA ontology is publicly available via <https://w3id.org/jochumsson/h2hoa>.

²The NYHKB knowledge base is publicly available via <https://w3id.org/jochumsson/nyhkb>.

4. Domain Ontologies (HO61508 and H2HO)

Figure 2 presents the hazard ontology HO61508, based on IEC61508, and the hydrogen domain extension H2HO, based on ISO15916, proposed by Jochumsson et al. [9]. While their primary contribution was to improve conceptual consistency across safety standardisation, the resulting ontological representations are explored in this work as a structured foundation for application ontologies.

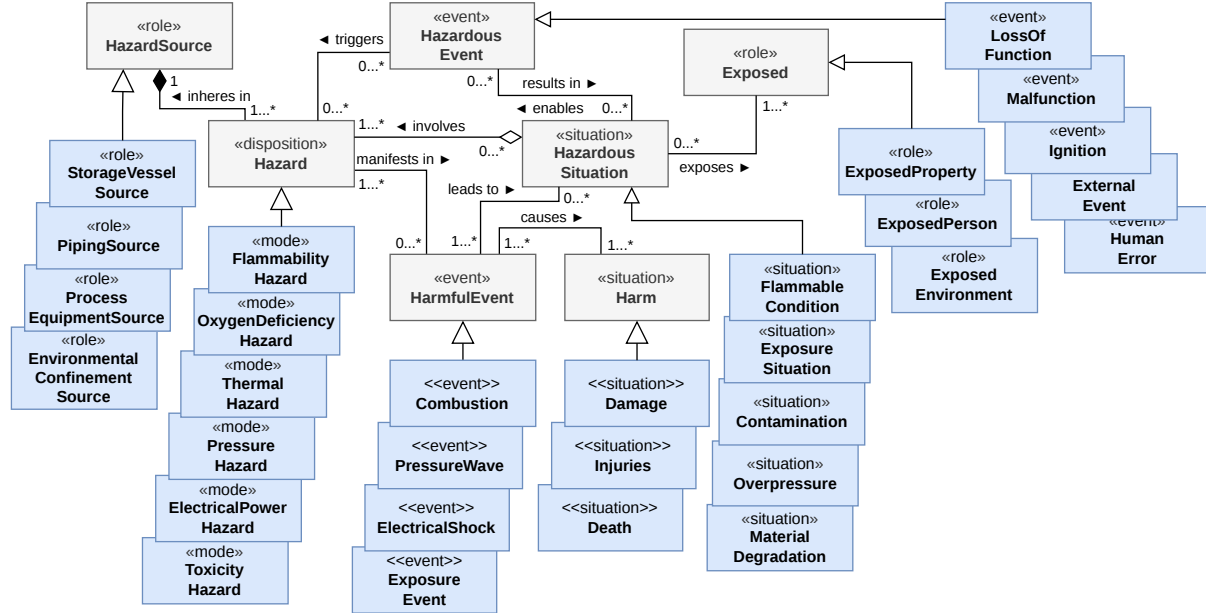


Figure 2: HO61508 and H2HO, ontological representations of IEC61508 and ISO15916 hazard concepts. HO61508 concepts are presented in gray and H2HO concepts are presented in blue. The figure illustrates how hydrogen-specific hazard concepts are represented through specialisation of the generic hazard concepts introduced in HO61508.

A central ontological interpretation in HO61508 is the representation of Hazard as a `ufo:Disposition`, aligned with the IEC61508 definition “potential source of harm”. A hazard is therefore represented as an enduring property of an entity rather than as an event or situation, which are common alternative representations [8]. This interpretation distinguishes the hazard itself from the events through which it may be manifested and the situations in which it may be involved. For example, the hydrogen-specific concept `FlammabilityHazard` in H2HO represents the potential for combustion associated with the flammability property of hydrogen, rather than combustion itself.

HO61508 introduces the roles `HazardSource` and `Exposed`, while H2HO further specialises these roles toward the hydrogen domain. These role-based concepts support application-ontology specialisation, guiding how application and domain entities can be related to abstract safety concepts. For example, the `HazardSource` role may be played by a storage vessel which, in a given situation, exposes a person playing the `Exposed` role.

HO61508 distinguishes between events and situations that form part of the causal sequence leading to hazard manifestation and those representing the resulting consequences. `HazardousEvent` and `HazardousSituation` represent causal events and situations, while `HarmfulEvent` and `Harm` represent the consequences resulting from hazard manifestation. This explicit separation of concepts according to their role in the hazard sequence is of importance when representing hazard analysis.

5. Application Hazard Ontology (H2HOA)

In accordance with Guarino’s description of domain and application ontologies [10], the application ontology H2HOA describes concepts, relations, and constraints that further specialise the generic concepts presented in the domain ontologies HO61508 and H2HO. This presents three main challenges

for an application ontology intended for hazard-analysis representation. Firstly, the application ontology must provide *representations of domain and application entities* that may participate in hazard scenarios. Secondly, the application ontology must introduce *application specialisation* through additional concepts and relations required for hazard-analysis representation. Finally, the application ontology must express *application constraints* that support knowledge-base instantiation and automatic reasoning.

5.1. H2HOA Representation of Domain Entities

The application ontology H2HOA extends the domain ontologies with representations of domain and application entities that participate in hazard scenarios. An important aspect is determining what needs to be represented and at what level of granularity or abstraction. In this work, the initial scope of domain and application entities is guided by requirements concerning hazard representation defined in IEC61508, Part 1, listed in Table 1. These requirements further support the evaluation by describing information that is required to be represented and retrievable through querying.

Table 1

Selected requirements related to representation of domain entities for hazard-analysis from IEC61508, Part 1.

Req.	Scope Entities	Ontological Implication
7.2.2.2	The likely sources of hazards, hazardous situations and harmful events	Further specialise HazardSource with hydrogen entities and their relations to Hazard
7.3.2.1	Define equipment, systems and humans associated with hazards and hazardous events	Represent equipment, systems and humans as domain entities and their relations to Hazard and HazardousEvent
7.3.2.2	Specify physical equipment, including EUC and EUC control systems	Represent physical equipment, systems and control systems as domain entities
7.3.2.3	The external events to be taken into account in the hazard and risk analysis shall be specified	Further specialise the concept ExternalEvent
7.3.2.4	Equipment and systems associated with hazards and hazardous events	Represent equipment and their relations to Hazard and HazardousEvent
7.3.2.5	The type of initiating events that need to be considered (for example component failures and human error) shall be specified	Further specialise the concept HazardousEvent
7.4.2.10	Components contributing to hazardous events	Represent entities participating in HazardousEvent

The conceptual model HO61508 provides the role-based concepts HazardSource, representing the bearer of a Hazard, and Exposed, representing entities exposed through a HazardousSituation. These concepts provide support for several of the relationship requirements identified in Table 1. However, no corresponding role-based concepts are defined for entities associated with HazardousEvent or HazardousSituation, as required by 7.2.2.2 and 7.3.2.4. This reflects the conceptual interpretation of Hazard as a Disposition, which requires an explicit bearer, whereas HazardousEvent and HazardousSituation are represented as events and situations whose conceptual representations do not intrinsically depend on a source entity.

Figure 3 presents the representation of domain entities adopted for H2HOA in order to support the requirements listed in Table 1. At a high level, it comprises the concepts HazardousComponent, ExposedEntity, and PhysicalLocation. HazardousComponent represents components associated with a Hazard, via HazardSource, HazardousEvent, or HazardousSituation. ExposedEntity represents physical entities exposed to a Hazard or through a HazardousSituation. PhysicalLocation represents locations by which the hazard analysis is organised.

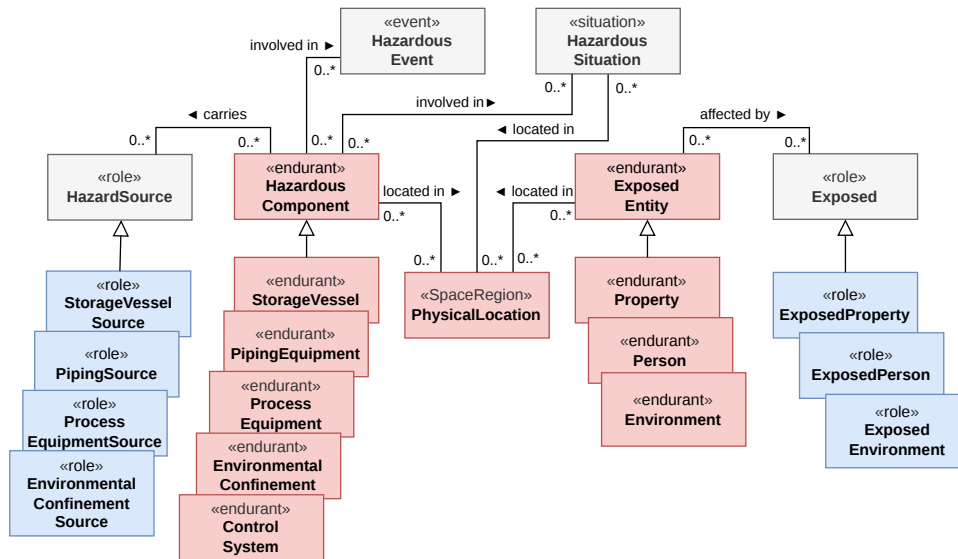


Figure 3: H2HOA representation of domain entities and their relations to the safety ontologies HO61508 and H2HO. H2HOA concepts are presented in red, while HO61508 and H2HO concepts are presented in gray and blue.

5.2. H2HOA Application Specialisation

While domain ontologies, HO61508 and H2HO, provide conceptual representations of generic and hydrogen-specific hazard concepts, hazard analysis requires a level of detail that goes beyond the granularity they provide. Table 2 summarises selected IEC61508 requirements that directly influence the concept specialisation and are later used for evaluation purposes. In addition to the requirements themselves, the table presents their ontological implications, identifying the concepts and relations that require further representation or specialisation in H2HOA.

Table 2

Selected requirements related to further specialisation of concepts for hazard-analysis representation from IEC61508, Part 1.

Req.	Short Description	Ontological Implication
7.2.2.2	Hazards, hazardous situations, harmful events and their likely sources	Represent hydrogen specialisations of Hazard, HazardousSituation, and HazardousEvent, and their relations to HazardousComponent
7.2.2.3	Hazard characteristics such as duration, intensity, toxicity, flammability and explosive conditions	Further specialise the concepts Hazard and FlammabilityHazard
7.3.2.5	Initiating events including component failures, procedural faults, human errors and dependent failures	Further specialise the concept HazardousEvent
7.4.2.3	Hazards, hazardous events and hazardous situations under all reasonably foreseeable circumstances	Further specialise the concepts Hazard, HazardousSituation, and HazardousEvent
7.4.2.4	Event sequences leading to hazardous events	Represent relations between Hazard, HazardousSituation, and HazardousEvent
7.4.2.6	Consequences associated with hazardous events	Further specialise the concepts HarmfulEvent and Harm, and represent their relations

As a representative example of how generic hazard concepts are further specialised, Figure 4 presents how requirement 7.4.2.6 is supported in H2HOA through specialisation of the domain concept Combustion to represent different combustion phenomena.

Introducing application-level specialisation for one concept may require corresponding specialisation of related concepts in order to preserve domain semantics. For example, in the hydrogen safety literature,

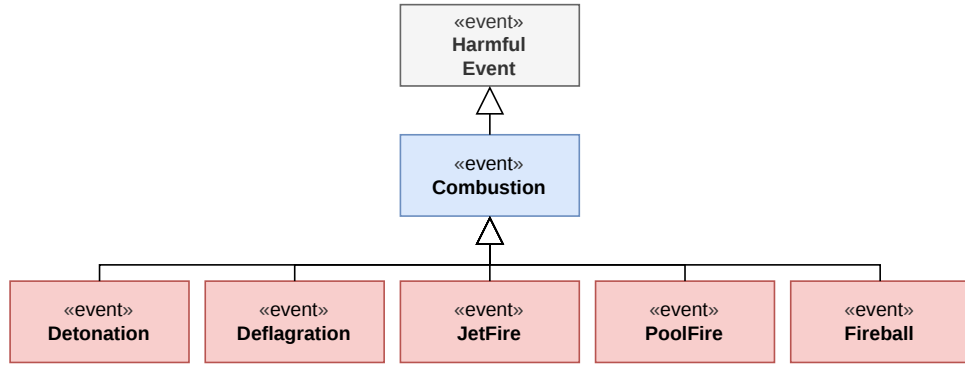


Figure 4: Representative hazard-analysis specialisation of the concepts HarmfulEvent and Combustion, illustrating the increased granularity of hazard knowledge requested by requirement 7.4.2.6 in Table 2.

different combustion types are associated with different ignition mechanisms, where detonation requires high-energy ignition. Representing such relations therefore requires Ignition to be specialised at a level of granularity that reflects the specialisation introduced for Combustion.

5.3. H2HOA Application Constraints

While the application ontology increases in size and complexity through the increased number of domain entities and application-level specialisations, maintaining the intended entity relations during knowledge base construction and maintenance becomes increasingly difficult. These relations represent domain knowledge that can be made explicit through constraints and assessed through automated reasoning during instantiation.

For example, the constraints expressed in Equation 1 and Equation 2 capture that Combustion is manifested through FlammabilityHazard, which in turn is triggered by Ignition³. This expresses the domain semantics that combustion requires ignition and flammability.

$$h2ho:Combustion \sqsubseteq \forall h2hoa:manifestedBy.h2ho:FlammabilityHazard \quad (1)$$

$$h2ho:FlammabilityHazard \sqsubseteq \forall h2hoa:triggeredBy.h2ho:Ignition \quad (2)$$

Together, these constraints represent semantics at an abstract level but remain too generic to capture domain-specific knowledge. Consequently, additional logical constraints are introduced for application-level specialisations. For example, Equations 3 and 4 constrain Detonation to be manifested through DetonationHazard, which in turn is triggered by HighEnergyIgnition. This expresses the domain semantics that detonation requires high-energy ignition. The example illustrates how application-level specialisations require corresponding specialisation of constraints and reinforces the need for a homogeneous level of abstraction across related concepts.

$$h2hoa:Detonation \sqsubseteq \forall h2hoa:manifestedBy.h2hoa:DetonationHazard \quad (3)$$

$$h2hoa:DetonationHazard \sqsubseteq \forall h2hoa:triggeredBy.h2hoa:HighEnergyIgnition \quad (4)$$

With constraints, such as those illustrated in this section, H2HOA supports the intended inference of relations across application-level specialisations during knowledge base construction and maintenance. For example, if a Combustion is manifested by a hazard other than FlammabilityHazard, or if a DetonationHazard is triggered by an Ignition that is not classified as HighEnergyIgnition, automated reasoning can identify the inconsistency with the ontology constraints.

³Using `h2hoa:manifestedBy` and `h2hoa:triggeredBy`, inverses of `ho61508:manifestsIn` and `ho61508:triggers`.

6. Nykvarn Hazard Analysis Knowledge Base (NYHKB)

The instantiation of the application ontology H2HOA as the knowledge base NYHKB, together with querying of the resulting knowledge base, forms the evaluation activity of this work. The evaluation assesses whether information associated with the selected IEC61508 requirements can be represented and retrieved through the ontological structures introduced in H2HOA. It comprises both the structured instantiation of hazard-analysis knowledge and assessment of its retrieval through querying. The evaluation also considers how the logical constraints introduced in H2HOA support consistency checking and inference during knowledge-base instantiation. This section first describes the *NYHKB instantiation* and then presents the *NYHKB querying* of hazard-analysis knowledge with respect to the selected IEC61508 requirements.

6.1. NYHKB Instantiation

The Nykvarn hazard analysis⁴, used as a basis for the knowledge base, is divided into descriptions and risk assessments of different hazards with respect to their physical locations. The descriptions are provided at a relatively high level of abstraction, reflecting hazard analysis performed during early stages of system development. A hazard is introduced with a description of the physical location, followed by descriptions of the causes and consequences of the hazard. This follows common engineering practices and addresses the requirements presented in Tables 1 and 2. Table 3 summarises a representative hazard scenario from the Nykvarn hazard analysis concerning an uncontrolled release of hydrogen in the location where hydrogen production and consumption take place.⁵

Table 3

Hydrogen release hazard description for the equipment room extracted from the Nykvarn hazard analysis.

Element	Description
Physical location	Equipment room containing electrolyser, dryer and fuel cell used for hydrogen production and consumption.
Hazard	Uncontrolled release of hydrogen.
Cause	Incorrect installation of hydrogen production or consumption equipment, or external physical influence on equipment.
Hazardous situation	Formation of an explosive atmosphere following hydrogen release.
Hazardous event	Ignition of the explosive atmosphere by nearby ignition sources.
Consequence	Fire or explosion causing damage to people and property.

Representing hazard scenarios, such as the one presented in Table 3, as a knowledge base introduced challenges related to the ambiguities and alternative interpretations that this work seeks to address. For this reason, instantiation was not merely a process of transforming a hazard analysis expressed in natural language into a knowledge base, but also a process of interpretation.

Abstract descriptions in Table 3, such as representing the hazard as an uncontrolled release of hydrogen, required interpretation to be decomposed into the more precise structures provided by H2HOA. Causal dependencies, such as the formation of an explosive atmosphere, are expressed implicitly and stated at a high level of abstraction. Related hazard information therefore had to be reconstructed explicitly within H2HOA through additional interpretation, including decisions regarding how implicitly stated entities and relations should be represented.

As such, the instantiation relied on interpretation rather than direct transformation from text to ontology. To structure this process, H2HOA was used as a framework from which a set of ontological questions was derived to guide the construction of NYHKB. Table 4 illustrates the outcome of applying these questions to the hazard scenario presented in Table 3.

⁴Nykvarn refers to a hydrogen energy facility located at Nykvarn 4, Västmanland, Sweden, assessed for hydrogen production, storage, and use.

⁵A comprehensive list of hazard scenarios used in this study is available at <https://github.com/jochumsson/h2hoa/blob/main/empirical-hazard-scenarios.txt>.

Table 4

Example results of the H2HOA instantiation questions for the equipment room hazard scenario in Table 3.

Ontological question	Example interpretation
Identified Hazards?	JetFireHazard, DeflagrationHazard, and FireballHazard (specialisations of FlammabilityHazard)
Identified domain entities?	Location_TechnicalRoom; Component_Electrolyser, Component_Dryer, Component_FuelCell, Component_TechnicalRoom_Enclosure; ExposedEntity_Personnel
Identified HazardousSituations and exposed entities?	Situation_ExplosiveAtmosphere_TechnicalRoom and Situation_FlammableCloud_TechnicalRoom exposing personnel and property (ExposedRole_Person, ExposedRole_Property)
Identified HazardousEvents?	Event_LowPressureRelease_TechnicalRoom; Event_HotSurfaceIgnition_TechnicalRoom, Event_StaticSparkIgnition_TechnicalRoom
Identified causal relations?	LowPressureRelease resultsIn explosive-atmosphere and flammable-cloud situations; situations enable ignition events; ignition events trigger JetFireHazard, DeflagrationHazard, and FireballHazard; hazards manifestIn JetFire, Deflagration, and Fireball
Identified HarmfulEvents and Harm?	HarmfulEvent_JetFire_TechnicalRoom, HarmfulEvent_Deflagration_TechnicalRoom, HarmfulEvent_Fireball_TechnicalRoom causing BurnInjury, PropertyDamage, and BlastTrauma

These questions provided a systematic method for structuring the instantiation of NYHKB and the identification of entities and relations. The resulting interpretation supports an explicit representation of domain entities, hazard concepts, causal relations, and consequences that may not be explicitly represented in the original hazard analysis documentation.

6.2. NYHKB Querying

Querying a knowledge base representing hazard analysis can serve different purposes. It can support development and maintenance activities through ad hoc retrieval of hazard-analysis information. For example, querying ignition-related hazardous events associated with a given physical location can support incident analysis, system development, and maintenance of that location. It may also support more structured assessment activities by retrieving information associated with normative requirements, such as those presented in Tables 1 and 2. As a representative example, the query in Listing 1 supports requirement 7.4.2.4 of IEC 61508-1 concerning event sequences leading to hazardous events.

Listing 1: SPARQL query supporting IEC 61508-1 requirement 7.4.2.4 by retrieving causal sequences linking hazardous events, hazardous situations, and triggered hazards.

```

PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX ho61508: <https://w3id.org/jochumsson/ho61508#>

SELECT ?priorEvent ?situation ?enablingEvent ?triggeredHazard
WHERE {
    ?priorEvent ho61508:resultsIn ?situation .
    ?situation ho61508:enables ?enablingEvent .
    ?enablingEvent ho61508:triggers ?triggeredHazard .

    ?priorEvent rdf:type/rdfs:subClassOf* ho61508:HazardousEvent .
    ?situation rdf:type/rdfs:subClassOf* ho61508:HazardousSituation .
    ?enablingEvent rdf:type/rdfs:subClassOf* ho61508:HazardousEvent .
    ?triggeredHazard rdf:type/rdfs:subClassOf* ho61508:Hazard .
}

```

The query further illustrates how abstract safety concepts can be used to retrieve detailed hazard-analysis knowledge. Although the query is formulated using the generic HO61508 concepts `HazardousEvent`, `HazardousSituation`, and `Hazard`, the returned results constitute application-specific concepts, examples of which are presented in Table 5. This demonstrates how the separation between conceptual, domain, and application ontologies supports the use of abstract safety concepts for categorisation and querying while still enabling retrieval of detailed application-level hazard-analysis knowledge.

Table 5

Representative event sequences returned by Listing 1, illustrating selected results supporting requirement 7.4.2.4.

Prior Event	Hazardous Situation	Enabling Event	Triggered Hazard
HighPressureRelease	HydrogenJet	StaticSparkIgnition	JetFire
_PipelineRoute	_PipelineRoute	_PipelineRoute	_PipelineRoute
LowPressureRelease	ExplosiveAtmosphere	HotSurfacelgnition	Deflagration
_TechnicalRoom	_TechnicalRoom	_TechnicalRoom	_TechnicalRoom
HighPressureRelease	FlammableCloud	EscalationIgnition	Fireball
_CompressorRoom	_CompressorRoom	_CompressorRoom	_CompressorRoom
ExternalFire	EquipmentDamage	Rupture	Pressure
_CompressorRoom	_CompressorRoom	_H2Cylinder	_H2Cylinder
Rupture	HydrogenJet	HighEnergyIgnition	Detonation
_H2Cylinder	_H2CylinderRoom	_H2CylinderRoom	_H2Cylinder

The query presented in this section serves as a representative example of how hazard-analysis knowledge can be retrieved from NYHKB. While only a single query is discussed in detail, additional queries covering the IEC61508 requirements considered in this work are available in the project repository⁶. Together, these queries show that information associated with the selected IEC61508 requirements is represented in NYHKB and can be accessed through querying.

7. Discussion and Conclusion

The paper outlines an ontological approach for structured hazard-analysis representation and demonstrates its applicability through a use case within the hydrogen domain. It describes the usage of the conceptual structures HO61508 and H2HO, the construction of the application ontology H2HOA, and the instantiation of the knowledge base NYHKB. The resulting ontological structures and the knowledge base NYHKB were evaluated through querying information associated with selected IEC61508 requirements relevant to hazard analysis.

This work indicates that HO61508 and H2HO can be applied as a foundation for application-level specialisation. In particular, the conceptual distinction provided by HO61508 between `Hazard`, concepts participating in causal sequences, and concepts representing harmful consequences is important for representing hazard analysis. This is reflected in requirements 7.2.2.3, 7.4.2.4, and 7.4.2.6 discussed in Section 5, which require these concepts to be identified and related. This conceptual representation, together with the queries presented in Section 6 that make use of these concepts to support the requirements, illustrates the practical applicability of using HO61508 and H2HO as a foundation for application-level specialisation.

Although the construction of the application ontology H2HOA is presented as three distinct activities in Section 5, their common goal is to increase the specificity of the ontology, supporting more detailed knowledge representation. The development of H2HOA further indicates that these activities should not be carried out independently, and that a common level of specificity must be maintained across all three dimensions.

This work is evaluated through instantiation, logical consistency checking, and SPARQL querying corresponding to competency questions formalised from a normative requirement in IEC61508. The

⁶<https://github.com/jochumsson/h2hoa/tree/main/queries>

usage of abstract safety concepts in the SPARQL queries indicates that application-level hazard knowledge can be accessed through the conceptual structures of HO61508 and suggests reuse of knowledge representation and competency questions across applications and domains. While these results suggest such reuse, the broader applicability of the ontological approach presented in this paper should be considered with respect to the scope of this research. The approach has only been evaluated within a single safety-critical domain, and its applicability to other safety domains remains unexplored. The evaluation was conducted using a single case study, the Nykvarn hazard analysis, representing a relatively small set of hazard scenarios. The knowledge base instantiation relied on interpretation of an existing hazard analysis expressed in natural language, and the applicability of the approach to other forms of hazard analysis artefacts has not yet been explored.

These limitations point to several directions for future work. These include investigating how the modelling trade-offs established for the conceptual ontology HO61508 [9] are reflected at the application level using additional domain knowledge sources for verification. Applying the approach across multiple safety domains and installations to assess its broader applicability. Investigating a formalised methodology for interpreting existing hazard analyses and guiding the structured instantiation of knowledge bases. Investigating ontology-driven hazard analysis where hazard analyses have not yet been conducted. Developing tool support for knowledge-base construction and maintenance. Finally, extending the ontological approach beyond hazard analysis toward risk analysis and a broader scope of IEC61508.

Acknowledgements

The authors acknowledge the support of H2solo and the Swedish Knowledge Foundation via the industrial doctoral school RELIANT, grant no. 20220130.

Declaration on Generative AI

All scientific contributions are the sole work and responsibility of the authors. Generative AI tools (OpenAI) were used for language refinement and structural feedback of the text of this manuscript.

References

- [1] IEC, Iec 61508:2010. functional safety of electrical, electronic and programmable electronic safety-related systems. parts 1–7, 2010.
- [2] IEC, Iec 61511:2025. functional safety. safety instrumented systems for the process industry sector, 2025.
- [3] ISO, Iso 26262:2018. road vehicles. functional safety, 2018.
- [4] CENELEC, En 50126:2017. railway applications. the specification and demonstration of reliability, availability, maintainability and safety (rams), 2017.
- [5] I. Hogganvik, K. Stølen, Risk analysis terminology for it-systems: Does it match intuition?, in: International Symposium on Empirical Software Engineering, 2005, pp. 246–255.
- [6] H. Kaindl, T. Rathfux, B. Hulin, R. Beckert, E. Arnautovic, R. Popp, A core ontology of safety risk concepts, in: Human-Centred Software Engineering and Human Error, Safety, and System Development, 2016, pp. 165–180.
- [7] L. Schnieder, E. Schnieder, T. Ständer, Railway safety and security: Two sides of the same coin?, in: International Railway Safety Conference, 2009.
- [8] J. Zhou, K. Hänninen, K. Lundqvist, L. Provenzano, An ontological interpretation of the hazard concept for safety-critical systems, in: European Safety and Reliability Conference (ESREL), 2017.
- [9] T. Jochumsson, K. Hänninen, M. Saadatmand, K. Lundqvist, A modular hazard ontology based on IEC61508, in: Proceedings of the European Safety and Reliability Conference (ESREL 2026), Research Publishing, 2026.

- [10] N. Guarino, Formal ontology in information systems, in: *Formal Ontology in Information Systems*, 1998, pp. 3–15.
- [11] G. Guizzardi, *Ontological Foundations for Structural Conceptual Models*, Ph.D. thesis, University of Twente, 2005.
- [12] G. Guizzardi, R. Falbo, R. S. S. Guizzardi, Grounding software domain ontologies in the unified foundational ontology (ufo): The case of the ode software process ontology, in: *International Database Engineering and Applications Symposium (IDEAS)*, 2008, pp. 127–140.
- [13] M. Uschold, M. Gruninger, *Ontologies: Principles, methods and applications*, *The Knowledge Engineering Review* 11 (1996) 93–136. doi:10.1017/S0269888900007797.
- [14] M. Poveda-Villalón, A. Fernández-Izquierdo, M. Fernández-López, R. García-Castro, Lot: An industrial oriented ontology engineering framework, *Engineering Applications of Artificial Intelligence* 111 (2022) 104755. doi:10.1016/j.engappai.2022.104755.