Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria

doi: 10.3850/ESREL2026061419_esrel26-p26241-cd

A Modular Hazard Ontology Based on IEC61508

Thorvaldur Jochumsson

Department of Computer Science & Engineering, Mälardalen University, Sweden.
E-mail: thorvaldur.jochumsson@mdu.se

Kaj Hänninen

Department of Computer Science & Engineering, Mälardalen University, Sweden.
E-mail: kaj.hanninen@mdu.se

Mehrdad Saadatmand

RISE Research Institutes of Sweden. E-mail: mehrdad.saadatmand@ri.se

Kristina Lundqvist

Department of Computer Science & Engineering, Mälardalen University, Sweden.
E-mail: kristina.lundqvist@mdu.se

This paper presents HO61508, a modular hazard ontology based on IEC61508. The ontology addresses ambiguities in safety terminology across domains in which IEC61508 is applied, providing a reusable foundation for domain-specific hazard ontologies. To demonstrate its adaptability, a hydrogen-specific ontological extension was developed, H2HO, which inherits the modular structure of HO61508 and is semantically aligned with ISO15916. Both ontologies were evaluated against quality criteria in terms of completeness, clarity, accuracy, and conciseness. The results indicate that the proposed modular approach enhances conceptual precision, supports interoperability across safety standards derived from IEC61508, and provides a formal basis for future standardization efforts in emerging domains.

Keywords: Safety, Functional Safety, Standardization, Ontology, IEC61508, Hydrogen, ISO15916

1. Introduction

As new industrial sectors emerge, standardization must often adapt to new challenges and industrial practices, for example the emerging hydrogen sector (ECH2A 2023). As part of this process, domain-specific functional safety standards are often required to align with a generic safety framework such as IEC61508 (IEC 2010), as has been done in the process industry (IEC 2025), the automotive sector (ISO 2018), and the railway domain (EN 2017), among others.

As the conceptual definitions provided in IEC61508 are contextually dependent, many derived domain-specific standards have developed alternative interpretations and extensions of IEC61508 terminology, as noted by Kaindl et al. (2016), which may result in inconsistencies, misalignments, and ambiguities during development and assessment. To avoid this recurring challenge, domain-specific standardization efforts could benefit from a clear and systematic alignment with the IEC61508 framework. This calls for increased formalization and modularization of IEC61508 concepts and terminology to address the ambiguities inherent in natural language and to facilitate clear and unambiguous communication within and across domain boundaries.

This article presents an ontological approach to address the need for formalization of IEC61508 terminology, providing an ontological module of the IEC61508 hazard concept, called HO61508.[a] The approach is modular, proposing loosely coupled ontological units with high conceptual cohesion. Beginning with the hazard module

[a] The HO61508 ontology is publicly available via `https://w3id.org/jochumsson/ho61508` and the source repository is available at `https://github.com/jochumsson/ho61508`.

HO61508, additional modules can be developed to systematically extend the ontological scope beyond the hazard analysis phase of IEC61508. In contrast to traditional monolithic designs, where an entire domain is represented within a single and tightly integrated ontology that is difficult to adapt or extend, this modular approach enables incremental development of flexible modules that can be independently reused and combined. By separating the domain into well-defined ontological units aligned with IEC61508, the approach provides an adaptable and reusable foundation for supporting domain-specific safety standardization.

This article further demonstrates, through a case study, how HO61508 can be applied to develop a hydrogen-specific hazard ontology, called H2HO.[b] H2HO formalizes key hydrogen safety hazards and related domain-specific terminology in strict alignment with IEC61508, grounded in basic safety considerations for hydrogen systems described in ISO15916 (ISO 2015). By explicitly aligning hydrogen-specific terminology with the underlying hazard concepts and semantics of IEC61508, H2HO has the potential to enhance precision in hydrogen hazard specifications. In this way, it demonstrates the practical utility of the modular approach introduced by HO61508 and provides a formal foundation for future hydrogen safety standardization efforts based on IEC61508.

2. Background

Kaindl et al. (2016) and Zhou et al. (2017) address the need for conceptual alignment of hazard concepts, but neither provides a modular ontology strictly based on IEC61508, nor do they explicitly aim to align new and existing standardization efforts with IEC61508. This leaves an important gap for emerging domains, such as the hydrogen sector, where IEC61508 is expected to serve as the foundation for new safety standards.

Kaindl et al. propose a core ontology of safety risk concepts based on definitions from the automotive and railway sectors, considering the safety standards IEC61508, ISO26262, and EN50126. The ontology unifies knowledge from these standards and provides clarity regarding their conceptual differences. However, it is not a strict formalization of IEC61508 and is therefore not primarily intended to support activities specified therein, such as IEC61508 hazard analysis, but rather to address such activities in the context of ISO26262 and EN50126.

A more abstract and generic approach was taken by Zhou et al., who propose a core hazard ontology for safety-critical systems. Their ontology is based on Zhou et al.'s general understanding of the safety-critical domain, with novel conceptual definitions and a formalization of the hazard concept. However, since Zhou et al.'s work is not based on IEC61508, it lacks the normative traceability required for engineering practices adopting the IEC61508 safety lifecycle. While this limitation could be addressed through terminological and conceptual mapping, it would come at the cost of simplicity, clarity, and precision of the ontological approach. This makes Zhou et al.'s work challenging to apply to activities directly linked to the safety lifecycle and assessment of IEC61508.

Together, these previous works demonstrate the value of ontological approaches for clarifying hazard and safety concepts, but they also highlight a gap that remains, namely a modular ontology aligned with IEC61508 that can serve as a foundation for new domain-specific standards. To close this gap, we use a foundational ontology and a modeling language for conceptual and representational precision.

The Unified Foundational Ontology (UFO) proposed by Guizzardi (2005) was adopted as a top-level ontology, since it provides the conceptual support required for modeling abstract safety concepts with the necessary precision. Without such high-level conceptual grounding, the development of HO61508 would likely suffer from increased complexity and reduced ontological clarity from a standardization perspective.

For the ontological representation in this work, we employ the conceptual modeling language OntoUML Guizzardi et al. (2018), which is tailored

[b]The H2HO ontology is publicly available via `https://w3id.org/jochumsson/h2ho`.

for representing UFO-based ontologies. Throughout the remainder of this article, we refer to UFO entities using the namespace `ufo:`, to clearly distinguish them from ontological entities introduced in this work.

3. Method

This study follows an iterative development approach grounded in the Design Science Research (DSR) framework as described by Hevner et al. (2004), producing HO61508 as the main artifact and H2HO as the outcome of the validation case study. The overall method, illustrated in Figure 1, alternates between (1) design, (2) verification, and (3) validation. The design phase applies the *Skeletal* development method by Uschold and Gruninger (1996); the verification phase adopts Vrandečić's (2009) *Context* evaluation aspect using IEC61508 as formalized context; and the validation phase is carried out through a hydrogen-domain case study, in which H2HO is designed (3.1) and verified (3.2).

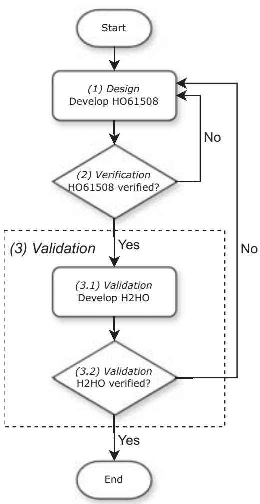

Fig. 1. Overview of the development approach for HO61508 and H2HO.

The design phase (1) ensures that foundational definitions and key concepts from relevant standards are captured. Terms and definitions are collected from the standards to establish conceptual completeness and terminological clarity. Each term's intended meaning is formalized, and relationships among concepts are encoded according to their contextual use. Redundant axioms are removed and necessary ones added to achieve ontological clarity and conciseness.

The verification phases (2) and (3.2) are grounded in the *Context* evaluation approach using IEC61508 as the formalized context against which the following criteria are verified:

- **Completeness**: Are all relevant concepts from the standard represented in the ontology?
- **Conciseness**: Is the ontology free from terminology from the standard that results in irrelevant or redundant axioms?
- **Clarity**: Does the ontology communicate effectively the intended meaning of the standard's terminology?
- **Accuracy**: Do the axioms comply with relevant aspects of the standard?

Although these quality criteria are presented as distinct properties, they have inherent dependencies and may even conflict with one another, as noted by Vrandečić. For example, striving for completeness with respect to the standard can negatively affect ontological conciseness. The iterative design and evaluation must consider these dependencies as compromises and tradeoffs, and the resulting ontology should be presented as a balanced design, explicitly stating the compromises involved.

The validation phase (3) concerns the adaptability of HO61508. Unlike the verification criteria, assessing adaptability requires application context. Therefore, a case study was conducted in which HO61508 was applied to the hydrogen domain, yielding the hydrogen-specific hazard ontology H2HO. Using domain input from ISO15916, H2HO development (3.1) and evaluation (3.2) followed the same principles as phases (1) and (2), illustrating how domain-specific knowledge can be systematically situated within the ontological framework of HO61508 by mapping hydrogen terminology to abstract hazard concepts.

Beyond the resulting ontologies, the development approach constitutes a secondary artifact that supports systematic integration of domain-specific knowledge within a generic safety framework and is potentially applicable in broader contexts than IEC61508.

4. Hazard Ontology 61508 (HO61508)

The scope of HO61508 aligns with the hazard analysis phase of the IEC61508 safety lifecycle and aims to formalize the conceptual knowledge described therein. Central to this phase is the concept of hazard, for which the standard provides the following core definitions:

Def. **Harm**: Physical injury or damage to the health of people or damage to property or the environment.

Def. **Hazard**: Potential source of harm.

Def. **HazardousSituation**: Circumstance in which people, property or the environment are exposed to one or more hazards.

Def. **HazardousEvent**: Event that may result in harm.

Def. **HarmfulEvent**: Occurrence in which a hazardous situation or hazardous event results in harm.

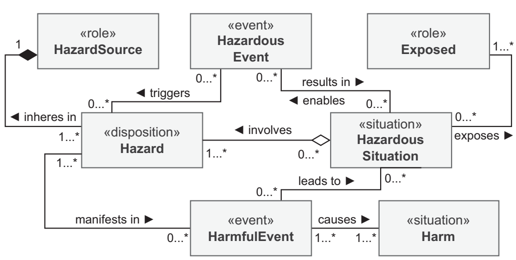

Fig. 2. OntoUML representation of the IEC61508 core hazard concepts.

Figure 2 represents the final iteration of HO61508, where the hazard concept is central to the ontology. Despite the simplicity of the IEC61508 definition of hazard, it poses an interesting ontological challenge. The notion of "potentiality" expressed in the definition implies that a hazard need not be manifested at all times, whereas being a "source" requires an enduring entity. The most fitting ontological design is therefore to separate the notion into a ufo:Disposition and its bearer. In other words, Hazard in Figure 2 is a ufo:Disposition, an intrinsic moment that inheres in and is existentially dependent on its bearer, HazardSource, a ufo:Role that is carried by a ufo:Endurant. In this way, the hazard's potentiality is modeled as an intrinsic moment, while the source aspect is modeled as a role that an enduring real-world entity carries. For example, a gaseous hydrogen cylinder carries a HazardSource role that bears a potential high-pressure Hazard that inheres in it.

The ontological representation of hazard as a ufo:Disposition implies that a hazard is constituted by a property of an enduring entity, either as the presence or the absence of that property. As such, the focus lies on representing hazard potentiality explicitly, as an existential and enduring attribute of its bearer, without addressing the probability or uncertainty associated with its manifestation. Although uncertainty regarding whether a hazard will manifest constitutes an essential aspect of safety and risk management, HO61508 remains within its intended scope of the hazard analysis phase of IEC61508 to explicitly represent hazards and the causal structure through which they may be triggered and manifested.

The notions of HazardousSituation and HazardousEvent were modeled more directly without requiring additional ontological interpretation. HazardousSituation is a ufo:Situation that exposes one or more ufo:Endurant playing the role Exposed to one or more Hazards. HazardousEvent was modeled as a ufo:Event that may trigger one or more Hazards.

In order to support the full objectives of IEC61508 hazard analysis, the entire causal event sequence leading to a hazard needs to be represented. This was done by modeling that HazardousEvent may result in HazardousSituation and HazardousSituation may enable HazardousEvent. For instance, a hydrogen attack HazardousEvent may result in a damaged containment HazardousSituation, which in its turn enables a rupture HazardousEvent.

The HarmfulEvent concept is represented

as `ufo:Event` in which `Hazard` is manifested, and `Harm` is modeled as a `ufo:Situation` that is caused by `HarmfulEvent`. Notably, the IEC61508 definition of `HarmfulEvent` presents an ontological challenge, as it states that `HarmfulEvent` is brought about by either `HazardousSituation` or `HazardousEvent`. According to UFO, only events and not situations bring about changes. Therefore, this definition cannot be directly modeled without interpretation and ontological reasoning. The ontological solution, represented in Figure 2, defines `HarmfulEvent` as the manifestation of `Hazard`, which in turn is triggered by `HazardousEvent` and may involve `HazardousSituation`. This formulation indirectly captures the idea that `HazardousEvent` brings about `HarmfulEvent`, and that `HarmfulEvent` may have a causal relation with `HazardousSituation`.

Further, the causal sequence pattern between `HazardousEvent` and `HazardousSituation` is extended with the notion that a `HarmfulEvent` may lead to additional `HazardousSituation`, capturing hazard propagation, for example a hydrogen jet fire causing a tank rupture.

In the design of HO61508 we incorporated tradeoffs made with respect to the different evaluation criteria proposed by Vrandečić. These tradeoffs are discussed in detail below.

Completeness vs. Conciseness: Not all terminology in the standard that can be associated with the hazard concept is represented in HO61508 in order to maintain conciseness and to avoid introducing overlapping ontological entities. For example, the notions of "initiating event" and "failure" overlap with `HazardousEvent`, and representing all three in the ontology would create conceptual overlap at the cost of conciseness.

Conciseness vs. Clarity: Introducing only the essential axioms grounded in the standard for conciseness can come at the cost of clarity when additional entities are required for a correct ontological representation. For example, the notion of `HazardSource` is not defined in IEC61508 but is introduced in the ontology as an ontological interpretation of the IEC61508 definition of hazard.

Clarity vs. Accuracy: Direct alignment with the standard for clarity may come at the cost of ontological accuracy when the standard is semantically ambiguous or inconsistent. In such cases, an ontological representation requires interpretation to maintain accuracy, possibly affecting clarity. For example, the manifestation of `HarmfulEvent`, as defined by the standard, requires ontological interpretation to maintain accuracy.

Accuracy vs. Completeness: Ontological accuracy can be a limiting factor for completeness toward the standard. For example, IEC61508 refers to "failure causing a hazardous situation" and "failure creating a hazard", where only the first can be represented accurately, since `Hazard`, as a `ufo:Disposition`, is an enduring property and therefore not "created".

5. Hydrogen Hazard Ontology (H2HO)

The H2HO ontology builds on hydrogen hazard knowledge from ISO15916, which describes basic safety considerations for hydrogen systems, and situates these concepts within the ontological framework of HO61508. Consequently, H2HO provides conceptual alignment between IEC61508 and abstract hazard concepts grounded in ISO15916.

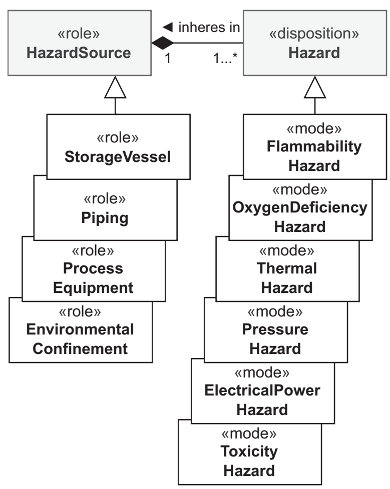

Fig. 3. Ontological representation of hydrogen related `Hazard` and `HazardSource`.

Figure 3 presents the identified subtypes of

Hazard and HazardSource, providing a high level ontological representation of hazard concepts within hydrogen systems. In this context, the terminology used in ISO15916 is inconsistent, applying terms interchangeably to denote the consequences of a hazard, the hazardous situation, the harmful event, or the source itself, for example fire, explosion, and asphyxiation hazards. Although such terms are accepted within the hydrogen domain, they are not aligned with the IEC61508 definition of hazard and are therefore avoided in H2HO to maintain conceptual clarity with respect to HO61508. Accordingly, the hazard concepts represented in H2HO consistently refer to the property that constitutes the potential harm, or the lack of that property, which affects completeness with respect to ISO15916.

Central to hydrogen systems is FlammabilityHazard, an abstract ontological entity representing hazards related to combustion potential from hydrogen's flammability property. Other key hazard types include OxygenDeficiencyHazard representing hazards related to lack of oxygen, ThermalHazard capturing hazards associated with extreme temperatures both cryogenic and high-temperature, PressureHazard representing hazards from high-pressure storage or transfer conditions, and ToxicityHazard representing hazards related to potential harmful properties of substances or by-products involved in hydrogen processes.

The ontological interpretation of HazardSource, presented in Figure 3, defines an abstract role categorisation of hazard bearers. StorageVessel refers to any type of hydrogen storage system, Piping to hydrogen distribution structures, ProcessEquipment to devices involved in hydrogen processing or transformation, and EnvironmentalConfinement to spaces where flammable hydrogen-air mixtures may accumulate. In this context, the ontological interpretation considers the hazard bearer to be an abstract system composite rather than the hydrogen substance itself, thereby providing a foundation for further subtype specification and more meaningful hazard analysis.

Figure 4 presents a high-level categorisation

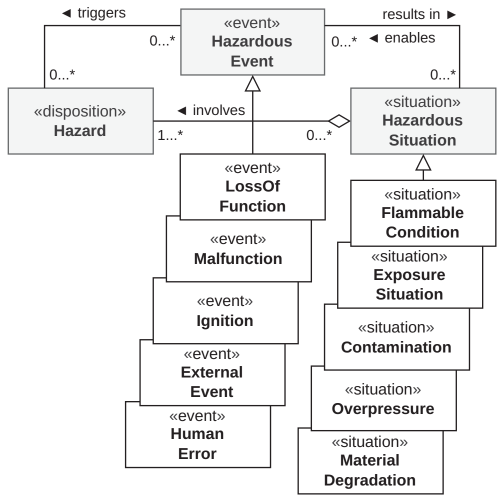

Fig. 4. Ontological representation of HazardousEvent and HazardousSituation concepts in hydrogen systems, shown in the context of HO61508.

of generic HazardousEvent and HazardousSituation concepts in hydrogen systems. Together these entities provide the means to capture causal sequences leading to hydrogen-related Hazard and ultimately to Harm.

The class HazardousEvent is divided into the subtypes LossOfFunction representing events where functional integrity is compromised, Malfunction representing events where functionality deviates from its specification, Ignition representing ignition occurrences, ExternalEvent representing external events compromising system integrity, and HumanError representing events caused by human errors during system lifecycle activities.

The class HazardousSituation is divided into the subtypes FlammableCondition representing a flammable mixture of hydrogen and air, ExposureSituation representing exposure of potentially harmful elements, Contamination representing the presence of foreign or reactive substances, Overpressure representing confined or transient pressure rise, and MaterialDegradation representing a state of reduced structural integrity.

Together, HazardousEvent and Hazardo

usSituation constitute an abstract modelling pattern that captures the chain of events and situations leading to the triggering of a hazard. For example, a LossOfFunction may result in a FlammableCondition, which enables Ignition, triggering a FlammabilityHazard. The high abstraction level of the pattern provides a generic framework suitable for further specialization when moving toward a specific application and context. For example, different human errors can be represented as subtypes of HumanError, providing an abstraction for a wide range of events that tend to be highly application- and context-specific.

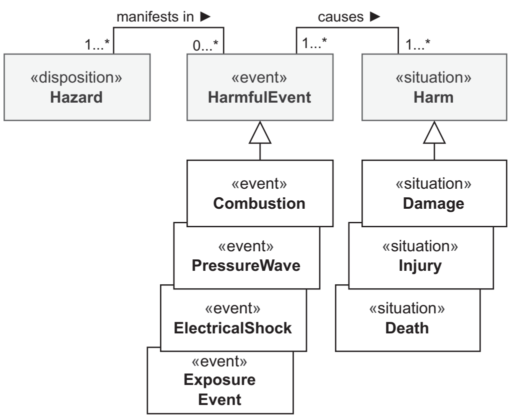

Fig. 5. Ontological representation of hydrogen related HarmfulEvent and Harm in context of HO61508.

Figure 5 presents the hydrogen-related HarmfulEvent and Harm concepts at a high abstraction level. HarmfulEvent includes Combustion, PressureWave, ElectricalShock, and ExposureEvent, representing manifestations of the hydrogen Hazard classes presented earlier in this chapter. The class Harm is specified into Death, Injury, and Damage, providing a general categorisation of harmful outcomes, with further specification considered beyond the scope of this work.

The representation of H2HO in this section has focused on situating concepts and terminology from ISO15916 within the ontological structure provided by HO61508. This alignment exposed several points of tension between the evaluation criteria, requiring careful design choices, as discussed below.

Completeness vs. Conciseness: H2HO has intentionally been kept at a high level of abstraction to limit the scope of this paper. Consequently, many concepts described in ISO15916 are not explicitly represented but can be mapped to higher-level abstractions within H2HO, such as Explosion to Combustion.

Conciseness vs. Clarity: Additional concepts have been introduced, such as the HarmfulEvent ExposureEvent. The concept of exposure as a harmful event is not explicitly mentioned in ISO15916 but is implicitly expected as part of the causal event chain. Although this may come at the expense of strict conciseness, its explicit inclusion in H2HO improves clarity.

Clarity vs. Accuracy: Maintaining conceptual clarity towards ISO15916 and ontological accuracy at the same time has proven challenging. This is mainly because ISO15916 is not grounded in IEC61508, resulting in a conceptual mismatch between the two. For example, the notion of a "fire hazard" in ISO15916 has been deliberately avoided in H2HO, since fire is considered a HarmfulEvent, a subtype of Combustion, rather than a Hazard. Furthermore, HO61508 is a generic ontology that supports varying abstraction levels adopted by derived ontologies. For example, a FlammabilityHazard may inhere in an individual physical object, such as a storage vessel, or in a higher-level construction, such as a hydrogen storage facility. The appropriate abstraction level should be chosen in accordance with the purpose and stage of the hazard analysis and is not specifically guided by ISO15916.

Accuracy vs. Completeness: H2HO's terminological accuracy is affected by the inconsistencies in ISO15916. However, emphasis was placed on maintaining conceptual accuracy rather than terminological completeness, ensuring that the representation of core hazards and their causal relations remains consistent with the intended meaning of IEC61508.

6. Conclusion

This paper demonstrates how a modular ontology can be developed to represent the hazard concepts of IEC61508, resulting in HO61508. It further illustrates the generic applicability of HO61508 through the construction of the domain-specific hazard ontology H2HO, grounded in knowledge from the hydrogen sector and ISO15916.

The development and evaluation of HO61508 demonstrated that ontological interpretation and a balanced design approach are required to satisfy conflicting evaluation criteria. The resulting design shows that such balance is achievable, though not without design compromise.

The construction of H2HO revealed considerable terminological and conceptual differences between IEC61508 and ISO15916, where the main ontological challenge lay in achieving clear alignment without diverging from core domain terminology. The evaluation further showed that the abstraction level chosen for a domain ontology requires careful attention in order to achieve the intended outcomes.

Overall, the results indicate that HO61508 and the ontological approach presented in this paper increase conceptual clarity in both generic and domain-specific safety standardization. Such improved precision and alignment support reusability, tooling integration, and a semantic structure for automated reasoning. Although H2HO is represented at a high level of abstraction, it demonstrates how HO61508 and the proposed ontological method can serve as a foundation for systematic domain alignment toward IEC61508, supporting further specialization and domain-specific knowledge bases. In addition, the modularity of the approach supports extending the ontology beyond hazard analysis, initially toward risk and probabilistic analysis, which may yield benefits across the entire safety lifecycle.

Acknowledgement

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

References

CENELEC (2017). EN 50126:2017. Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS).

European Clean Hydrogen Alliance (2023). Roadmap on hydrogen standardisation. Technical report, European Commission.

Guizzardi, G. (2005). *Ontological Foundations for Structural Conceptual Models*. Ph. D. thesis, University of Twente, The Netherlands.

Guizzardi, G., C. M. Fonseca, A. B. Benevides, J. P. A. Almeida, D. Porello, and T. P. Sales (2018). Endurant types in ontology-driven conceptual modeling: Towards OntoUML 2.0. In J. C. Trujillo, K. C. Davis, X. Du, Z. Li, T. W. Ling, G. Li, and M. L. Lee (Eds.), *Conceptual Modeling*, Cham, pp. 136–150. Springer International Publishing.

Hevner, A. R., S. T. March, J. Park, and S. Ram (2004). Design Science in Information Systems Research. *MIS Quarterly 28*(1), 75–105.

IEC (2010). IEC 61508:2010. Functional safety of electrical, electronic and programmable electronic safety-related systems. Parts 1–7.

IEC (2025). IEC 61511:2025. Functional safety. Safety instrumented systems for the process industry sector.

ISO (2015). ISO/TR 15916:2015 basic considerations for the safety of hydrogen systems.

ISO (2018). ISO 26262:2018. Road vehicles. Functional safety.

Kaindl, H., T. Rathfux, B. Hulin, R. Beckert, E. Arnautovic, et al. (2016, August). A core ontology of safety risk concepts. In *6th International Conference on Human-Centred Software Engineering (HCSE) / 8th International Conference on Human Error, Safety, and System Development (HESSD)*, pp. 165–180. Springer.

Uschold, M. and M. Gruninger (1996). Ontologies: Principles, methods and applications. *The Knowledge Engineering Review 11*(2), 93–136.

Vrandečić, D. (2009). Ontology evaluation. In S. Staab and R. Studer (Eds.), *Handbook on Ontologies*, pp. 293–313. Berlin, Heidelberg: Springer Berlin Heidelberg.

Zhou, J., K. Hänninen, K. Lundqvist, and L. Provenzano (2017, June). An ontological interpretation of the hazard concept for safety-critical systems. In *27th European Safety and Reliability Conference*.