Chapter 6

Paper A: An Ontological Interpretation of the Hazard Concept for Safety-Critical Systems

Jiale Zhou, Kaj Hänninen, Kristina Lundqvist, and Luciana Provenzano.
Proceedings of the 27th European Safety and Reliability Conference
(ESREL'17), Portoroz, Slovenia, June 2017.

Abstract

The hazard concept has been extensively used in the literature and defined in an informal way, which serves as a guidance on identifying the potential hazards during the development of safety-critical systems. Intuitively, the definitions seem to be consistent and easy to understand. However, when we take a closer look at these definitions, ambiguities may arise, and real-world semantics need to be defined. In this work, we propose a hazard domain ontology, i.e., the Hazard Ontology (HO), to provide an ontological interpretation of hazard. To tackle the aforementioned issues, the HO is grounded in the Unified Foundational Ontology (UFO) to utilize the benefits provided by taking foundational concepts into account. Finally, we show some useful findings when we use the proposed ontology to analyze the hazard descriptions from an industrial passenger train project.

6.1 Introduction

The concept of hazard has been extensively used in the literature and defined in an informal way, which serves as a guidance on identifying potential hazards during the development of safety-critical systems. For instance, Leveson [1] defines a hazard as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)". In the standard MIL-STD-882 [2] and EN-50129 [3], similar definitions are put forward as "hazard is any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment, or property; or damage to the environment" and "hazard is a condition that could lead to an accident", respectively.

Intuitively, these definitions seem to be consistent and easy to understand. However, when we take a closer look at them, ambiguities may arise, e.g., whether a hazard is a particular system state, or is a combination of the system and environment states. Furthermore, these definitions suffer from a lack of the precise definition of the term "condition" from the perspective of real-world semantics, i.e., the correspondence between the term "condition" and entities (e.g., object, relation, property, event, etc.) in the real world. Therefore, in practice, the identified hazards are usually formulated in an arbitrary way, in the sense of what are presented and how they are presented. Last but not least, many terms are used to represent the causal relation between "condition" and "accident", such as "contribute to", "cause", and "lead to". Although these terms are in line with people's intuitive idea, there is still a need to add constraints to these relations from the perspective of real-world semantics, i.e., to define what real-world entities can be connected when a causal relation is referred to, and to explain how the real-world entities together make the causal relation true. These considerations motivate us to formulate the following research questions: Can we provide an interpretation of hazard from the real-world semantics perspective, to cope with these issues?

An ontology is a reference model about a certain subject or domain that consists of a set of subject-/domain-specific concepts, relations, and axioms. It aims to achieve a better understanding of the subject or domain from modelers and model users point of view. Several ontologies, which are related with hazard, have been proposed in the literature, e.g., [4], [5] [6] [7]. Nevertheless, either they leave the real-world semantics out of consideration, or the real-world semantics is provided in an informal way. In order to interpret hazard in the real-world semantics, foundational concepts (e.g., object, event, relator, universal, etc.) should be explicitly taken into account. A foundational ontology is a

theoretically well-founded subject-/domain-independent ontology, which consists of a set of foundational concepts and relations. It can be grounded in to provide a sound real-world semantics for a subject-/domain-specific ontology.

In this paper, we devote our efforts into constructing a hazard ontology and grounding the hazard ontology in a foundational ontology. The hazard ontology serves as an ontological interpretation of hazard, together with real-world semantics. We employ Unified Foundational Ontology (UFO) as the foundational ontology, for two reasons: 1) it has been successfully applied in multiple research areas, and 2) comparing other existing foundational ontologies, UFO provides a more complete set of foundational concepts and relations to cover important aspects of hazard. The contributions of this work can be summed up as follows:

- We propose a hazard ontology, consisting of a set of concepts, relations, and axioms, and
- We take a foundational ontology into account, i.e., the Unified Foundational Ontology (UFO), to provide the real-world semantics on the concepts and relations that pertain to the hazard ontology, and
- We show the usefulness of our work by using the proposed ontology to evaluate the hazard identification results from an industrial passenger train project.

The remainder of this paper is organized as follows: Section 6.2 briefly elaborates the background. Section 6.3 presents the hazard ontology in detail. Section 6.4 describes some practical implications of our work. Section 6.5 introduces state-of-the-art, and finally concluding remarks and future work are outlined in Section 6.6.

6.2 Background

In this section, we introduce the foundational ontology, i.e., UFO and a traditional informal interpretation of hazard underpinning the hazard analysis.

6.2.1 The Unified Foundational Ontology - UFO

In this work, we employ the Unified Foundational Ontology (UFO) [8] as the foundational ontology. Comparing other existing foundational ontologies, such as GFO [9], BFO [10], DOCLE [11], etc., we notice that UFO provides a more

complete set of concepts to cover important aspects of hazards, such as **Situation**, **Disposition**, and **Kind/Role**. A complete description of UFO falls outside the scope of this paper. In the following, we present a fragment of the UFO containing the concepts that are germane for the purposes of this paper. We then illustrate these concepts and some contextually relevant relations using UML (Unified Modeling Language) diagrams, as shown in Figure 6.1. These diagrams express typed relations (represented by lines with a reading

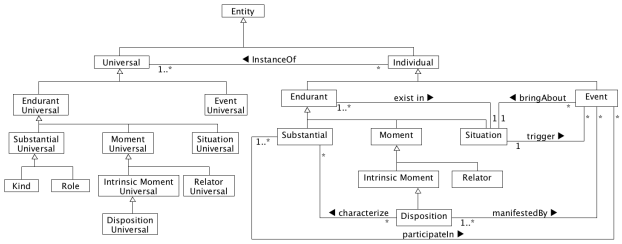

Figure 6.1: A fragment of the UML diagrams of UFO. Concepts are represented as rectangles. Typed relations are represented by lines with a reading direction pointed by "►", from open end to aggregated end. Cardinality constraints are labeled on each end of typed relations. Subsumption constraints are represented by lines with an open-ended arrow "△" connecting a sub-concept to its subsuming super-concept.

direction pointed by "►", from open end to aggregated end) connecting categories (represented as rectangles), cardinality constraints for these relations, as well as subsumption constraints (represented by lines with an open-ended arrow "△" connecting a sub-concept to its subsuming super-concept).

We begin by distinguishing between **Individual** and **Universal**. An individual, i.e., an instance of **Individual**, is an entity that exists in reality possessing a unique identity (e.g., *a person*, *a passenger train*, *a track*, *the kinetic energy of a train*, or *a collision*), while an universal, i.e., an instance of **Universal**, represents a pattern of features that are repeatable in a number of different individuals (e.g., *Person*, *Train*, *Track*, *Kinetic Energy* or *Collision*). For example, *a person* and *a passenger train* are individuals that instantiate the universals *Person* and *Train* respectively.

UFO includes a taxonomy of individuals (as shown in the right part of Figure 6.1). The topmost distinction in the taxonomy of individuals is that between **Endurant** and **Event** (also referred to as **Perdurant**). An endurant,

i.e., an instance of **Endurant**, is an entity that exists in time while keeping its identity (e.g., *a person*). An event, conversely, extends in time accumulating temporal parts. Especially, whenever an event is present, it is not the case that all its constituent parts are present.(e.g., *a collision*).

Endurant is further classified into **Substantial** (also referred as **Object**), **Moment** and **Situation**. A substantial or an object is an endurant whose existence in time does not depend on other endurants, i.e., existentially-independent of other endurants (e.g., *a person* and *a passenger train*). A moment, in contrast, is an endurant that inheres in another endurant(s) (e.g., *the kinetic energy of a train* is existentially-dependent of *a train*). Moments that are existentially-dependent of one single endurant are instances of **Intrinsic Moment** (e.g., *the kinetic energy of a train*), whereas moments that depend on a plurality of individuals are instances of **Relator** (e.g., *a being-crossing relator between a person and a track*). A relation of **mediation** is defined between a relator and all the individuals it depends on.

A disposition, i.e., an instance of **Disposition**, is an intrinsic moment that can only **be manifested** by the occurrence of event(s) (e.g., *the kinetic energy of a train* can only be manifested by the occurrence of the moving of the train). The *inhere in* relation between a disposition and a substantial is referred as **characterize**.

A situation, i.e., an instance of **Situation**, is constituted by possibly many endurants. A situation is considered here to be synonymous to what is named state of affairs, i.e., a portion of reality that can be comprehended as a whole. An **exist in** relation (also referred to as *being present at*) is defined between a situation and its constituent endurants. For example, In the situation "a passenger train is approaching a person who is crossing the track", there exist three substantials (i.e., *a passenger train*, *a person*, *a track*) and two relators (i.e., *being-approaching* and *being-crossing*). Moreover, two foundational relations are defined between events and situations in the UFO, i.e., a situation can **trigger** events and then an event will **bring about** another situation. The motivation behind these relations is two-fold: 1) the occurrence of an event is the manifestation of a collection of dispositions existing in a situation, and 2) an event may change reality by changing the state of affairs from one situation to another situation. Moreover, events are ontologically dependent entities in the sense that they existentially depend on their participants in order to exist.

These taxonomy of individuals are reflected in the taxonomy of universals, as shown in the left part of Figure 6.1. Here, we solely introduce **Kind** and **Role** which are most related with our work. The ontological concept of **Substantial Universal** (also referred as **Object Universal**) is further specialized

into **Kind** and **Role**, according to the ontological notions of identity and rigidity [8]. **Kind** denotes a substantial universal with rigidity, i.e., every individual instantiating a kind universal is necessarily an instance of the kind universal in every possible situation. For instance, a person is necessarily an instance of *Person* during his/her existence, that is, *Person* is a kind universal and *a person* is a kind object. On the contrary, there are non-rigid universals, named **Role**, such as *Driver*. The individuals of a kind universal can instantiate a role universal in some circumstances but not in others (e.g., after driving, a person will no longer be an instance of the role universal *Driver* until next time). A relation of "play" is defined between kind individuals and the role individuals they instantiate.

6.2.2 An informal interpretation of hazard

The Hazard Triangle Model (HTM) [12] provides an informal yet typical interpretation of hazard, as shown in Figure 6.2. It illustrates that a hazard is

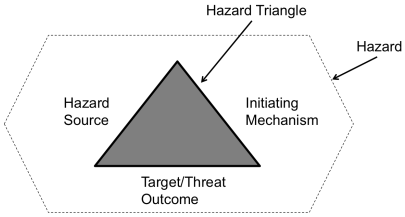

Figure 6.2: The Hazard Triangle Model.

an entity that is composed of three necessary and coupled components: hazard source, initiating mechanism (causes), and target/threat outcome (consequences), each of which forms the side of a triangle. **Hazard Source** is the rudimentary component of a hazard. It creates the potential hazardous impetus for the hazard to exist, which are generally energy sources or safety critical functions, for instance, electricity, fuel, gas, aircraft velocity, etc. **Initiating Mechanism** represents the initiator events that cause transformation of the hazard from a dormant state to an active mishap state, e.g., hardware failure, human errors, etc. **Hazard Target/Threat Outcome** is the resulting severity outcome after the hazard is transformed to an active mishap state, such as injury of people, loss of the system, and damage to the environment. As claimed in [12], all three sides of the hazard triangle are essential and required in order

for a hazard to exist. By removing any one of the triangle sides, the hazard will be eliminated because it is no longer able to trigger an accident. Also, by reducing the possibility of any of the components of the triangle the mishap possibility is reduced. When all the components comprising a hazard are in alignment, the hazard are highly probable to transition from a dormant state to an active mishap state. Since its proposal, the HTM has received considerable attention, and served as guidance on the identification of potential hazards. However, in our experience, this informal interpretation of hazards has several deficiencies:

- ***Deficiency 1:*** It lacks a real-world semantics for the concepts within the HTM, i.e., what are the foundational categories that HTM concepts can be categorized into? Take the hazard source as an illustration. A hazard source can be e.g., electricity, fuel, gas, or aircraft velocity, etc. The first three sources refer to an amount of matter, respectively, whereas the last one refers to a quality. Apparently, this superfluous inconsistency could cause confusions for stakeholders when either performing the hazard analysis or examining the hazard analysis results throughout the development process.
- ***Deficiency 2:*** There are no clear definitions on the relations among these concepts, without which the interpretation would sacrifice its preciseness and cause ambiguities. For instance, it is not clear whether the hazard source and threat outcome will participate in the initiating mechanism event or not.
- ***Deficiency 3:*** The HTM is oversimplified to capture various factors that lead to an accident. For example, "Insufficient fire fighting capability" is a typical hazard description. Taking a closer look at this hazard, it will be noticed that it can hardly be categorized into 1) initiating mechanism, since it is describing a static situation rather than an event and, 2) hazard source, since it will do no harm by itself and, 3) threat outcome, since it is not necessarily caused by an accident. However, this description is typically regarded as a potential hazard, in that, it is likely to play a significant role in leading to serious fire accidents.

6.3 The Hazard Ontology

In this section, we propose an ontological interpretation of hazard, i.e., the Hazard Ontology (HO). It stores three kinds of facts about hazards, in the sense

of 1) Concepts that represent entities of importance to interpret the concept of hazard and, 2) Relations that are labeled and directed connections between concepts and, 3) Axioms that are used to model knowledge that are always true, e.g., **subsumption** axiom (which specifies that the instances of one concept are a subset of the instances of the super concept) and **instanceOf** axiom, labeled as *insOf*, (which specifies that one concept is an instance of the other concept). Section 6.3.1 elaborates on a brief overview of the methodology to engineering the Hazard Ontology, and Section 6.3.2 introduces the concepts in detail.

6.3.1 The Methodology to Engineering the HO

In general, the methodology, which we adopted to build the HO, consists of two main steps: 1) by reviewing the existing literature, we ground the core HO concepts (i.e., **Hazard** and **Mishap**) in the UFO concepts (i.e., these two concepts are interpreted in the light of UFO concepts) and, 2) by following the ontological pattern defined in the UFO, other HO concepts are further proposed and grounded in the UFO. In this way, the HO will be able to utilize the benefits provided by the foundational ontology as follows:

- ***Benefit 1:*** the proposed concepts will inherently possess the real-world semantics to facilitate their definitions, which helps to address the ***Deficiency 1***.
- ***Benefit 2:*** the HO can directly use the relations (such as "bring about", "trigger", "exist in", and "play") that are well-founded in the UFO, which helps to address the ***Deficiency 2***.
- ***Benefit 3:*** the HO will be able to capture various factors that contribute to accidents, which helps to address the ***Deficiency 3***.

Figure 6.3 depicts the proposed Hazard Ontology (HO) using UML diagrams which have been explained in Section 6.2.1. We propose 11 main concepts (colored in gray), and ground them in 5 foundational concepts in the UFO (colored in white).

To be specific, we examine some widely accepted definitions of hazards in the context of SCSs, as mentioned in Section 6.1, which can serve as a starting point to interpret the concept of hazard. Basically, the main idea behind our ontology is in line with these definitions, that is, the **Hazard** in the HO is supposed to be characterized by two essential features. Particularly, on one hand, the nature of a hazard is a set of states, which motivates the interpretation that **Hazard** is a sub-concept of **Situation**. On the other hand, the states are

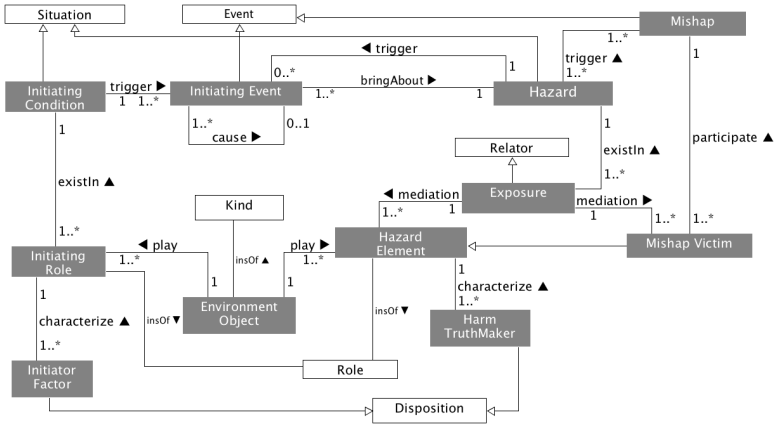

Figure 6.3: The UML diagrams of the Hazard Ontology. Concepts are represented as rectangles. Proposed concepts are colored in gray, and UFO concepts are colored in white. Typed relations are represented by lines with a reading direction pointed by "▶", from open end to aggregated end. Cardinality constraints are labeled on each end of typed relations. Subsumption constraints are represented by lines with an open-ended arrow "△" connecting a sub-concept to its subsuming super-concept. InstanceOf axiom, labeled as **insOf**, specifies that one concept is an instance of the other concept.

likely to lead to severe consequences, which is interpreted into the modeling decision that **Hazard** can trigger **Mishap** which is a sub-concept of **Event**. An insight that comes out of these interpretations is that, as a situation, there exist many endurants (kind objects, role objects, relators, etc.) in a hazard situation, which can help to capture the hazardous factors. Although there may exist various endurants in a hazard situation according to UFO, we argue that there must exist four types of endurants in a hazard situation, in terms of the **Mishap Victim** role objects, the **Harm TruthMaker** dispositions, the **Hazard Element** role objects, and the **Exposure** relators, to be introduced in detail later.

Furthermore, the causal factors that activate a dormant hazard is of importance in the understanding of a hazard. Inspired by the foundational relation "bring about" between **Event** and **Situation**, we define that a **Hazard** situation can be brought about by at least one **Initiating Event** event. Additionally, 3

concepts are defined to capture the knowledge that play a significant role in triggering the initiating events. These are the **Initiating Condition** situation, the **Initiating Role** role objects, and the **Initiator Factor** dispositions.

Essentially, the **Kind** and **Role** categories in the UFO, provide a separation of concerns (SoC) mechanism for domain conceptualization. Through this mechanism, those non-rigid moment individuals can be dissected from its bearer and conceptualized separately. In the HO, the **Environment Object** kind object and all the other aforementioned role objects are proposed to implement the SoC mechanism.

6.3.2 The Concepts and Relations in the Hazard Ontology

Mishap represents the accidental events that will consequently cause injuries to people, damage to the environment or significant financial losses. A collision accident is a typical mishap.

Hazard is defined as a situation universal whose instances are situations that comprise a set of essential endurants as well as other possible endurants, in order to trigger severe mishaps. For example, *a running train misses the red light signal before a crossroad at which cars and persons will go across the railway*, labeled as *H1*, is an instance of *Hazard*. In the HO, the essential endurants existing in a hazard consist of the instances of **Mishap Victim**, **Harm TruthMaker**, **Hazard Element**, and **Exposure**.

Harm TruthMaker represents a harmful or critical disposition universal whose instances will characterize certain hazard element role objects that exist in **Hazard**. When a harm truthmaker is manifested by events, harms (e.g., damages, losses, or injuries) are likely to occur. For example, it could be argued that the kinetic energy is the harm truthmaker in the collision hazard, since the collision event manifests the kinetic energy of the train. Moreover, some critical dispositions are regarded as harm truthmaker as well, in that, they can lead to harms, when breached. For example, the timeliness of some safety or mission-critical tasks will pose temporal harms to the system, i.e., once the system misses the deadline of the tasks, losses or system failures will occur.

Hazard Element represents a role universal in **Hazard** whose instances can bear harm truthmaker dispositions. These roles can be played by kind objects. Taking the collision hazard as an example, *a train* is the kind object that plays the *mover* role bearing the *kinetic energy* harm truthmaker.

Mishap Victim is a sub-concept of **Hazard Element** represents a role universal whose instances are not supposed to but have the potential to encounter damages or injuries when a hazard situation triggers severe mishaps. Further,

a mishap victim can bear harm truthmakers as well. Taking *H1* as an example, "cars" and "persons" are the kind objects at the risk of being the victims of the resulted collision mishaps.

Exposure is defined as a relator universal that mediate hazard elements and at least one mishap victim. An exposure represents the relation through which victim(s) will be exposed to the safety threats posed by hazard elements in a hazard. For instance, in the collision hazard *H1*, the cars are exposed to the running train threat through the spatial relation "cars are at the crossroad which the train is running towards".

Initiating Event represents an undesirable or unexpected event that can bring about a hazard, e.g., "the diver fails to properly slow down the train when approaching to a red light", labeled as *IE1*, is a possible initiating event that brings about the collision hazard *H1*.

Initiating Condition is a situation universal whose instances are situations that comprise the necessary endurants to trigger initiating events. For example, a possible initiating condition that triggers the initiating event *IE1* is the fact that "the driver is disturbed by strong sunshine", denoted as *IC1*. Furthermore, the necessary endurants consist of **Initiator Factor** and **Initiating Role**.

Initiator Factor and **Initiating Role** represent a disposition universal and a role universal, respectively, which are necessary in an initiating condition to trigger initiating events. With the example of the initiating condition *IC1*, the sunshine plays the initiating role (i.e., disturbance source) who bears the initiator factor (i.e., strong light brightness), and the people (who plays the driver role as well) plays the initiating role (i.e., disturbance receiver) that bears the initiator factor (i.e., "susceptible to glare")

Environment Object is categorized as a kind universal in terms of UFO, which represents a rigid entity that can play different roles in a hazard, e.g., *a car*, *a train*, *the sunshine*, and *persons* in the collision hazard.

We notice that "initiating" is a relative term, which means that an "initiating event" can always be traced back to a former event that brings about a former initiating condition that triggers it. The consideration is simplified and represented by using a "cause" relation from **Initiating Event** to itself. In addition, a hazard can as well trigger initiating events that subsequently bring about other hazards, which is represented by using a "trigger" relation from **Hazard** to **Initiating Event**. Last but not least, a mishap event can be an initiating event as well.

6.4 Practical Implications

We show in this section the usefulness of the ontological interpretation of hazard by analyzing a set of hazard analysis results from an industrial passenger train project. The hazard analysis results consist of 45 hazard descriptions. Due to the space limitation, we select a sample of the descriptions, as shown in Figure 6.4, for illustration purposes.

Label	Natural Language Hazard Description
H1	Object on the track, when train is approaching
H2	Train getting stuck on the line
H3	Fall from moving train
H4	Harmful chemicals

Figure 6.4: The sample of identified hazards of a passenger train.

Then, we proceed in two stages: 1) we propose a set of heuristic questions to categorize the natural language hazard descriptions (NLHDs) of the hazard analysis results, in accordance to the HO, and 2) we show how the ontological interpretation of hazard can help to reveal some interesting findings hidden in the traditional hazard analysis results.

6.4.1 The Categorization of Hazard Descriptions

To perform the hazard description categorization, we propose a set of heuristic questions. For each NLHD, we will go through all the questions. Based on the answers, we can identify the key concerns of each hazard description in the light of UFO. The heuristic questions are listed as follows:

- **Q1: "Is the NLHD describing a situation (state of affairs) or event?"**. Q1 can be asked to determine if the NLHD is describing a hazard/initiating condition (if the answer is "situation") or mishap/initiating event (if the answer is "event"), according to the HO.
- **Q2: "If the NLHD is describing a situation, can the situation trigger mishaps when some dispositions in the situation are manifested?"**. Q2 can be asked to determine if the NLHD is describing a hazard (if the answer is yes) or initiating condition (if the answer is no), according to the HO.
- **Q3: "If the NLHD is describing a situation, what kind objects or role objects can be identified in the situation?"**. Q3 can be asked to

inspire the environment objects, and hazard element/initiating role of the NLHD.

- **Q4: "If the NLHD is describing a situation, what qualities or properties can be identified in the situation?"**. Q4 can be asked to inspire the harm truthmaker/initiator factors of the NLHD.
- **Q5: "If the NLHD is describing an event, can the event bring about losses or injuries or damages?"**. Q5 can be asked to determine if the NLHD is describing a mishap (if the answer is yes) or initiating event (if the answer is no), according to the HO.
- **Q6: "If the NLHD is describing a hazard situation or a mishap event, who or what will be damaged in the NLHD?"**. Q6 can be asked to determine the mishap victims of the NLHD.

To illustrate how to apply these questions, take as an example the first hazard description "Object on the track, when train is approaching" (labeled as HA-H1). First we apply Q1 and identify that this hazard description is describing a situation. By further examining whether the identified situation could trigger mishaps according to Q2, it is noticed that the described situation is likely to trigger a collision mishap. Moreover, based on Q3 and Q4, we can identify three kind objects (i.e., an object, a train and a track), a disposition (i.e., the kinetic energy of the train), three role objects (i.e., an obstacle played by an object, a mover played by a train, and a place played by track), and a exposure relator (i.e., the mover is approaching the place of an obstacle). After applying Q6, the "both the obstacle and the mover" can be regarded as the mishap victim in this hazard description, since both of them could be damaged after the occurrence of a collision.

Figure 6.5 lists the categorized hazard descriptions with respect to the example hazard list. Note that with the increased experience, the list of questions can be further expanded.

6.4.2 Findings

The main benefit of capturing the ontological meaning of hazards is the conceptual clarification of hazard. In this section, we discuss some interesting findings based on the conceptual analysis of the NLHDs:

- The first type of findings in the hazard analysis results is that the analyst may occasionally regard a mishap event as a hazard. For example, "fall

Label	Natural Language Hazard Description	Categorization according to the HO				
		Initiating Event	Exposure	Hazard Element	Harm TruthMaker	Mishap
H1	Object on the track, when train is approaching		Mover is approaching to obstacle	Mover (Train); Place (Track); Obstacle (Object)	Kinetic energy (Mover); Following a path (Mover); Located on the path (Obstacle)	Collision
H2	Train getting stuck on the line	Train getting stuck on the line				
H3	Fall from moving train					Fall from moving train
H4	Harmful chemicals				Harmfulness of chemicals	

Figure 6.5: A list of categorized hazard descriptions.

from moving train" describes a falling event. Since the mishap victim will be the object (such as a passenger) that participates in the event, this event will be categorized into a mishap. Therefore, hazard analysis such as fault tree analysis should be further conducted, in order to provide more information on how to avoid such mishap.

- The second type of findings is that we can merely identify the harm truthmakers and hazard elements in some NLHDs. However, it is sometimes hard to find information about the exposure and mishap victims in the NLHDs, for example, "harmful chemicals". This type of findings imply that the analyst has documented very generic hazards, without specifying how these generic hazards can lead to a mishap in the context of the system under analysis. Therefore, these generic hazards will not provide useful information for guiding the safety requirements elicitation.

- The third type of findings is that we can merely identify the initiating event/condition in some NLHDs. Nevertheless, finding information about the hazard situation is difficult in those NLHDs, for example, "train getting stuck on the line". The analyst might think that the subsequent hazard (e.g., "Another train is approaching to the stuck train") and mishap (e.g., "Collision") can be easily foreseen in this case. However, the missing information will be very useful for facilitating the reuse of analysis results. Supposed that, in another project, the passenger train will solely engage a line, then the "Train getting stuck on the line" might no longer be a hazard.

- The fourth type of findings is that the categorized hazards can help to reveal similarities or patterns between different hazard descriptions. When

we identify the key concerns of NLHDs in accordance to the HO, we may find the same exposure relation or role objects in different NLHDs. For example, the hazards "object on the track, when a train is approaching" and "train getting stuck on the line" both belong to the mover-obstacle-collision hazard. The major difference lies in that the kind object (i.e., the train) will play different hazard element roles (i.e., the mover and the obstacle, respectively) in these hazards. Therefore, we believe that the similarities or patterns behind different hazards will be helpful for the analyst to identify new hazards, by analyzing the possibility that a kind object play different roles in a known hazard pattern.

6.5 Related Work

Winther et al. [4] propose an ontological conceptualization of hazard to address the confusion concerning what are called hazards. Different from ours, they regard a hazard as an event or state at the boundary of a system that can lead to an accident. In our ontology, a hazard is regarded as a situation where a system can play different roles, which means the system can not only lead to a hazard, but also is exposed to hazards.

Lawrynowicz et al. [6] describe an ontology design pattern for modeling hazardous situations. They take some foundational concepts (such as object, event) into account as well, but their work is not grounded in well-founded foundational ontology. Therefore, some concepts suffers from a lack of real-world semantics. For example, what is a hazard is not properly answered.

Daramola et al. [13] presents a framework and tool prototype that facilitates the early identification of potential system hazards. A HAZOP ontology is defined in the framework, which consists of types of study node, description, guidewords, deviations, causes, consequences, risk level, safeguards, and recommendation. Their main objective is, different from ours, to discover potential hazards.

In [14], the authors propose an ontology to support the methodology behind typical preliminary hazard analysis. Our work is related in the sense that we define the entities, events and situations leading to a hazard, however, our ontology contains additional entities, e.g., initiating factors (allowing an understanding of dependencies between hazards), role (facilitating the understanding of how environmental object contribute to initiating hazardous events under different conditions).

In [15], the authors present a conceptual ontology for risk analysis in med-

ical environments. Contrary to our focus on SCSs, the aim of their work is to overcome the difficulties in applying HAZOP for medical processes.

Vargas et al. [5] propose an ontology-based approach to hazard identification within the preliminary hazard analysis worksheet by utilizing the reasoning capability of ontologies. However, their ontology is not grounded in a well-founded foundational ontology.

Functional hazard assessment (FHA) is a technique advocated in ARP4754 [16] and ARP4761 [17] as a way of systematically identifying hazards. The FHA treats hazard as a functional failure problem. In contrast, we regard hazard as a situation that can lead to accidents. Therefore, failures are not necessarily equal to hazards, since the environment when failures occur need to be considered as well.

Habli et al. [18] propose a product-line functional hazard model which is integrated with product-line context and domain models. Similarly, the authors treat hazard as a functional failure problem, and the core concepts in the hazard model are Failure Condition and Effect.

Leveson et al. [1] present a recent accident casualty model that provides a vision of hazards differently. Hazards are defined based on the system control theory, i.e., potential hazards are regarded as a situation when component failures, external disturbances, and/or potentially unsafe interactions among system components are not handled adequately or controlled. Differently, we provide a formal definition of hazard based on the foundational ontology, UFO.

UFO has been applied as a foundational ontology in many pieces of work. Falbo et al. [19] use an industrial case to illustrate how UFO can serve as a foundational ontology to conceptualize a specific domain. Ruy et al. [20] present an ontological analysis of the Software Engineering Metamodel for Development Methodologies (SEMDM), provided by the ISO/IEC 24744 Standard. This analysis is done in the light of the UFO. As a result, some of the problems identified in SEMDM is presented. In addition, In [21], Guizzardi et al.present the latest developments in the UFO ontology. Furthermore, they elaborate on the relevance of these foundational ontologies in the development of domain ontologies by showing a case study in the software process domain. Bringuente et al. [22] discuss the re-engineering of part of a Software Process Ontology based on the UFO, which is an extension of the work presented in [21].

6.6 Conclusion and Future Work

In this paper, we have proposed the Hazard Ontology (HO) to define an ontological interpretation of hazard. In particular, the main idea behind our ontology is that, a hazard represents a situation which comprises the necessary entities to trigger mishaps, and further the hazard is brought about by some initiating events. In addition, the HO takes the foundational categories into account, by dint of being grounded in the Unified Foundational Ontology (UFO). In this way, the HO is able to utilize the benefits offered by the foundational ontology, such as real-world semantics, ontology design patterns, and pre-defined relations between foundational categories. Furthermore, an industrial train project is used to show how the proposed ontology can categorize hazard descriptions and reveal some interesting findings.

This work provides a starting point for our future work. Our next step is to conduct more industrial case studies to further evaluate the usefulness of the proposed ontology and improve it. Moreover, we believe the Hazard Ontology can provide guidance to hazards identification and mitigation. Therefore, one interesting piece of future work is to propose an approach to the identification of hazards and the elicitation of safety requirements, based on the conceptual clarity and rationale behind hazards that ontologies provide. Finally, tooling support is considered as an essential part of future work as well.

Bibliography

[1] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press, 2011.

[2] MTL-STD-882, "DoD Standard Practice for System Safety, version D," 2000.

[3] EN-50129, "Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling," 2003.

[4] R. Winther and W. Marsh, "Hazards, accidents and events - a land of confusing terms," in *Safety, Reliability and Risk Analysis Beyond the Horizon*, pp. 2545–2553, 2013.

[5] A. P. Vargas and R. Bloomfield, "Using Ontologies to Support Model-based Exploration of the Dependencies between Causes and Consequences of Hazards," in *Proceedings of KEOD'15,*, pp. 316–327, 2015.

[6] A. Lawrynowicz and I. Lawniczak, "The Hazardous Situation Ontology Design Pattern," in *Proceedings of WOP'15*, 2015.

[7] M. A. Cheatham, H. Ferguson, C. Vardeman, and C. Shimizu, "A Modification to the Hazardous Situtation ODP to Support Risk Assessment and Mitigation," 2016.

[8] G. Guizzardi, *Ontological Foundations for Structural Conceptual Model*, vol. 015. 2005.

[9] H. Herre, B. Heller, P. Burek, R. Hoehndorf, F. Loebe, and H. Michalek, "General Formal Ontology (GFO): A Foundational Ontology Integrating Objects and Processes. Part I: Basic Principles (Version 1.0)," tech. rep., 2006.

[10] R. Arp, B. Smith, and A. Spear, *Building Ontologies with Basic Formal Ontology*. MIT Press, 2015.

[11] C. Masolo, S. Borgo, A. Gangemi, N. Guarino, and A. Oltramari, "Ontology Library," in *WonderWeb Deliv. D18*, 2003.

[12] C. A. Ericson, *Hazard Analysis Techniques for System Safety*. Wiley, 2005.

[13] O. Daramola, T. Stålhane, G. Sindre, and I. Omoronyia, "Enabling Hazard Identification from Requirements and Reuse-Oriented HAZOP Analysis," in *Proceedings of MARK'11*, pp. 3–11, 2011.

[14] M. H. Mazouni and J. F. Aubry, "A PHA based on a Systemic and Generic Ontology," in *Proceedings of SOLI'07*, pp. 1–6, Aug 2007.

[15] T. Sigwarth, K. Loewe, E. Beck, L. Pelchen, and T. Schrader, "Conceptual Ontology of Prospective Risk Analysis in Medical Environments - the OPT-Model-Ontology," in *Proceedings of ICICIS'15*, pp. 88–93, Dec 2015.

[16] ARP4754, "Certification Considerations for Highly-Integrated or Complex Aircraft Systems," *Society of Automotive Engineers*, 1994.

[17] ARP4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," *Society of Automotive Engineers*, 1995.

[18] R. P. Ibrahim Habli, Tim Kelly, "Functional Hazard Assessment in Product-Lines - A Model-Based Approach," in *Proceedings of MDPLE'09*, pp. 26–33, June 2009.

[19] R. Falbo, F. Baião, M. Lopes, and G. Guizzardi, "The Role of Foundational Ontologies for Domain Ontology Engineering: An Industrial Case Study in the Domain of Oil and Gas Exploration and Production," *International Journal of Information System Modeling and Design*, vol. 1, pp. 1–22, Apr. 2010.

[20] F. B. Ruy, R. de Almeida Falbo, M. P. Barcellos, and G. Guizzardi, "An Ontological Analysis of the ISO/IEC 24744 Metamodel," in *Proceedings of FOIS'14*, pp. 330–343, 2014.

[21] G. Guizzardi, R. Falbo, and R. S. S. Guizzardi, "Grounding Software Domain Ontologies in the Unified Foundational Ontology (UFO): The case of the ODE Software Process Ontology," in *Proceedings of IDEAS08*, pp. 127–140, 2008.

[22] A. C. O. Bringuente, R. A. Falbo, and G. Guizzardi, "Using a Foundational Ontology for Reengineering a Software Process Ontology," *Journal of JIDM*, vol. 2, no. 3, pp. 511–526, 2011.