An Ontological Approach to Hazard Identification for Safety-Critical Systems

Jiale ZHOU, Kaj Hänninen, Kristina Lundqvist, Luciana Provenzano
Mälardalen University
Västerås, Sweden
zhou.jiale@mdh.se

Abstract—**Hazard identification is an essential and demanding task for the development of safety-critical systems (SCSs). Current practices suffer from one or several drawbacks: 1) a common hazard conceptualization is missing and thereby ambiguities may arise and, 2) there is still a need to formalize the experience of analysts and lessons learned from previous system development. It should be done in a structured way to facilitate future reuse and, 3) some hazard identification techniques require well-known system behaviors represented by models, such as automata and sequence diagrams, to identify hazards. However, such models are typically susceptible to changes or even not available in early stages of the development process. In this paper, we propose an ontological approach to support hazard identification in the early stages of the development of SCSs. The approach aims to improve the completeness of hazard identification results and to avoid ambiguities. A robotic strolling assistant system is used to evaluate the proposed approach.**

Keywords—hazard ontology; safety-critical systems; hazard identification

I. Introduction

Safety-critical systems (SCSs) have, for some time, been an intrinsic part of human life in multiple domains, e.g., in the automotive, avionics, rail industries and medical domain. Such systems are likely to be involved in various hazardous situations[1], which can lead to severe consequences [1]. Preliminary hazard analysis (PHA) is a key safety-concerned technique, applied during the early stages of the SCSs development process, aiming to provide stakeholders, e.g., developers, organizations and authorities, with a general understanding of potential hazards. When analysts conduct the PHA to discover hazards, they typically start by using a list of common hazards together with the system descriptions as initial inputs. After a brainstorming session, potential hazards are identified and then recorded in the form of natural language hazard descriptions in the PHA worksheet [2]. The hazard descriptions will serve as a heuristic and negotiation basis to design hazard mitigation mechanisms in the subsequent risk reduction activities. However, it is not an easy task to perform hazard identification in the PHA. A consensus has been reached that the most significant flaws in hazard analysis techniques are typically related to the omission of potential hazards [3].

Much effort has been devoted into exploring how hazard identification should be conducted in the early stages of SCSs development, e.g., HAZOP [4], EAST-ADL based PHA [5], STMP/STECA [1] [6], and model-based PHA [3]. The main drawbacks of the current practice applied in the hazard identification, lie in that: 1) due to the lack of a common understanding of the hazard concept, the hazards are typically identified in accordance to the intuition and experience of the analysts [2], with the risk of missing environmental assumptions and causing ambiguities in the recorded hazard descriptions [7] and, 2) since the hazard identification highly relies on the experience possessed by the analysts and the lessons obtained from previous systems development, there is a need to formalize these experiences in a structured way for the purpose of reuse [8] and, 3) since traditional hazard identification techniques are usually based on well-known system behaviors [9] represented by models, such as automata and sequence diagrams, a new approach is needed when such behavioral models are not available.

In our earlier work [7], we have presented an ontological interpretation of the hazard concept, i.e., the Hazard Ontology (HO), aiming to achieve a better understanding of the hazard concept. Generally, the HO is a reference model, including a set of hazard-related concepts (such as, **Mishap**, **Hazard**, **Initiating Event**) and relations (such as causal relations), which provides a conceptual basis to perform hazard identification. These considerations motivate us to formulate the following research question: Based on system descriptions, is it possible to utilize the Hazard Ontology to improve the identification of potential hazards associated with the system under analysis?

In this paper, we propose an ontological approach to hazard identification, called OHI, aiming to improve the completeness of hazard identification results and to avoid ambiguities. In general, the hazard identification approach consists of three steps:

- **OHI-Step 1: System Description Formalization** formalizes the system descriptions from natural language into the HO-style models.
- **OHI-Step 2: Mishap Victim Identification** identifies all the possible mishap victims in the HO-style model

[1] The involvement includes two aspects: 1) the system causes a hazard or; 2) the system is exposed to a hazard

978-1-5386-0918-7/17/$31.00 ©2017 IEEE

and then brainstorms possible harms threatening the victims.

- **OHI-Step 3: Hazard Population** brainstorms to identify hazardous situations that can lead to the corresponding harms, in accordance to the concepts and relations defined in the Hazard Ontology.

We have applied the OHI approach on a robotic strolling system that has been analyzed by the HAZOP-UML method to identify hazards [9]. The results obtained by the OHI approach have shown a promising potential that OHI can achieve a more complete and useful set of hazards when compared with the results of the HAZOP-UML method.

The remainder of this paper is organized as follows: Section II briefly elaborates the Hazard Ontology. Section III presents the proposed approach in detail, and the robotic strolling system is used to illustrate the approach. Section IV describes the evaluation results of our work. Section V introduces related work, and finally concluding remarks and future work are outlined in Section VI.

II. The Hazard Ontology

The Hazard Ontology (HO) proposed in [7] is an ontological interpretation of the hazard concept. In order to interpret the hazard-related concepts in real-world semantics[2], the HO is explicitly grounded in a theoretically well-founded foundation ontology, i.e., the Unified Foundational Ontology (UFO) [10]. Comparing with other existing foundational ontologies, such as GFO [11], BFO [12], DOCLE [13], etc., we notice that UFO provides a more complete set of concepts to cover important aspects of hazards. Figure 1 depicts the Hazard Ontology (HO) using a UML class diagram.

Generally, the UFO provides the system analysts with a uniform perspective to observe the entities in the real-world. The HO inherits this merit, and it includes a set of foundational concepts to represent these real-world entities. An event, i.e., an instance of **Event**, is an entity where its constituent parts cannot be present simultaneously. For instance, *a car collision event* can comprise two parts "cars crash into each other" and "cars bounce off". These two parts can only exist in a chronological order. Two concepts are defined to categorize objects in the HO, i.e., **Kind** and **Role**. For example, a person is a *kind* object, and conversely, a driver is a *role* object. A "play" relation is defined between a *kind* object and a *role* object, such as "a person" can play the role "a driver". A relator, i.e., an instance of **Relator**, is a relational property connecting multiple objects. A disposition, i.e., an instance of **Disposition**, denotes a property that can characterize an object. A situation, i.e., an instance of **Situation**, is considered as state of affairs, i.e., a portion of reality that can be comprehended as a whole. The constituent parts of a situation can be *kind*/*role* objects, relators, and dispositions. For example, in the situation "a passenger train is approaching a person who is crossing the track", there exist three objects (i.e., *a train, a person, a track*), two relators (i.e., *being-approaching* and *being-crossing*), and two *kinetic energy* dispositions that characterize *a person* and *a train*, respectively.

Two foundational ***causal relations*** are defined between events and situations, i.e., a situation can **trigger** an event and the event will then **bring about** another situation. The idea behind the causal relations is: 1) the occurrence of an event is the manifestation of a collection of dispositions existing in a situation, for instance, an "a train enters a temporary speed restriction area" event is the manifestation of the "kinetic energy" disposition of the train and the "boundary" disposition of the temporary speed restriction area, and 2) an event may change reality by changing the state of affairs from one situation to another, for example, the "a train enters a temporary speed restriction area" event will change the reality from the situation "a train is running on the track at a high speed" to the situation "a train is running on the track where it should slow down".

The HO provides the analysts with a UFO-consistent perspective to explain the hazard-related concepts and relations. The main idea behind the HO is in line with some widely accepted definitions of hazards in the context of SCSs [1] [14], that is, a hazard is supposed to be characterized by two essential features. On one hand, the nature of a hazard is a set of states, which motivates the interpretation that **Hazard** is a type of **Situation**. On the other hand, the states are likely to lead to severe consequences, which is interpreted into the modeling decision that **Hazard** can trigger **Mishap**. A mishap is an accidental event that will consequently cause injuries to people, damage to the environment or significant financial losses. Inspired by the first idea behind the causal relations, the essential constituent parts existing in a hazard consist of mishap victims, harm truthmakers, hazard elements, and exposures. **Harm TruthMaker** represents the harmful or critical dispositions in a hazard. When such harm truthmakers are manifested, mishaps are likely to occur. **Hazard Element** denotes the *role* objects that bear the harm truthmaker dispositions. These roles can be played by various *kind* objects. **Mishap Victim** is a sub-concept of **Hazard Element**. A mishap victim denotes a *role* object that is not supposed to but have the potential to encounter damages or injuries. **Exposure** represents the relations through which victim(s) will be exposed to harms posed by hazard elements.

According to the foundational casual relations "bring about" and "trigger" between events and situations, we define that a hazard can be brought about by at least one initiating event. An initiating event, i.e., an instance of **Initiating Event**, is an undesirable or unexpected event that can bring about a hazard situation. **Initiating Condition** is defined to capture the knowledge that are of importance to understand how the initiating events are triggered. An initiating condition, i.e., an instance of **Initiating Condition**, is a situation that comprises the necessary constituent parts to trigger initiating events. Furthermore, **Initiator Factor** and **Initiating Role** represent the dispositions and roles, respectively, which are necessary constituent parts of an initiating condition to trigger initiating events. An environment object, i.e., an instance of **Environment Object**, is a *kind* object that can play different roles in a hazard

[1] Real-world semantics indicates the correspondence between a domain-specific concept (e.g., hazard) and foundational concepts (e.g., object, relation, situation, event, etc.) in the real world.

or initiating condition. The **cause** relation implies that a pre-initiating event can bring about an initiating condition which will trigger another post-initiating event to bring about a hazard.

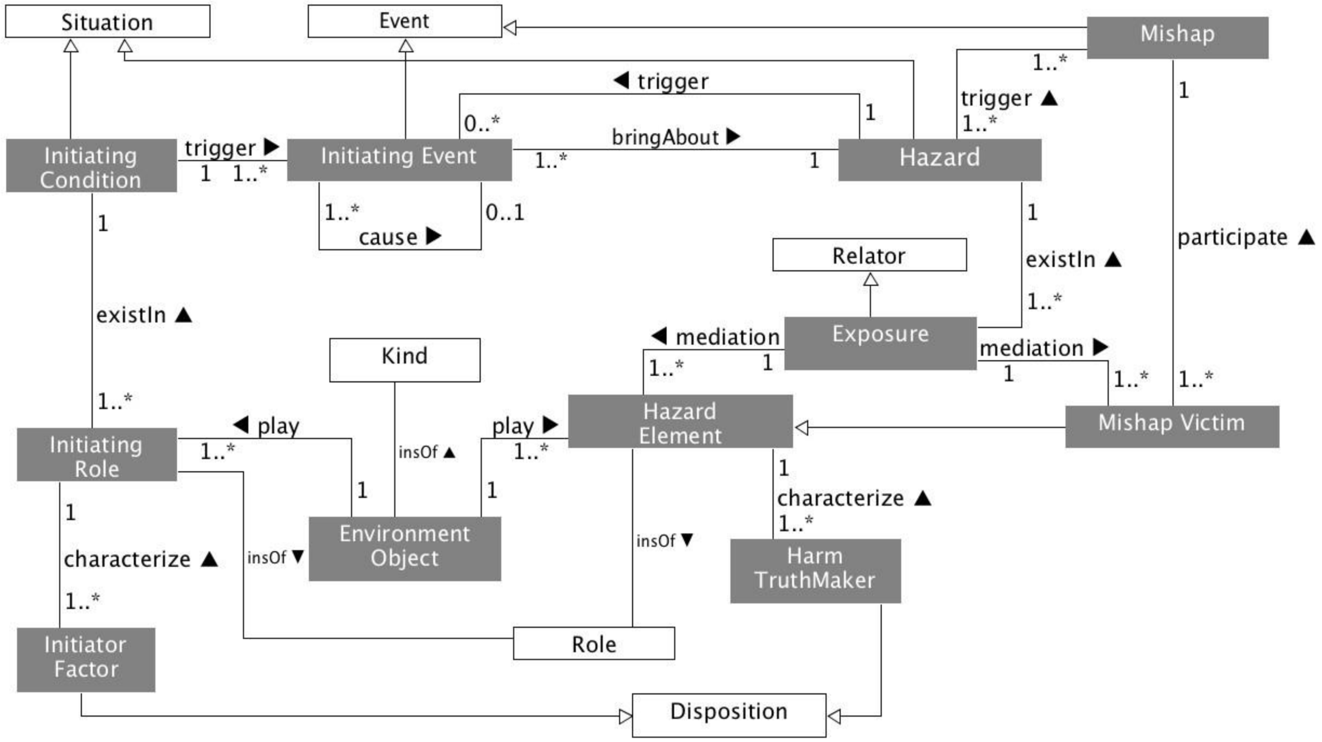


Figure 1. The UML class diagram of the Hazard Ontology. Concepts are represented as rectangles. The hazard-related concepts are colored in gray, and the foundational concepts are white. Typed relations are represented by lines with a reading direction pointed by "►", from open end to aggregated end. Cardinality constraints are labeled on each end of typed relations. Subsumption constraints are represented by open-headed arrows lines with "△" 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.

III. The Ontological Approach to Hazard Identification - OHI

In this section, we describe the robotic strolling system [9] in Section III-A, which will be used to illustrate and further to evaluate our approach. Then, we introduce the ontological approach, called OHI, to identify potential hazards in detail, consisting of three steps: system description formalization in Section III-B, mishap victim identification in Section III-C, and hazard population in Section III-D.

A. Description of the Robotic Strolling System

The robotic strolling system [9] aims to help partially-disabled persons to stand up, stroll and sit down, when medical care staff are not available. It is intended to be used in elderly care centers by patients suffering from gait and orientation problems. The system consists of a wheeled base and a moving handlebar, as shown in Figure 2. The robotic strolling system is also equipped with several sensors to detect physiological parameters and the posture of patients. When an abnormality occurs, it will raise an alarm to inform the medical care staff. It is designed to be able to move autonomously and navigate itself to the patients when it is called. The preliminary design of the robot is described by 11 use cases: Standing up operation (UC01), Strolling (UC02), Sitting down operation (UC03), Balance loss handling (UC04), Call and autonomous movement of the robot (UC05), End of use detection and movement to a waiting position (UC06), Positioning the robot by hand (UC07),

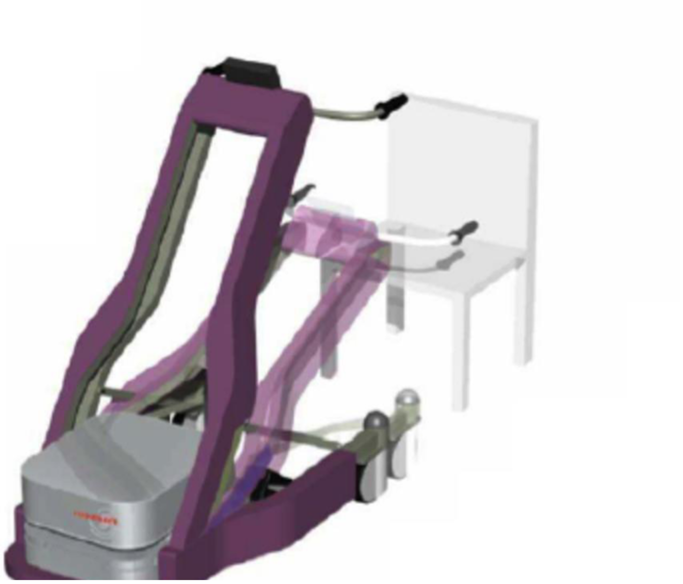


Figure 2. The first prototype of the robotic strolling system [9].

Alarms handling (UC08), Patient profile programming (UC09), Patient profile learning (UC10), and Robot set-up (UC11).

B. *OHI-Step 1: System Description Formalization*

The first step in the OHI approach is to formalize the system description from natural language into the HO-style models. In this step, the analysts will identify the objects described by the system description and clarify the relations between the objects in accordance to the system description and their expertise. The aim of this step is to achieve a clear understanding of the system from a real-world perspective. The formalization can be conducted by going through the following steps:

- **SDF-Step 1**: Identify the *kind* and *role* objects explicitly presented in the system description.
- **SDF-Step 2**: For each *kind* object obtained in SDF-Step 1, identify all the roles it can play, considering the system description.
- **SDF-Step 3**: For each *role* object obtained in SDF-Step 1 and SDF-Step 2, identify the relator that connects this role, and specify all the other roles connected by the identified relator, considering the system description and the analysts' expertise.
- **SDF-Step 4**: For each *role* object obtained in SDF-Step 1, SDF-Step 2 and SDF-Step 3, identify all the *kind* objects that can play the role, considering the system description.

We choose the UC01 "Standing up operation" of the robotic strolling system to further illustrate this step. The description of the UC01 is shown in Table I.

TABLE I. UC01: STANDING UP OPERATION

Use case name	UC01. Standing up operation
Abstract	The patient stands up with the help from the robot.
Pre-condition	The patient is sitting down. The robot is waiting for the standing up operation. Battery charge is sufficient to do this task and to help the patient to sit down again. The robot is in front of the patient.
Post-condition	The patient is standing. The robot is in admittance mode.
Invariant	The patient holds both handles of the robot. The robot is in standing up mode. Physiological parameters are acceptable.

We can identify *Robot*, *Robot Handle*, *Battery*, *Patient* as *kind* objects according to the description. The *Patient* can play two roles *BeingSupported* and *BeingLifted*. The *Robot Handle* can play two roles *BalanceSupporter* and *ObjectLifter*. The *Robot* can play the *ElectricityConsumer* role, and the *Battery* can play the *ElectricitySource* role. The *BalanceSupport*, *LiftUp*, and *ElectricityConsumption* relators can be further identified. The *BalanceSupport* relator connects the *BalanceSupporter* and *BeingSupported* roles, played by *Robot* and *Patient* respectively. The *LiftUp* relator connects the *ObjectLifter* and *BeingLifted* roles, played by *Robot Handle* and *Patient* respectively. The *ElectricityConsumption* relator connects the *ElectricitySource* and *ElectricityConsumer* roles, played by *Battery* and *Robot* respectively. After performing the SDF-Step 1 to SDF-Step 4, we obtain the formalized description for the UC01, as shown in Figure 3.

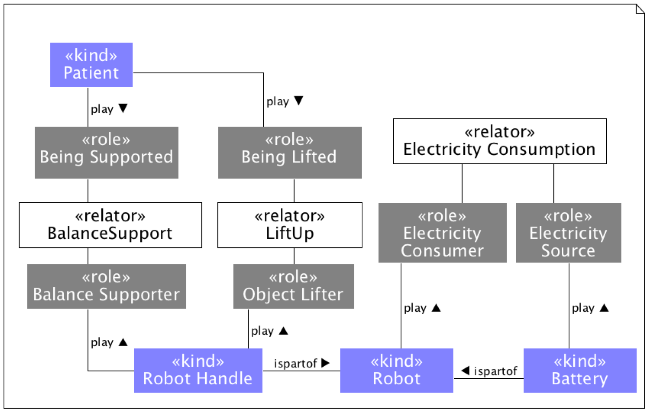


Figure 3. The formalized description for the UC01 "Standing Up Operation". Kind objects are colored in purple, role objects are colored in gray, and relators are white.

C. *OHI-Step 2: Mishap Victim Identification*

Since the occurrence of a mishap event must have more than one mishap victim to participate in the event, this step identifies all the possible mishap victims from the HO-style model obtained in OHI-Step 1. As defined in the HO, a mishap victim denotes a *role* object. Therefore, we need to go through all the roles presented in the HO-style model and analyze if the roles are not supposed to but have the potential to encounter harms. Furthermore, the analysts continue with identifying possible harms that can affect the victims, including but not limited to, physical damages, chemical injuries, fatal illness, explosion, etc.

Take the UC01 as an example. The possible roles presented in Figure 3 that have the potential to encounter harms are *BeingLifted* at the risk of physical damage (e.g., falling down on the ground, colliding with other obstacles), *BeingSupported* at the risk of physical damage (e.g., falling down on the ground), and *ElectricityConsumer* at the risk of explosion and electric shock. Then, we can identify that the mishap victims of the UC01 are identified as *BeingLifted*, *BeingSupported* and *ElectricityConsumer* roles.

D. *OHI-Step 3: Hazard Population*

This step identifies the hazardous situations that are likely to harm the identified mishap victims, in accordance to the concepts and relations defined in the Hazard Ontology.

According to the HO, the occurrence of a mishap is the manifestation of the *harm truthmaker* dispositions that characterize the *hazard element* roles in a hazardous situation. The following steps can be taken to populate the possible hazardous situations based on the HO-style model from OHI-Step 1 and the identified mishap victims together with the possible harms from OHI-Step 2:

- **HP-Step 1**: Select one mishap victim from the identified mishap victims from OHI-Step 2.
- **HP-Step 2**: Identify the environment object playing the selected mishap victim, the relator connecting the

selected mishap victim and the roles that are connected by the identified relator, according to the HO-style model from OHI-Step 1.

- **HP-Step 3**: For each role identified in the HP-Step 2, explore the possible dispositions that characterize this role. When such possible dispositions are manifested, a mishap that can cause harm is likely to be triggered. Furthermore, the role will be identified as **Hazard Element**, the dispositions as **Harm TruthMaker**, and the relators connecting the hazard elements as **Exposure**.
- **HP-Step 4**: For each hazard element identified in HP-Step 3, explore the possible *kind* object that can play the hazard element role. The *kind* object will be identified as **Environment Object**.
- **HP-Step 5**: Repeat HP-Step 1, until all the mishap victims are analyzed.

We continue with the UC01 to illustrate this step. Note that we have identified three mishap victims along with the harms they are likely to encounter. Therefore, we can explore the possible *environment object* and *exposure* relators, and identify the possible *harm truthmaker* dispositions. The identified hazards are shown in Table II. Each row in the table denotes a HO-style hazard. The *Mishap Victim (Env Object)* column denotes the mishap victim selected in HP-Step 1 and its environment object. The *Exposure*, *Hazard Element (Env Object)*, and *Harm Truthmaker* in the same row represents the identified hazardous situation: 1) the *Exposure* column denotes the identified relator in HP-Step 2 and, 2) the *Hazard Element (Env Object)* column denotes the *role* object analyzed in HP-Step 3 and its corresponding environment object identified in HP-Step 4 and, 3) the *Harm Truthmaker* column denotes the identified disposition in HP-Step 3 which characterizes the corresponding hazard element. Meanwhile, each HO hazard is interpreted into natural language as well, shown in the *Natural Language Hazard Description* column.

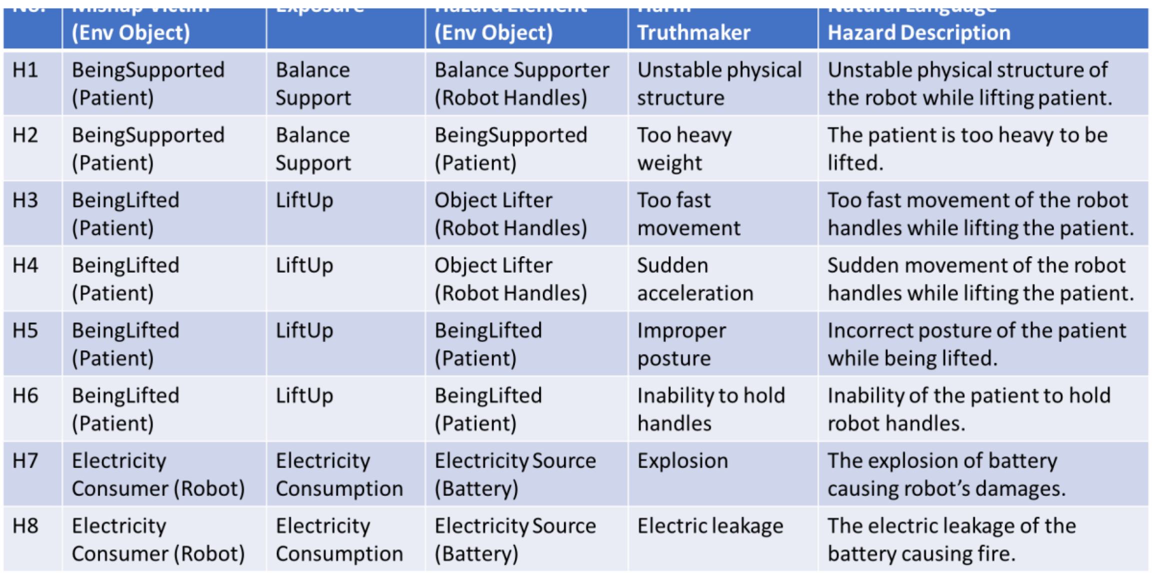
IV. Evaluation

We evaluated the ontological approach to hazard identification (OHI) by applying it on the 11 use cases of the robotic strolling system presented in Section III-A. The results produced by the OHI were compared with those by the HAZOP-UML method presented in [9]. The HAZOP-UML method identified 16 types of hazards in total, as shown in the right part of Table III, which were referred to as *RH*. After we went through all the 11 use cases, the hazards identified by the OHI were categorized into 21 types of hazards in total. The natural language hazard descriptions are listed in the left part of Table III, which were referred to as *LH*.

From the comparison, we can notice that: 1) the OHI identified more types of hazards than the HAZOP-UML, which means the 16 types of hazards identified by the HAZOP-UML can find their counterparts in the 21 types of hazards by the OHI but not vice versa; for instance, the OHI can identify not only the types of hazards that may cause physical harms (e.g., LH1, LH2, etc.), but also the types of hazards that may cause chemical harms (e.g., LH18 and LH19) and, 2) the hazards identified by the OHI were situations where certain mishaps could occur, and these hazards could provide guidance information for subsequent risk reduction activities; conversely, some of the hazards by the HAZOP-UML were simply mishaps, such as RH9 and RH10, which provide little information about how these mishaps could occur and, 3) the hazards identified by the OHI explicitly considered the environmental factors that are very important for stakeholders to understand the hazards, such as LH9 and LH14. Although this evaluation was limited to one case, the comparison has shown that our approach has a potential to discover additional types of hazards compared to HAZOP-UML. We also notice that OHI provides useful guidance for subsequent risk reduction activities, based on the same set of system description.

Both the HAZOP-UML and the OHI require some personal experience and domain expertise to properly apply guide-words

TABLE I. The identified hazards for the UC01 "STANDING UP OPERATION" by the OHI.



No.	Mishap Victim (Env Object)	Exposure	Hazard Element (Env Object)	Harm Truthmaker	Natural Language Hazard Description
H1	BeingSupported (Patient)	Balance Support	Balance Supporter (Robot Handles)	Unstable physical structure	Unstable physical structure of the robot while lifting patient.
H2	BeingSupported (Patient)	Balance Support	BeingSupported (Patient)	Too heavy weight	The patient is too heavy to be lifted.
H3	BeingLifted (Patient)	LiftUp	Object Lifter (Robot Handles)	Too fast movement	Too fast movement of the robot handles while lifting the patient.
H4	BeingLifted (Patient)	LiftUp	Object Lifter (Robot Handles)	Sudden acceleration	Sudden movement of the robot handles while lifting the patient.
H5	BeingLifted (Patient)	LiftUp	BeingLifted (Patient)	Improper posture	Incorrect posture of the patient while being lifted.
H6	BeingLifted (Patient)	LiftUp	BeingLifted (Patient)	Inability to hold handles	Inability of the patient to hold robot handles.
H7	Electricity Consumer (Robot)	Electricity Consumption	Electricity Source (Battery)	Explosion	The explosion of battery causing robot's damages.
H8	Electricity Consumer (Robot)	Electricity Consumption	Electricity Source (Battery)	Electric leakage	The electric leakage of the battery causing fire.

TABLE II. Result of contrasting the OHI with the HAZOP-UML method.

The hazards identified by the OHI	The hazards identified by the HAZOP-UML
1. Incorrect posture of the patient during robot use 2. Inability of the patient to hold robot handles (due to too slippery handle or patient tiredness) 3. No alarm or late alarm to inform medical staff during the fall of the patient 4. No alarm or late alarm to inform medical staff during the physiological problem of the patient 5. Unstable physical structure of the robot (due to bad quality or too heavy weight of the patient) 6. Imbalance of the robot (due to bumpy ground or uneven wheel) 7. Easy to catch patient’s clothes during robot’s or its handles’ movement 8. Inability of the robot to detect obstacle ahead during its autonomous movement 9. Inability of the robot to detect dangerous situation during its autonomous movement (such as road curbs, downstairs) 10. Inability of the robot to navigate to the right position 11. Not easy to operate the robot for the patient 12. Too fast movement of the robot for the patient during strolling 13. Too fast movement of the robot’s handle for the patient during helping the patient stand up or sit down 14. Prevent the patient from noticing dangerous situation ahead during strolling (such as downstairs, road curbs) 15. Disturbance of medical staff during an intervention 16. Injuries of the patient due to robot sudden movements while carrying the patient 17. Fall of the patient from the robot seat 18. Battery explosion to cause injuries of robot and patients 19. Electric leakage to cause fire or electric shock 20. Inability of the robot to detect the fall of the patient 21. Inability of the robot to detect the physiological problem of the patient	1. Incorrect posture of the patient during robot use 2. Fall of patient due to imbalance not caused by the robot 3. Robot shutdown during its use 4. Patient falls without alarm or with a late alarm 5. Physiological problem of the patient without alarm or with a late alarm 6. Fall of the patient due to imbalance caused by the robot 7. Failure to switch to safe mode when a problem is detected. The robot keeps on moving 8. Robot parts catching patient or clothes 9. Collision between the robot (or robot part) and the patient 10. Collision between the robot and a person other than the patient 11. Disturbance of medical staff during an intervention 12. Patient loses his/her balance due to the robot (without falling) 13. Robot manipulation causes patient fatigue 14. Injuries of the patient due to robot sudden movements while carrying the patient on its seat 15. Fall of the patient from the robot seat 16. Frequent false positive alarms (false alarm)

in the HAZOP-UML method and to build the HO-style models in the OHI. One advantage of the HAZOP-UML is that they provide a systematic way to analyze unintended deviations and then to identify hazards, but the HAZOP-UML also requires a more detailed system description in terms of use case textual descriptions, UML state-machine diagrams and sequence diagrams [9]. When performing the OHI, we only use the use case textual descriptions to identify the *kind/role* objects and relators. Furthermore, our OHI approach can reuse some patterns to formalize the system descriptions, which to a large extend facilitates the identification process. For instance, the *BalanceSupport* relator along with its corresponding roles is repeatedly identified in different use cases, e.g., UC01 “Standing up operation”, UC02 “Strolling”, and UC03 “Sitting down operation”. The identified hazards of the UC01 which are associated with the *BalanceSupport* relator and its roles can enlighten analysts when they identify potential hazards of the UC02 and UC03. Therefore, such patterns can to a great extent facilitate the hazard identification to save effort. When the analysts have more experience on the OHI approach, more useful patterns can be identified.

V. Related Work

A number of different hazard analysis techniques have been proposed over the years, and some are currently used by safety-critical industries [15]. There are different examples of their use in complex systems. There are also examples of adaptations of standard hazard analysis techniques for identifying hazards [5] [16].

Despite the wide use of the standard hazard analysis techniques, new techniques emerge. For example, Leveson describes a new approach to hazard analysis, STPA (System-Theoretic Process Analysis) [1], which has been particularly applied for the analysis of hazards and their causes in today's complex socio-technical systems [17]. Another example is the Ontological Hazard Analysis (OHA) [18] proposed by Ladkin for the analysis and maintenance of safety hazard lists using a refinement approach. Different from their approaches, we employ the HO to formalize the knowledge of the system and the analysts' expertise and thereby explore potential hazards, which inherently accords with the way in which people explore the reality.

Daramola et al. [19] 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. Different variations of HAZOP are presented as well, such as [9]. Vargas et al. [3] propose an ontology-based approach to hazard identification within the preliminary hazard analysis worksheet by utilizing the reasoning capability of ontologies. Their main objectives are different from ours, since they discover potential hazards based on existing PHA results, whereas our approach aims to discover hazards based on the system descriptions and analysts' expertise.

VI. Conclusion and Future Work

In this paper, we have proposed an ontological approach to hazard identification, called OHI. The main idea of our approach is to use the Hazard Ontology (HO) [7] to provide a consistent way to formalize the system descriptions and analysts' expertise of hazards. The formalized HO-style models can provide a basis for the identification of hazards.

In general, the approach consists of three steps, in terms of system description formalization to understand the system and its environment, mishap victim identification to find possible mishap victims, and hazard population to identify potential hazardous situations. In addition, our approach has been evaluated using a robotic strolling system and the identified hazards are compared with the results produced by the HAZOP-UML method. The comparison shows a promising potential of our approach to identify different types of hazards from existing techniques and provide guidance information for subsequent risk reduction activities. We are currently evaluating the proposed approach to identify hazards on a more complex system consisting of autonomous vehicles.

The hazard identification can provide a heuristic and negotiation basis for subsequent risk reduction activities. As future work, we also plan to propose a requirement elicitation approach based on the identified hazards, which can have a trade-off mechanism to elicit suitable safety requirements. Tooling support is considered as an essential part of future work as well.

Acknowledgement

Our research is supported by the Dependable Platforms for Autonomous systems and Control (DPAC) project through the Knowledge Foundation (KKS).

References

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

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

[3] 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, 2015, pp. 316–327.

[4] F. Crawley, M. Preston, and B. Tyler, HAZOP: Guide to Best Practice: Guidelines to Best Practice for the Process and Chemical Industries, 2000.

[5] R. Mader, G. Griessnig, A. Leitner, C. Kreiner, Q. Bourrouilh, E. Armengaud, C. Steger, and R. Weiss, "A computer-aided approach to preliminary hazard analysis for automotive embedded systems," in Proceedings of ECBS'11, 2011, pp. 169–178.

[6] C. Fleming, Safety-driven Early Concept Analysis and Development, 2015.

[7] J. Zhou, K. Hänninen, Y. Lu, K. Lundqvist, and L. Provenzano, "An ontological interpretation of hazard for safety-critical systems," Proceedings of ESREL'17, 2017.

[8] S. P. Smith and M. D. Harrison, "Measuring reuse in hazard analysis," Journal of Reliability Engineering & System Safety, vol. 89, no. 1, pp. 93–104, 2005.

[9] J. Guiochet, Q. A. D. Hoang, M. Kaaniche, and D. Powell, "Model-based safety analysis of human-robot interactions: The miras walking assistance robot," in Proceedings of ICORR'13, June 2013, pp. 1–7.

[10] G. Guizzardi, Ontological Foundations for Structural Conceptual Model,2005.

[11] 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.

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

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

[14] "MIL-STD-882, DOD standard practice for system safety, version D," 2000.

[15] T. Stålhane and G. Sindre, "A comparison of two approaches to safety analysis based on use cases," Proceedings of ER'07, pp. 423–437, 2007.

[16] J. Hwang and H. Jo, "Hazard identificaiton of railway signaling system using PHA and HAZOP methods," Journal of Automation and Power Engineering, vol. 2, no. 2, pp. 32–39, 2013.

[17] R. Wang, W. Zheng, C. Liang, and T. Tang, "An integrated hazard identification method based on the hierarchical colored Petri net," Safety Science, vol. 88, pp. 166–179, 2016.

[18] P. B. Ladkin, "Ontological hazard analysis of a communications bus," 2010.

[19] 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.