An Ontological Approach to Identify the Causes of Hazards for Safety-Critical Systems

Jiale Zhou, Kaj Hänninen, Kristina Lundqvist, Luciana Provenzano
Mälardalen University, Västerås, Sweden
e-mail: zhou.jiale@mdh.se

Abstract—**Preliminary hazard analysis (PHA) is a key safety-concerned technique, applied in early stages of safety critical systems development, aiming to provide stakeholders with a general understanding of potential hazards together with their causes. Various studies have asserted that most significant flaws in hazard analysis techniques are related to the omission of causes associated with the identified hazards. In addition, identified causes are sometimes described in too generic terms to provide useful guidance for subsequent activities. In this paper, we propose an approach to explore and identify the causes associated with the hazards from a PHA, aiming to improve the results of hazard causes identification in terms of completeness and usefulness. To achieve the goal, the proposed approach utilizes the hazard-related concepts and relations defined in a hazard domain ontology presented in our previous work [1]. Furthermore, an application scenario of a train control system is used to evaluate our approach.**

Keywords-causes analysis; preliminary hazard analysis; safety-critical systems; hazard ontology

I. INTRODUCTION

Preliminary hazard analysis (PHA) is a key safety-concerned technique, applied in early stages of the safety-critical systems (SCSs) development process, aiming to provide stakeholders, e.g., developers, organizations and authorities, with a general understanding of potential hazards as well as the causes associated with the hazards. When analysts conduct a PHA to discover potential hazards of a system, they typically start by using a list of common hazards together with the system descriptions as initial inputs [2]. The discovered hazards are then recorded in the form of natural language hazard descriptions in the PHA worksheet, and the causes of the recorded hazard descriptions are to be identified. The causes of the hazards identified in the PHA 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 causes identification. Various studies have asserted that the most significant flaws in hazard analysis techniques are typically related to the omission of possible causes associated with the identified hazards [3].

The main drawbacks of the current practice applied in the hazard causes identification, lie in that: 1) analysts are inclined to identify generic causes for a certain hazard description, for example, "*Design flaw, Coding error, and Human error*" can be listed as possible hazard causes, but this type of generic information is not particularly useful for guiding the safety requirements elicitation [4] and, 2) since the hazard causes identification highly relies on the experience possessed by the analysts and the lessons obtained from previous projects/systems, there is a need to formalize these experiences in a proper way which can be reused to identify a more complete set of hazard causes as well as to save effort [5] and, 3) due to the lack of precise definition on causal relations, the causes of a certain hazard description are typically identified in accordance to the intuition and experience of the analysts [2], with the risk of missing the rationale behind the identified causes and the corresponding hazard description.

Much effort has been devoted into exploring how hazard identification should be conducted in the early stages of SCSs development, e.g., HAZOP [6], EAST-ADL based PHA [7], STMP/STECA [4] [8], and model-based PHA [3]. These techniques mainly aim to discover more hazards that can lead to accidents. There is still a need to make up for the aforementioned deficiencies related with the identification of possible causes associated with the recorded hazard descriptions. In our earlier work [1], 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 domain. 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 causes identification. These considerations motivate us to formulate the following research question: Based on the recorded hazard descriptions in the PHA, is it possible to utilize the Hazard Ontology to improve the identification of possible causes associated with the hazards, to make the results of a PHA more complete and useful?

In this paper, our main contribution is to propose an approach, called OCH, to identify the causes associated with the hazard descriptions from a PHA worksheet. The OCH aims to improve the results of hazard causes identification in terms of completeness and usefulness by making up for the aforementioned deficiencies of current practices. To achieve this goal, the OCH utilizes the hazard-related concepts and relations defined in the HO. In general, after potential hazards have been documented in the PHA worksheet, the OCH selects a hazard description as initial input to identify causes. Then, the OCH proceeds until all the hazard descriptions are analyzed. To be specific, the causes identification consists of three main steps:

978-1-5386-3322-9/17/$31.00 ©2017 IEEE

- **OCH-Step 1:** Hazard Description Categorization categorizes the selected hazard description in accordance to the Hazard Ontology [1]. This step will help analysts achieve a common understanding of the hazard description.
- **OCH-Step 2:** Hazard Description Expansion: produces an expanded description for the categorized hazard description from Step 1 by correlating it with system descriptions, which provides an analysis basis for the causes exploration in Step 3.
- **OCH-Step 3:** Causes Exploration analyzes the expanded description by following a set of sub-steps, and explores the possible causes.

We utilize an application scenario of a train control system, which has been introduced in [9], to evaluate the OCH approach. The results obtained by the OCH have shown a promising potential that the original PHA results can be further improved, with respects to the hazard causes identification.

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 an application scenario 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 [1] is an ontological interpretation of the hazard concept. In order to interpret the hazard-related concepts in real-world semantics[1], the HO is explicitly grounded in a theoretically well-founded foundation ontology, i.e., the Unified Foundational Ontology (UFO) [10]. Compared 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. Fig. 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. An event, i.e., an instance of **Event**, is an entity where not all of its constituent parts are 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. Different from other foundational ontologies, UFO defines two concepts to categorize objects, 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-style 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 [8] [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 UFO 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 has the potential to encounter with 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

[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.

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 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.

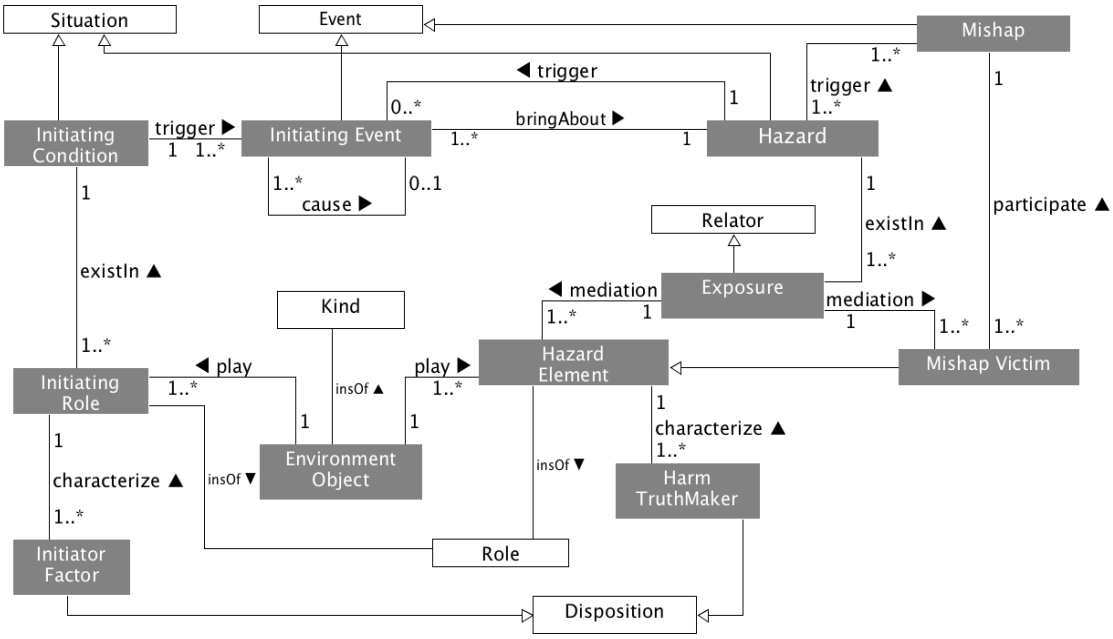

Figure 1. The UML class diagram of the Hazard Ontology. Concepts are represented as rectangles. The hazard-related concepts are colored in gray, and the foundational concepts are white. Typed relations are represented by lines with a reading direction pointed by "▶", from open end to aggregated end. 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 Identify the Causes of Hazards - OCH

In this section, we describe the Temporary Speed Restriction (TSR) scenario of the Chinese Train Control System level 3 (CTCS-3) [9] in Section III-A. Different types of hazard descriptions identified in [9] for the TSR application scenario will be used to illustrate our approach. Then, we introduce the ontological approach, called OCH, to identify the causes of hazards in detail, consisting of three steps: hazard description categorization in Section III-B, hazard description expansion in Section III-C and causes exploration in Section III-D.

A. Description of Application Scenario

CTCS-3 [9] is a radio-based train control system, which has two main subsystems: a ground subsystem and an on-board subsystem. The ground subsystem includes balises, track circuits, wireless communication network (GSM-R), and a Radio Block Centre (RBC). The on-board subsystem includes on-board devices and an on-board wireless module. If there is an emergency or track maintenance requirements, the train control system should be capable to set the temporary speed restriction (TSR) command to the specified track section. Both the on-board subsystem and train driver can have the authority to apply the brake.

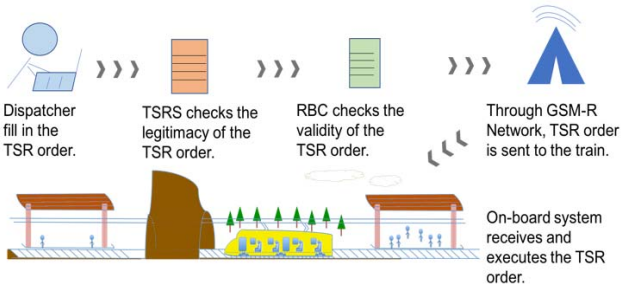

Figure 2. The TSR application scenario of CTCS-3 [9].

The process of issuing TSR command consists of four steps, as shown in Fig. 2: 1) Dispatcher should fill the TSR parameter and activate the TSR 30 minutes ahead of the scheduled time and, 2) The temporary speed restriction server (TSRS) verifies the legitimacy of the drafted TSR and sends the TSR to RBC and, 3) the RBC is responsible to verify the validity of this order by checking the track occupancy based on both of the information transferred in the track circuit and train position reports sent by the on-

board system via GSM-R and, 4) the RBC sends motion authority (MA) with the TSR to all CTCS- 3 trains in its precinct and the on-board systems calculate and plot the train running profiles according to MA with TSR, track descriptions received from balises, and the data of current speed and running distance sent by the speed distance unit (SDU).

B. OCH-Step 1: Hazard Description Categorization

This first step in the OCH approach is to assist analysts to achieve a common understanding of the selected hazard description (HD), which is considered important for safety analysis [1]. To perform the hazard description categorization, we propose a set of heuristic questions. We begin by selecting a hazard description from the original PHA results, and go through all the questions. Based on the answers, the selected HD will be categorized into four categories, in terms of **Hazard**, **Initiating Condition**, **Initiating Event**, and/or **Mishap** [1]. The heuristic questions are listed as follows:

- **Q1: "Is the hazard description describing a situation (state of affairs) or an event?".** Q1 shall be asked to determine if the hazard description is describing a hazard/initiating condition (if the answer is situation) or mishap/initiating event (if the answer is event), according to the HO. Note that 1) if a hazard description describes that some event is supposed to occur but does not, then the hazard description is regarded as a generic situation that will not trigger the specific event, such as "the brake command is not issued", and 2) if a hazard description describes a repetitive and continuous behavior, it can be regarded as a situation, such as "a train is running on the track".
- **Q2: "If the hazard description is describing a situation, can the situation trigger mishaps when some dispositions in the situation are manifested?".** Q2 shall be asked to determine if the hazard description is describing a hazard (if the answer is yes) or an initiating condition (if the answer is no), according to the HO.
- **Q3: "If the hazard description is describing an event, can the event bring about severe injuries of people or damages to the environment?".** Q3 shall be asked to determine if the hazard description is describing a mishap (if the answer is yes) or an initiating event (if the answer is no), according to the HO.

Take as an example the hazard description "SDU does not provide current speed and travel distance", 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, it is noticed that the described situation will not trigger any accident directly, when its dispositions are manifested. Thereby, HA-H1 will be categorized into **Initiating Condition**.

C. OCH-Step 2: Hazard Description Expansion

This step expands the categorized hazard description (CHD), taking both the expertise of analysts and the system description into consideration. The output of this step are UFO-style semi-formal models. The semi-formal models will not only formalize a portion of the system description related with the corresponding CHD from the natural language to the UFO-style models, but also express the expertise of analysts structurally to facilitate reuse. The expanded description will provide a paramount basis for the subsequent causes identification.

If the CHD is categorized into **Initiating Condition** or **Hazard**, the expansion steps are:

- **IC/HA-DE-Step 1:** Identify the constituent parts presented in the CHD, including *kind* objects, *role* objects, dispositions, and relators.
- **IC/HA-DE-Step 2:** For each *kind* object, identify all the roles it can play, considering the system description.
- **IC/HA-DE-Step 3:** For each *role* object, identify the relators that are existentially-dependent of this role and specify all the other roles based on the identified relators, considering the system description and the analysts' expertise.
- **IC/HA-DE-Step 4:** For each *role* object, identify all the *kind* objects that can play the role, considering the system description.
- **IC/HA-DE-Step 5:** For each *kind* object, if the *kind* object is a part of a super-system and has impacts on certain dispositions possessed by the super-system, then identify the roles the super-system can play when the dispositions are manifested, considering the system description. Moreover, the corresponding relators, roles and *kind* objects should be identified as well.

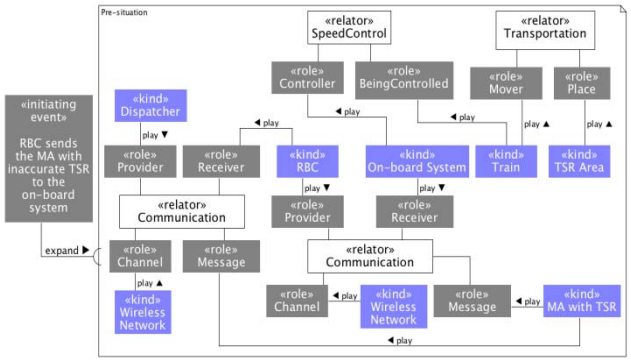

Figure 3. The expanded description for the HA-H1. *Kind* objects are colored in purple, *role* objects are colored in gray, and relators are white.

Continuing with the HA-H1 from the TSR scenario, i.e., "SDU does not provide current speed and travel distance", which is an initiating condition. We can identify SDU, and speed/distance message as *kind* objects. The SDU can play two roles "Sensor" and "Provider", due to the fact: 1) it monitors the train wheel to collect the speed and distance information and, 2) it provides the information to the on-

board system. The "Monitor" and "Control Parameter Communication" relators can be further identified. The "Monitor" relator will connect the "Sensor" and "BeingSensed" roles, played by SDU and the train wheel respectively. Meanwhile, based on the system description and analysts' expertise, all the other roles can be identified for the "Control Parameter Communication" relator, including "Receiver" played by "on-board system", "Communication Channel" played by "Wireless network", and "Message" played by "Speed/Distance Message". Since the train wheel and on-board system are components of the train, we need to consider the roles played by the train in the TSR scenario. When performing IC/HA-DE-Step 1 to IC/HA-DE- Step 5, we shall obtain the expansion description for the HA- H1, as shown in Fig. 3.

If the CHD is categorized into **Initiating Event** or **Mishap**, we will identify the pre-situation that are likely to trigger the event. The following steps can be taken to obtain the pre-situation:

- **IE/MS-DE-Step 1:** We begin by identifying the participants of the CHD, comprising *kind* objects and *role* objects.
- **IE/MS-DE-Step 2:** Based on the identified objects, we can go through from the IC/HA-DE-Step 2 to IC/HA-DE-Step 5 to expand the pre-situation.

To exemplify the approach, we consider another hazard description from the TSR scenario "RBC sends the MA with inaccurate TSR to the on-board system", labeled as HA-H2, which is an initiating event. We can identify RBC, MA, TSR, on-board system as *kind* objects. After going through from IC/HA-DE-Step 2 to IC/HA-DE-Step 6, we can obtain the expanded description for the HA-H2, as shown in Fig. 4.

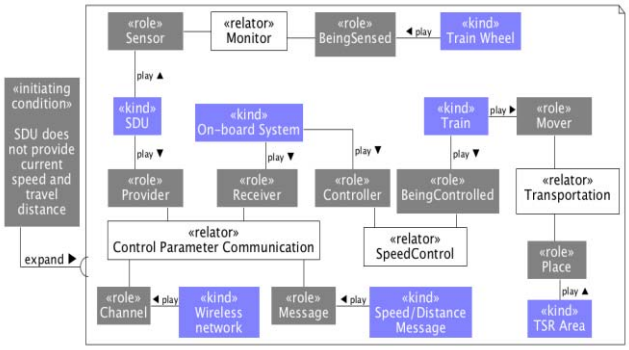

Figure 4. The expanded description for the HA-H2.

D. OCH-Step 3: Causes Exploration

The expanded description (ED) formalizes the portion of the system description related to the corresponding categorized hazard description (CHD), which provides an analysis basis for the identification of causes.

According to the UFO, a situation is brought about by events. So the causes exploration for a situation is about identifying the possible pre-events. If the CHD is an initiating condition or a hazard, the following steps can be taken to explore the pre-initiating event for the CHD:

- **IC/HA-CE-Step 1:** For each role in the ED, explore the possible dispositions that characterize this role. When such possible dispositions are manifested, the event triggered by the ED is the same as the event by the CHD. If the CHD is an initiating condition, the role is identified as **Initiating Role** and the dispositions as **Initiator Factor**. If the CHD is a hazard, the role is identified as **Hazard Element**, the dispositions as **Harm TruthMaker**, and the relators mediating hazard elements as **Exposure**.
- **IC/HA-CE-Step 2:** For each identified initiating role or hazard element, explore and identify the corresponding *kind* object that can play this role. Then, the pre-initiating event that makes the *kind* object play the role can be considered as a candidate for the causes of the hazard.
- **IC/HA-CE-Step 3:** For each initiator factor or harm truthmaker, explore the components of the corresponding *kind* object. Such components will enable the disposition of the *kind* object. Then, the pre-initiating event that impacts the components will be a candidate for the causes of the hazard.
- **IC/HA-CE-Step 4:** For each relator or exposure, the pre- initiating event that hampers or breaks the relator will be a candidate for the causes of the hazard.

Take the initiating condition HA-H1 as an example. Note that the HA-H1 describes a generic situation that will not trigger the "SDU provide current speed and travel distance" event, which means 1) the constituent parts of the HA-H1 can be different combinations of initiating roles, initiator factors, relators and environment objects and, 2) all these combinations must not trigger the event. Therefore, we first explore all the possible combinations, and then identify the possible pre-initiating events that can bring about the corresponding combination. The results are shown in Table I.

TABLE I. THE IDENTIFIED CAUSES OF THE HA-H1 THANT IS AN INITIATING CONDITION

Causes	Initiating Role	Initiator Factor	Environment Object	Relator	Pre-Initiating Event
Cause 1	Message	Inaccurate information	Speed/distance message		Certain objects tamper the speed/ distance message
Cause 2	Communication channel	Interference to message	Wireless network		EMI hampers the wireless transmission
Cause 3	Receiver	Abnormal message decoding	On-board wireless module		On-board decoding module malfunctions.
Cause 4	Provider	Abnormal message coding	SDU		SDU coding module malfunctions
Cause 5	Sensor	Abnormal monitoring	SDU		SDU sensor malfunctions
Cause 6	BeingSensed	Improper information source	Train wheel		Train wheel parameters change
Cause 7				Monitor	Monitoring algorithm doesn't work

According to the UFO, an event is a manifestation of certain dispositions. So the causes exploration for an event includes a search for the manifested disposition(s) that exist

in the pre- situation. Suppose that the CHD is an initiating event or a mishap, the following steps can be taken:

- **IE/MS-CE-Step 1:** For each role in the ED, explore the possible dispositions that characterize this role. When such possible dispositions are manifested, the CHD will be triggered. If the CHD is an initiating event, the role is identified as **Initiating Role** and the dispositions as **Initiator Factor**. If the CHD is a mishap, the role is identified as **Hazard Element**, the dispositions as **Harm TruthMaker**, and the relators mediating hazard elements as **Exposure**.
- **IE/MS-CE-Step 2:** For each initiating role or hazard element identified in IE/MS-CE-Step 1, explore the possible *kind* objects that can play this role. When such *kind* objects are characterized by the corresponding initiator factors or harm truthmakers, the CHD will be triggered. The *kind* objects will be identified as **Environment Object**.

Take the HA-H2 as an example, the possible causes are shown in Table II.

TABLE II. THE IDENTIFIED CAUSES OF THE HA-H2 THAT IS AN INITIATING EVENT.

Causes	Initiating Role	Initiator Factor	Env Object
Cause 1	Message	Inaccurate information	MA with TSR
Cause 2	Communication Channel	Interference to messages	Wireless network
Cause 3	Receiver	Abnormal message decoding	On-board system/RBC
Cause 4	Provider	Abnormal message coding	RBC/TSR Server
Cause 5	Producer	Negligence	Dispatcher

IV. EVALUATION

To evaluate our work, we applied the OCH approach on the Temporary Speed Restriction (TSR) application scenario. There were three reasons for us to choose the TSR application scenario for the purpose of evaluation:

- Several safety analysis techniques [9] [15] [16] had been applied on the TSR application scenario and,
- The potential hazards of the TSR application scenario were identified and published in [9] and we were able to directly use the hazard identification results to apply the OCH for hazard causes identification and,
- The causes of some potential hazards were also identified and published in [9], and therefore the results of applying the OCH for hazard causes identification could be compared with those identified in [9].

In [9], a total of 49 hazards were identified for the TSR application scenario, including 6 hazards related to socio-technical factors, 9 hazards involving human factors, and 34 technical factors. We went through all of the identified hazards. The OCH identified 244 causes associated with the 49 hazards in total. Since the causes of 6 potential hazards were identified in [9], we could make a limited comparison between our results and the results presented in [9], as shown in Fig. 5.

A. Comparison Analysis

The method in [9] identified 17 causes for the 6 selected hazards, in contrast our approach identified 32 causes for the same hazards. After a further analysis of the relation between the causes identified by either method, the hazard numbers in the parenthesis next to each cause identified in [9], as shown in Fig. 5, were highlighted to indicate the corresponding causes identified by the OCH.

Furthermore, some observations could be noticed:

- *Observation 1:* The causes identified by the OCH was a superset of those in [9], since each cause identified in [9] could find at least one corresponding cause by the OCH. The causes identified by the OCH, which could not find a counterpart in the causes identified in [9], were marked using red in Fig. 5. The new identified causes in red indeed provide a more detailed explanation of the ones identified in [9]. Such useful details can be available for engineers in subsequent development phases, such as during safety requirements elicitation.
- *Observation 2:* In some cases, the causes identified in [9] seemed to be more precise and detailed than the corresponding causes by the OCH. However, in our opinion, it was mainly because the causes identified in [9] were actually the causes of causes. For instance, the cause OCH1-3 "Balise loses without notice" corresponded to two causes C1-1 "Absence the interlocking mechanism of alarming when losing balise" and C1-2 "Miss balise in the way due to incorrect linkage info. among balise." in [9]. Nevertheless, C1-2 was more like the cause of C1-1 than the cause of "Train does not receive track data or any package from balise".
- *Observation 3:* In some cases, the causes identified in [9] corresponded to more than one cause by the OCH. The OCH could provide more details. For example, invalid train speed, invalid travel distance and invalid track descriptions were stated in the C2-1 that corresponded to two causes OCH2-2 and OCH2-3. The OCH2-2 and OCH2-3 explained how these invalid data were produced. The OCH2-2 emphasized that "On-board system receives invalid TSR or track data." and the OCH2-3 emphasized that "On-board system wrongly calculates train speed and/or travel distance."

Based on these observations, it could be concluded that our approach had a potential to discover better causes, in terms of completeness and usefulness, based on the same set of hazard descriptions.

B. Discussion

We discuss the validity of our evaluation, from the following two categories [17]. The first category is internal validity. The internal validity of our evaluation can be affected by the construction of UFO-style models. The OCH requires some personal experience and domain expertise to

establish the UFO-style models for the OCH. However, with the increase of experience, the OCH approach can reuse well-specified patterns to expand the hazard description, which to a large extend facilitates the identification process. For instance, the "communication" relator along with its corresponding roles is a well-specified pattern. Moreover, such patterns can make the process of causes identification standardized.

NO.	Hazard	Causes Identified by the OCH	Causes Identified in [9]
1	Train does not receive track data or any package from balise	**OCH1-1**. The data receiver of the on-board (OB) system malfunctions. **OCH1-2**. Communication interference between the balise and OB system causes package loss. **OCH1-3**. Balise loses without notice. **OCH1-4**. Balise transmission module malfunctions.	**C1-1.** Absence the interlocking mechanism of alarm when losing balise. (**OCH1-3**) **C1-2.** Miss balise in the way due to incorrect linkage info. among balise. (**OCH1-3**) **C1-3.** Software or hardware of balise transmission module failure. (**OCH1-4**)
2	OB system does not send brake command to EMU	**OCH2-1**. OB system transmission module malfunctions. **OCH2-2**. OB system receives invalid TSR or track data. **OCH2-3**. OB system wrongly calculates train speed and/or travel distance. **OCH2-4**. Line between the OB system and EMU is down. **OCH2-5**. The RBC fails to send TSR order.	**C2-1.** Invalid train speed and travel distance or invalid track descriptions. (**OCH2-2, OCH2-3**) **C2-2.** TSR is not received from RBC or TSR is wrong. (**OCH2-1, OCH2-2, OCH2-5**) **C2-3.** Dysfunction of vital computer of OB. (**OCH2-1**)
3	DMI does not display speed data and TSR info to driver	**OCH3-1**. DMI fails to receive the TSR and speed data. **OCH3-2**. DMI receives right data, but wrongly displays to driver. **OCH3-3**. DMI receives invalid data to display. **OCH3-4**. DMI decoder cannot recognize received data. **OCH3-5**. DMI can not notify the info to drivers in time. **OCH3-6**. The RBC fails to send TSR order. **OCH3-7**. SDU fails to send speed data.	**C3-1.** Invalid train speed and travel distance or invalid track descriptions. (**OCH3-1, OCH3-3**) **C3-2.** TSR is not received from RBC or TSR is wrong. (**OCH3-1, OCH3-3, OCH3-4, OCH3-6**) **C3-3.** Dysfunction of encoding and decoding. (**OCH3-3**)
4	Driver does not send brake command	**OCH4-1**. DMI fails to display correct info **OCH4-2**. DMI does not receive correct info. **OCH4-3**. The TSR and speed data info is not obviously displayed by the DMI. **OCH4-4**. Poor personal status of Driver. **OCH4-5**. Driver is interfered or distracted by external factors **OCH4-6**. Driver does not realize the emergency.	**C4-1.** The speed displayed on DMI is lower than the actual speed due to wrong speed calculation or DMI decoding error. (**OCH4-1**) **C4-2.** SDU delivers the wrong train speed and travel distance. (**OCH4-2**) **C4-3.** Driver has poor personal status and makes negligent errors. (**OCH4-4**)
5	EMU brake does not be activated	**OCH5-1**. Both the OB system and driver do not send brake command **OCH5-2**. EMU failure **OCH5-3**. Brake mechanism failure	**C5-1.** Both OB and driver do not send brake command. (**OCH5-1**) **C5-2.** Air brake failure. (**OCH5-3**)
6	SDU does not provide current speed and travel distance	**OCH6-1**. Certain objects tamper the speed/ distance message. **OCH6-2**. EMI hampers the wireless transmission channel. **OCH6-3**. On-board decoding module malfunctions. **OCH6-4**. SDU coding module malfunctions. **OCH6-5**. SDU sensor malfunctions. **OCH6-6**. Train wheel parameters change without notice. **OCH6-7**. Monitoring algorithm doesn't work.	**C6-1.** Wheel diameter is unknown due to negligence of maintainer or flaw in scheme of running test. (**OCH6-6**) **C6-2.** Communication channel Blocked or dysfunction of encoding and decoding. (**OCH6-2, OCH6-3, OCH6-4**) **C6-3.** Laser and radar velocity sensor failure or logic confusion in 2 out of 3 structure. (**OCH6-5, OCH6-7**)

Figure 5. Result of contrasting the OCH with the method in [9] for a part of the identified hazards. The numbers in the parenthesis next to each cause identified in [9] indicated the corresponding causes identified by the OCH. The causes identified by the OCH, which could not find a counterpart in the causes identified in [9], were marked using red.

The second category is external validity, related to the extent to which we can generalize the study results. In this work, we chose the TSR application scenario of the CTCS- 3 system to evaluate our approach. The OCH was evaluated based on the 49 hazards identified in [9]. Moreover, a limited comparison between the causes presented in [9] and those identified by the OCH was conducted. It could be observed that the OCH approach could identify better causes in terms of completeness and usefulness. Although the evaluation was conducted in a limited way, which might threaten the validity of the observations, it can still be concluded that the results of our approach are promising. Furthermore, to mitigate this threat, we are currently evaluating the OCH approach on a more complex system consisting of autonomous vehicles.

V. Related Work

A number of different hazard analysis techniques have been proposed over the past years, and they are currently widely used by safety-critical industries [18]. There are

different examples of their use in complex systems. There are also examples of adaptations of standard hazard analysis techniques for identifying hazards [7], [19].

Despite the wide use of the standard hazard analysis techniques, new techniques emerge promisingly. For example, Leveson describes a new approach to hazard analysis, STPA (System-Theoretic Process Analysis) [8], which has been particularly applied for the analysis of hazards and their causes in today's complex socio-technical systems [9]. Another example is the Ontological Hazard Analysis (OHA) [20] 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 the causes of hazards, which inherently accords with the way in which people explore the reality.

Daramola, Stålhane, Sindre, and Omoronyia [21] present a framework and tool proto- type 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. Vargas and Bloomfield [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, to discover potential hazards. Our approach aims to discover hazard causes based on identified hazards, and during this process, more hazards could be identified as well.

VI. Conclusion and Future Work

In this paper, we have proposed an ontological approach to identify the causes of hazard (OCH), based on results from preliminary hazard analysis (PHA) technique. The main idea of our approach is to use the Hazard Ontology (HO) [1] to provide a consistent way to formalize the system descriptions and analysts' expertise of hazards. The formalized models can provide a basis for the identification of the causes associated with identified hazards.

The approach consists of three steps, in terms of "Hazard Descriptions Categorization" to achieve a common understanding of the selected hazard description, "Hazard Description Expansion" to formalize the knowledge of the system and analysts, and "Causes Exploration" to explore the possible causes according to the casual relations defined in the HO. A set of practical questions and sub-steps are proposed to provide guidance for ontological modelling and analysis. Therefore, the approach does not require much knowledge on theoretical foundations of ontology.

Our approach was evaluated using the TSR application scenario of the CTCS-3 system. Meanwhile, we performed a limited comparison between the causes identified by the OCH and those presented in [9]. The comparison results showed a promising potential of our approach. We are currently evaluating the proposed approach to identify causes of hazards on a more complex system consisting of autonomous vehicles, and a more conclusive evaluation of the benefits of the OCH approach will be provided to convince the safety practitioners. Such evaluation requires a separate paper to make good sense.

The causes identification can provide a heuristic and negotiation basis for safety requirements elicitation. As future work, we plan to propose a requirement elicitation approach based on the identified hazard causes, 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. We are developing a toolset to facilitate the UFO-style model construction and hazard causes identification.

Acknowledgment

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

References

[1] 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.

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

[5] 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.

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

[7] 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.

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

[9] 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.

[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] X. Yao, K. Li, D. Zhou, X. Mo, and Y. Yao, "Application of UML Sequence Diagram in CTCS-3 On-board System Hazard Identification," in *Proceedings of ICIRT'13*, Aug 2013, pp. 169–173.

[16] K. Li, X. Yao, D. Chen, L. Yuan, and D. Zhou, "HAZOP Study on the CTCS-3 On-board System," *Journal of IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 1, pp. 162–171, 2015.

[17] B.Kitchenham,L.Pickard,andS.L.Pfleeger,"Case studies for method and tool evaluation," *Journal of IEEE Software*, vol. 12, no. 4, pp. 52–62, Jul. 1995.

[18] 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.

[19] 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.

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

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