Role-based Approach as Support for Safety Analysis of Collaborative Systems

1st Luciana Provenzano, 2nd Kaj Hänninen, 3rd Kristina Lundqvist
School of Innovation, Design and Engineering
Mälardalen University
Västerås, Sweden
{luciana.provenzano, kaj.hanninen, kristina.lundqvist}@mdh.se

***Abstract*—Modern collaborative and dynamic systems, such as System of Systems (SoS), can be considered as a set of interacting entities where the interactions are seen as the core activity for these systems. The study of interactions is of importance in order to discover emergent and interdependent properties that impact the overall system's behaviour. We introduce a role-based approach together with a taxonomy of roles for safety as a means to deal with emergent behaviours of high-collaborative systems that may impact the safety of the whole system. The aim of our role-based approach is to discover the interactions that may be harmful for the system and use them as starting point for common safety analysis techniques.**

***Keywords*—role; role-based approach; hazard; hazard identification; safety analysis; complex system; collaborative system; System of Systems (SoS); emergence; interdependence; safety requirements elicitation**

I. Introduction

There exist a large number of different analysis techniques to perform safety analysis to identify potential system's failures, causes and consequences. Each analysis technique requires, to different extent, a knowledge of the system from different perspectives. Many of the techniques currently used in safety analysis derive the expected behaviour of a system from the system's description [1]. System descriptions often include the main functions the system is supposed to provide and their high-level design. Functions mostly define the expected system's behaviours, that is 'what the system shall do' to fulfil the users' and stakeholders' expectations. The system description does generally not define what the system shall not do. Also, functional descriptions are not always supported by architectural models which clearly describe the relations between the system's functions and the system's components that realize them. Besides, the behaviours of high-collaborative systems, that is systems where interactions are seen as the core activity, cannot be described only as the sum of the individual functions of their constituent systems [2] since interactions among the different systems create emergent behaviours that form the behaviour of the system as a whole.

As a result, the description of the system through its functions, that is a widespread and well-established approach in system and software engineering, may present some limitations for safety analysis. Indeed, it may limit safety analysts to search for system's hazards as exceptions to the described system's behaviours (the functions). This results in not looking for unplanned situations or unwanted events that may cause the system to respond in a harmful way. Moreover, missing the description of unwanted system's behaviours usually result in additional effort to find hazards since unwanted behaviours are most likely to bring about, sooner or later, dangerous situations. Finally, missing relations between functions and components make it difficult to identify the interactions that alter the normal system's behaviour or generate new behaviours that may end-up in a hazard. This is particularly important for collaborative and dynamic systems, in which the interactions among entities often create emergent behaviours that can be harmful to the system [3].

We propose the use of the *role concept* as a complementary technique to deal with the safety of modern collaborative systems that are characterized by complex interactions which stem from the collaboration of the system or its components with other systems or components [4], [5]. Roles have been widely used in different domains in order to deal with interactions, as explained in II. Specifically, we adapt the role concept for safety by defining a *taxonomy of roles for safety*, and we propose a *role-based approach* which leverages the roles for safety to obtain a more complete set of system's functions and a more detailed description of them in terms of interactions among the system's entities. This enhances the system's description in input to subsequent safety analysis especially regarding interactions. The paper is structured as follows: in section II, the motivations for the introduction of the role concept to support safety analysis are explained; in sections III and IV, the taxonomy of roles for safety and the role-based approach as well as an example of its application are described; in section V, the related works are reviewed. Conclusions are drawn in section VI.

II. Background

We argue that role-based thinking should be adopted in dealing with safety of high-collaborative systems. Our assumption, which forms the main reason behind this statement, is that a hazard can happen due to the interactions of entities in the safety-critical system and/or its operational and natural environments in different situations, as proposed in [6].

Roles are widely used in different domains, that range from computer science where multi-agent systems (such as in [7], [8]) and modelling of business processes (such as in [9]) are

possible examples, to sociology [10], to deal with interactions. Roles are connected to the notion of behaviour. In Role Theory a role is '*those behaviours characteristic of one or more persons in a context*' [10]. In [9], a role is defined as '*the observable behaviour of a business object defined in a specific collaboration context*' and in [11] a role '*captures [..] the collaborative behaviour of objects*'. Behaviours refer to the dynamic aspect of an entity that interacts with another entity in a given context. Roles therefore model the collaboration among entities according to Biddle's notion of '*behavioural presence*', that is '*roles occur in the presence of others*' and '*are directed towards others*' [10]. By modelling interactions through roles, it is possible to change the entity's behaviour depending on the situation (context) without changing its nature (its static properties). Also, roles are *patterned* since they describe behaviours that are '*understood and accepted scripts*' [12] by all the interacting entities. So, each role is related to a '*characteristic behaviour*' [10]. This makes the roles *predictable* [10] in terms of the behaviour they manifest in a given interaction. This also means that roles are related to the notion of '*expectations for behaviour*' [12], i.e. the behaviour that an entity expects to get from the entity it is interacting with. The concept of role is shown in 'Fig. 1'.

To adapt the role concept for safety, we borrow from the Role Theory [10] the notions explained above, i.e. 1) *behavioural presence*, 2) *expectations for behaviour*, 3) *role as characteristic behaviours* and 4) *role as patterned behaviours*, to build upon the roles for safety. These concepts allow to identify and model the interactions among the safety-critical system's entities and the environment that may cause a hazard to happen. In particular, the *behavioural presence* allows to define the interactions among entities based on the *dependence property* [10], [13] that forces to identify a role in terms of the role upon which the behaving role acts. This enables to discover behaviours that are not directed towards a role, which means being able to discover that some entities do not play the role needed to interact correctly as it should be according to the notions of '*role as patterned behaviours*' and '*role as characteristic behaviours*'. This knowledge is fundamental to identify wrong system's behaviours due to missing interactions among entities that may lead to a hazard. Moreover, the *expectations for behaviour* [12] makes it possible to reason about how an interaction can fail because the expectation for a given behaviour (the *patterned behaviour*) associated with an entity's role is no longer maintained, and how this 'failed' expectation may impact the overall system's behaviour. So, the *expectations for behaviour* represents the key concept of the application of roles for safety because it tacitly implies that there may exist an *unexpected* behaviour for the same role. In particular, Biddle [12] observes that social actors do not always behave according to the expectations, especially in emergency situations. This implies that there may be a difference between the role expectation and the *role enactment* in particular situations or due to specific events. As a result, reasoning through the *expectations for behaviour* enables to search for unwanted or unexpected interactions that may be harmful to the system, as also pointed out in [8].

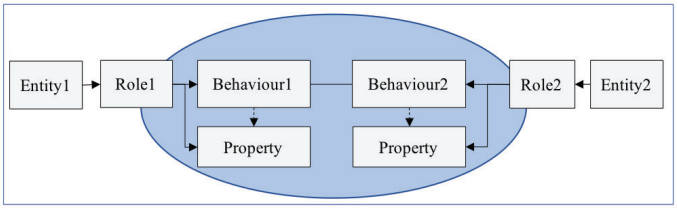

Fig. 1. Exemplification of the concept of role. The oval represents the interaction that results from the manifestation of behaviours. Each behaviour in the interaction belongs to a specific role. Also, the manifestation of behaviours depends on the role's properties, as shown by the dotted arrows that connect behaviour to property in the figure.

III. Taxonomy of Roles for Safety

There exist many definitions of role in literature. We define the ***role for safety*** as '*one or more possible observable behaviours of an abstract or concrete entity in the safety-critical system and its environment that exist and manifest when the entity interacts with other entities*'. This definition is based on the following two definitions of role:

- role as '*behaviours that are characteristic of a person within a context*' [10]
- role as '*the observable behavioural of a business object defined in a specific collaboration context*' [9]

The role for safety, as we define it, obeys the main properties of roles i.e. anti-rigidity [14] and dependence [13]. Also, it has behaviours that can manifest if some properties are verified [6]. The role for safety is therefore aligned with the role exemplified in 'Fig. 1'.

In the following subsections, we provide the definition of the roles to be used in reasoning about safety. These definitions are founded on four main concepts of the Role Theory [10], i.e. '*behavioural presence*', '*role as characteristic behaviours*', '*role as patterned behaviours*' and '*expectations for behaviour*', as explained in II. We also classify the roles for safety in four categories according to how they are identified (*identification*), how they are characterized (*characterization*), where they are described (*description*), how they contribute to safety (*safety*). These roles compose the taxonomy of roles for safety, as summarized in 'Fig. 2'.

A. Identification of Roles for Safety

Based on the notion of '*behavioural presence*' [10], we define

- ***Behaving role***, that is '*the role that exhibits the behaviour*'.
- ***Counter role***, that is '*the role upon which the behaviour of the behaving role impinges*'.

B. Characterization of Roles for Safety

Based on the notion of '*role as characteristic behaviours*' in [10], we define

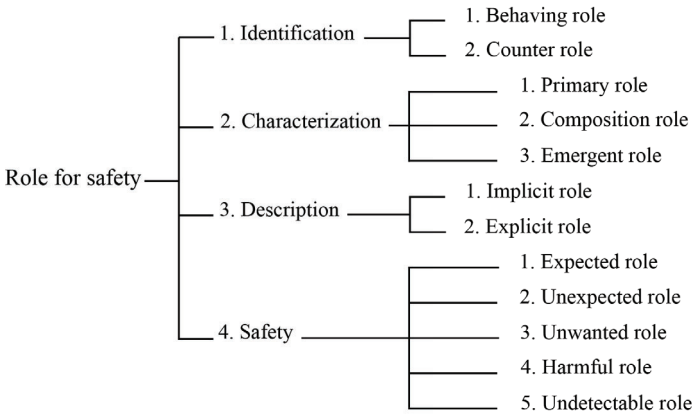

Fig. 2. The proposed taxonomy of roles for safety.

- ***Primary role***, that is '*the role that is associated with the characteristic behaviours of an entity*'.
- ***Composition role***, that is '*one of the possible roles which the primary role can be divided into*'.
- ***Emergent role***, that is '*the new role that arises from the interaction of two or more existing entities' roles*'.

C. Description of Roles for Safety

Based on the notion of '*role as patterned behaviour*' in [12], we define

- ***Explicit role***, that is '*the role that is associated with a behaviour that is described in or can be extracted from the system's description*'.
- ***Implicit role***, that is '*the role that exists for an entity but it is not explicitly defined in the system's description since it is the obvious role that the entity must play*'.

D. Safety Roles

Based on the notion of '*expectations for behaviour*' in [12], we define

- ***Expected role***, that is '*the role that is defined and agreed for a given entity interacting with another entity*'.
- ***Unexpected role***, that is '*the role that is not defined in a given interaction but it is played anyway*'.
- ***Unwanted role***, that is '*the role the entity must not play in a given interaction*'.
- ***Harmful role***, that is '*the role that alters a system's function in such a way that the resulting behaviour causes a hazardous situation*'.
- ***Undetectable role***, that is '*all roles that cannot be foreseen*'.

E. Insights into the Roles for Safety

The *emergent role* is the additional role that is or should be played by one or more entities involved in the interaction and/or by other entities within the system. The *emergent role* participates therefore to the creation of a new system's behaviour. The *emergent role* has been introduced to explicitly address the emergent properties that stem from the interactions of components in complex systems. An *emergent role* as well as *implicit* and *explicit* roles may be both *primary* and *composition* roles. The *harmful role* can be any of the above-mentioned roles.

IV. The Role-based Approach for Safety

Our goal is to identify interactions among entities to deal with the emergent behaviours of high-collaborative systems that may impact the safety of the whole system. From this perspective, the final aim is not to identify all situations in which the system works properly but to identify situations in which the system's behaviour is violated, as pointed out in [15]. The role taxonomy, as defined in the previous section (III), suggests how to apply the role concept to search for interactions. We therefore define the role-based approach for safety based on the taxonomy of roles for safety.

The role-based approach consists of two main activities: defining interactions for the safety-critical system (Activity A) and searching for harmful interactions (Activity B). In activity A, dependencies among entities in the safety-critical system and its environment are identified by abstracting the system's description into roles and by combining roles into interactions (see 'Fig. 3'). In activity B, the interactions resulting from the previous activity are used as basis to reason about how incorrect or unwanted behaviours while playing a given role may lead to harmful interactions (see 'Fig. 4').

A. Activity A: Defining Interactions for the Safety-critical System

This activity consists of four steps that are supported by the role taxonomy as follows:

1) *Identifying roles (Step A.1 in 'Fig. 3')*: from the system's description [1] and by applying the concepts of *implicit role* and *explicit role* along with *primary role* and *composition role*, one can identify the main roles that are played or should be played by the entities in the system and in its environment.
2) *Identifying behaving-counter interactions among roles (Step A.2 in 'Fig. 3')*: by applying the concept of *behaving role* and *counter role* to each role previously identified, it is possible to obtain a set of interactions among these roles, that are called *behaving-counter interactions*.
3) *Searching for emergent behaviours (Step A.3 in 'Fig. 3')*: by combining roles that are not connected through a behaving-counter interaction and/or roles that interact with each other indirectly (i.e. through other roles), it may be possible to discover new interactions by figuring out in which way one role affects the other. This may also lead to discover emergent behaviours of the safety-critical system, especially when one combines roles unlikely to interact. As a consequence, some *emergent roles* need to be defined so to make the roles in the specific interaction interact correctly.

[1]The system's description may include functions, requirements, high-level architecture, design, technical documents, and so on.

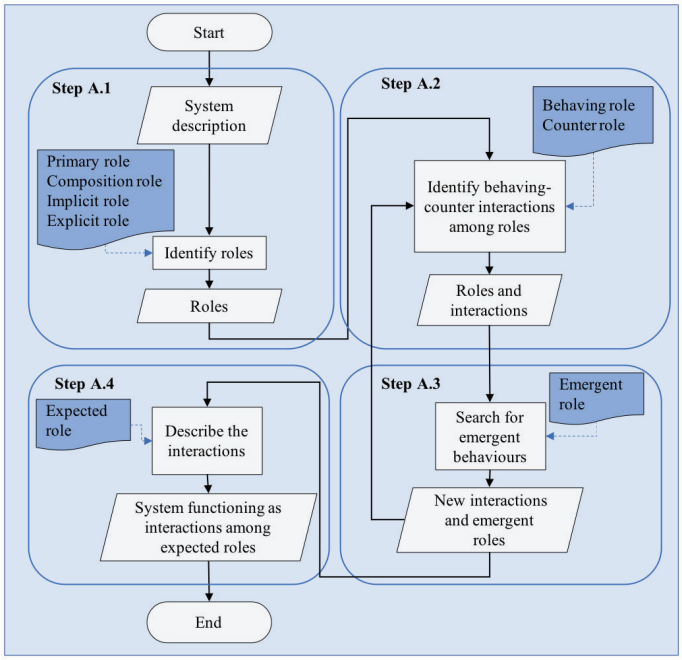

Fig. 3. Activity A: Defining interactions for the safety-critical system. Notice that the document shapes connected to each activity highlight the roles from the taxonomy of roles for safety that are used to perform that activity.

4) *Describing the interactions (Step A.4 in 'Fig. 3')*: for each role in each interaction, one can describe what is the *expected behaviour* for that role and the properties that allow to play that specific role in the interaction. Note that these roles are the *expected roles*, i.e. the roles that are expected to be played by the entities involved in each interaction, as defined in the taxonomy of roles for safety.

B. Activity B: Searching for Harmful Interactions

This activity is carried out in two steps and is supported by the *safety roles* in the role taxonomy as explained as follows.

1) *Seeking unwanted and unexpected roles (Step B.1 in 'Fig. 4')*: for each interaction, one can identify the possible *unwanted role/s* and *unexpected role/s* that could be played in that specific interaction, based on the description of the interaction from step A.4.
2) *Identifying harmful roles (Step B.2 in 'Fig. 4')*: for each interaction, the *unwanted roles* and the *unexpected roles* identified in the previous step (step B.1) are combined with *expected roles* in the same interaction and with roles in other interactions, and the resulting interactions are studied to identify the *harmful roles*.

It is worth noting that step B.2 shall be performed by safety analysts during risk assessment since decisions about whether 'a behaviour alters a system's function and causes hazards' belong to the risk assessment activities. However, we propose this step as the last step of the role-based approach to provide analysts with a possible way to use the information gathered in the previous steps, especially the information about *unwanted roles* and *unexpected roles*, as a basis for safety analysis. Notice that the role-based approach describes a highly iterative process to cope with the fact that roles change with respect to situations and over time.

C. Outcomes of the Role-based Approach

The role-based approach produces two main outcomes:

- The description of the functions of the safety-critical system through interactions among expected roles (as output of the Activity A). By performing the steps in Activity A it is possible to discover new behaviours, especially when searching for emergent behaviours (Step A.3). This implies that studying interactions contributes to widen the knowledge of the safety-critical system's functions. Moreover, by describing interactions one can figure out situations in which interactions happen and why they happen. This information is valuable to reflect upon what can prevent an interaction from taking place.
- The list of the identified *unexpected roles* and *unwanted roles* along with the description of the interactions in which they participate (as output of the Activity B). This forms the knowledge to understand whether an interaction is harmful for the system or not and, as such, an input for safety analysis.

D. Insights into the Role-based Approach

We suggest some insights based on our experience as guidance to apply the role-based approach:

- Each role must be part of at least a *behaving-counter interaction* to guarantee that the role can be played out. This is necessary to ensure the application of the *dependence property* of roles [13]. This also means that when checking the *dependence property* for the existing roles, it is possible to discover new roles that are needed

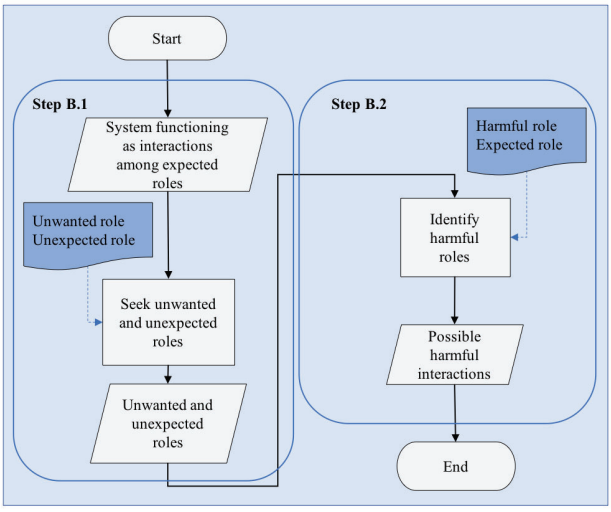

Fig. 4. Activity B: Searching for harmful interactions. Notice that the document shapes connected to each activity highlight the roles from the taxonomy of roles for safety that are used to perform that activity.

for a given interaction to take place. This reasoning also applies for new *emergent roles* (refer to step A.3).

- To search for *unwanted roles* one should consider the interaction and think to which roles can hamper it; while to identify the *unexpected roles* one should examine the properties that make the role becomes another role or cease its existence. This implies to think about how one of the *expected roles* in the interaction could not behave as expected, and why it happens.
- An interaction can be thought as a mutual agreement among the roles taking part in the interaction, that binds the roles to behave in a certain way. Behaviours and properties describe the interaction among the corresponding roles since they encode the reasons why the interaction exists. A short story telling can therefore be written based on properties and behaviours to describe an interaction.

E. An Example of the Role-based Approach

To exemplify the role-based approach, we consider a parking brake function implemented in a high-speed train to mitigate the collision hazard. The parking brake prevents the train from rolling away when at standstill and colliding with persons or objects in the surrounding environment. The example we propose considers the parking brake lamp, that is one of the risk mitigation at software level for the collision hazard, as described in the following system's description: '*The parking brake (PB) is manually activated by the train driver through a PB push button. When pressing the PB push button, the parking brake is applied if previously released, and released if previously applied. The PB status (i.e. applied or released) is shown by the PB lamp installed on the PB push button. The PB lamp is controlled by the Train Control System (TCS)*'. Note that the example is meant to show one of the possible ways of using the role-based approach and it has intentionally been kept simple to serve this purpose.

By performing the four steps in Activity A, we obtain the roles depicted in 'Fig. 5' represented as a UML-like class diagram [16]. The roles `PB Status Indicator`, `PB Status Controller`, and `PB Changer` can be considered as *explicit roles* since they can be obtained by the system's description from the behaviours of the PB lamp, the TCS, and the PB push button respectively. The role `PB Status Supervisor` could be thought as an *implicit role* since it is obvious from the system's description that there must be an entity that supervises the PB status to be able to display it. Also, all these roles can be considered as *primary roles* while the roles `PB Status Receiver`, `PB Status Sender` and `PB Status Checker` are possible *composition roles* for the role `PB Status Controller`. Note that the role `PB Status Supervisor` could also be thought as an *emergent role* that arises from the interaction between the roles `PB Status Controller` and `PB Changer`. Concerning the *behaving role* and the *counter role* (represented with *b* and *c* respectively in 'Fig. 5'), the `PB Status Controller` is the *behaving role* in the interaction with the `PB Status Indicator` based on the reasoning that if a controller

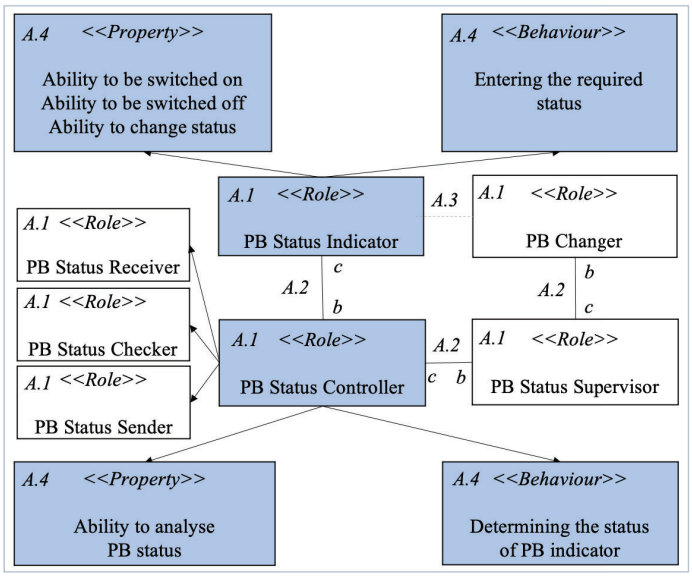

Fig. 5. Activity A: Roles and interactions for the parking brake function. Notice that the roles and interactions are labelled (*A.1*, *A.2*, *A.3* and *A.4*) to indicate in which step of Activity A they have been obtained in this specific example. Also, interactions (labelled with *A.4*) have been described only for the roles in the colored rectangles to keep the example simple.

determines the status of the PB then an indicator must show it. The same reasoning can be applied to justify the *behaving role* and the *counter role* in the other interactions in 'Fig. 5'.

By analysing the interaction between the roles `PB Status Indicator` and `PB Status Controller` in 'Fig. 5' through the steps in Activity B, we obtain the *unwanted role* and *unexpected role* as shown in 'Fig. 6', 'Fig. 7' and 'Fig. 8' respectively. Note that the *unwanted role* `Out of order Indicator` in 'Fig. 6' and the *unexpected role* `PB Status Indicator` in 'Fig. 7' have the same property and behaviour. However, we apply a different reasoning to obtain them. The `Out of order Indicator` is the role planned to not be part of the interaction (because it destroys it). So, we search for the properties and the behaviours that shall not happen. The `PB Status Indicator` is the role that must be played in the interaction (because it is needed). So, we search for the properties that can alter its (expected) behaviour. The interactions in which at least one of the participating roles is an *unwanted role* or an *unexpected role* are the most likely to result in *harmful* interactions. For example, the interaction in 'Fig. 7' in which the `PB Status Indicator` is the *unexpected*

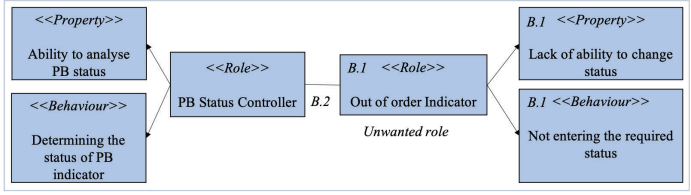

Fig. 6. Activity B: The `Out of order Indicator` as a possible *unwanted role* for the interaction considered in this specific example.

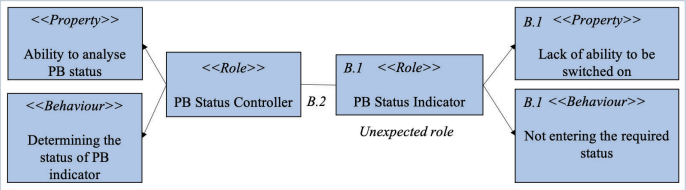

Fig. 7. Activity B: The `PB Status Indicator` as a possible *unexpected role* for the interaction considered in this specific example.

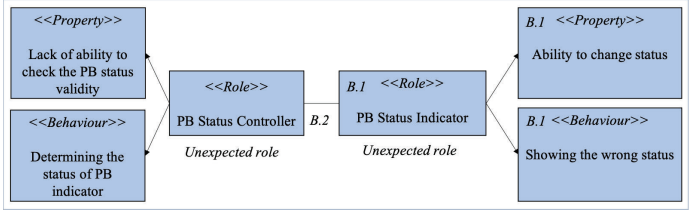

Fig. 8. Activity B: The `PB Status Indicator` and `PB Status Controller` as possible *unexpected roles* for the interaction considered in this specific example.

role, is harmful because the `PB Status Indicator` is not entering the new status 'switched on', as ordered by the `PB Status Controller`, because of a lack of the ability to switched on. So, the role `PB Status Indicator` is a *harmful role* in this interaction. This means that the actual status of the parking brake shown by the lamp is not correct, which may result in a dangerous action by the train driver (i.e. the unintended release of the parking brake).

V. Related Work

A. Preparing the System for Safety Analysis

There exist a number of methods that can be used to prepare information that is later used in safety analysis. In the following, we briefly describe a few of them. The Functional Resonance Analysis Method (FRAM) [17] may be used to analyze activities and creating models (of key functions) that can be used in risk analysis. The role-based approach is similar to FRAM in the sense that relations between activities are established based on dependencies. FRAM is however more focused on discovering emergent behaviours rather than emergent roles. The AcciMap approach [18] and the System Theoretic Accident Model and Processes (STAMP) [19] can be applied on systems to investigate contributing factors of accidents and for systems design. They both utilize control structure diagrams to show information exchanged between hierarchies of actors/entities. The role-based approach is related to both AcciMap and STAMP in the sense that the role-based approach considers relationships between entities. The role-based approach is, however, not focused on causal analysis or dependent on hierarchical control diagrams, but rather on abstracting and enriching information at an early stage of the development. This means that the role-based approach can be used to complement the information in control diagrams for both AcciMap and STAMP.

B. The Role Concept for Dealing with Interactions

The role concept is studied in several domains, such as linguistics, cognitive semantics, philosophy, computer science. In sociology, the role concept is fully treated by Biddle in Role Theory [10] in which it is used to analyze various forms of social systems by focusing on persons and their behaviours. The main idea is that people perform everyday activities by acting in a role (e.g. manager, teacher) that is predictable and has '*effects or functions within the social systems*' [10], i.e. the action of a role is always directed towards another role.

In software engineering, roles have been widely used mainly to achieve the *separation of concerns*, i.e. to separate the dynamic aspect of objects (their behaviours) involved in an interaction from their static properties in order to manage changing domains, as proposed for instance in [9].

The above cited works show that the role concept is strictly connected to interactions and dynamic behaviours. Our work uses the role concept proposed in these works to support safety analysis of complex systems, being this type of systems characterized by complex interactions that may end-up in emergent functions, as explained for instance in [20].

C. Theoretical Foundations of the Role

In computer science, the role concept has been studied in many areas, such as knowledge representation, conceptual modelling and object oriented modelling, as summarized in [21]. Here, the main focus is the nature of the role and the way of representing it in modelling and programming languages, such as in [11], [22]. So, these studies build the theoretical foundation of the role concept that provides the definitions and the properties necessary to implement it.

Despite the fact that roles are used in various domains of computer science, there does not exist a unique definition of role. In literature the focus is rather on what characterizes a role and how one makes use of it. From this perspective, it is clearly agreed that roles are used to '*capture both context-dependent and collaborative behaviour of objects*' [11]. It is also agreed that the two main properties of a role are: the lack of semantic rigidity, also called *anti-rigidity* [14], and the *dependence* [13]. The anti-rigidity denotes that a role can cease to hold for the object it is associated with without ceasing the object to exist. The dependence relates to the property of being '*founded in terms of relationships with other things in a given context*' [9]. In other words, the anti-rigidity concerns '*the ability of roles to be played*' [11] and the dependence '*characterizes the need of roles to be defined as part of a context*' [11]. The taxonomy of roles for safety proposed in this paper, is grounded in the Role Theory [10] and the role properties in [13], [14]. So, the taxonomy builds upon the theoretical basis from these works new roles for the purpose to deal with safety-critical systems.

D. The Role Concept to Infer and Explain Functions

Roles have also been introduced in robotics to improve the robot's capability to understand human behaviour. In [23], the authors propose a method called *Object Functional Role*

Perspective Method that uses the roles played by the different objects in the human being's environment, to interpret why the human is performing a given action (the intention) and how the human thinks to perform it. Entities in the safety-critical system interact with other entities in the system or in its environment. So, through the entities' roles one can understand how and why the system's behaviours occur, as it is done in this work for humans.

Another application of roles is the *object-role* in data modelling, where roles are used to gain a better understanding of the application area and modelling it in a less ambiguous and clearer way [24]. Specifically, objects and roles in the Object-Role Modelling enable to reason on '*whether there are any relationships which are of interest but which have been omitted so far*' [24]. This means that by connecting roles, it is possible to discover interactions that may generate functions that are fundamental for the system but unspecified for some reasons.

The role-based approach focuses on the interactions among roles to discover new system's functions and new hazardous scenarios. This is in-line with the idea of using roles to discover functions or infer human behaviours, as in [23], [24]. However, the role-based approach for safety aims at discovering 'what the system shall not do' and establishing explicit dependencies among the system's entities to manage the safety of complex systems.

VI. Conclusion and Future Work

This paper introduces a role-based approach together with a taxonomy of roles for safety. The approach describes a structured sequence of steps to extract roles and interactions among roles from the system's description, and use them to discover the interactions that may be harmful for the system. Roles contribute to improve the system's description by emphasizing the interactions among the system's entities. This is particularly important when dealing with complex and dynamic systems, in which the growing size of the interactions among components often cause emergent behaviours that can be harmful for the system. The result of the role-based approach is therefore used as a basis for subsequent safety analysis, using a suitable analysis technique, and as a support for addressing safety in the system architecture.

A future improvement of the proposed approach is the definition of a 'role diagram' that implements the taxonomy of roles for safety and a tool, based on the role diagram, that supports the application of the role-based approach. The purpose is to facilitate the use of the role-based approach by, among other things, automating the storage of roles and interactions among roles that result from this method, the retrieval of the needed information, the creation of 'patterns of reasoning' to be suggested to analysts. This will enable to apply and test the role-based approach in an industrial case study. This will also help to achieve the scalability of the approach. Finally, the information stored in the role diagram can be used as basis for the elicitation of the safety requirements.

Acknowledgment

This work is supported by the SERENDIPITY project funded by The Swedish Foundation for Strategic Research (SSF) and the DPAC project funded by the Knowledge Foundation (KK-stiftelsen).

References

[1] C. A. Ericson, *Hazard analysis techniques for system safety*. New Jersey: Wiley, 2016.

[2] M. W. Maier, "Architecting principles for systems-of-systems," *System Engineering*, vol. 1, no. 4, pp. 267–284, 1998.

[3] C. Szabo, Y. M. Teo, and G. K. Chengleput, "Understanding complex systems: using interactions as a measure of emergence," in *2014 Winter Simulation Conference*, (Savannah, USA), pp. 207–218, 2014.

[4] A. J. Rae and R. D. Alexander, "Is the 'system of systems' a useful concept for hazard analysis?," in *29th ISSC*, 2011.

[5] P. F. Katina, C. B. Keating, and R. M. Jaradat, "System requirements engineering in complex situations," in *RE*, vol. 19, pp. 45–62, 2014.

[6] L. Provenzano, K. Hänninen, J. Zhou, and K. Lundqvist, "An ontological approach to elicit safety requirements," in *24th Asia-Pacific Software Engineering Conference (APSEC)*, (Nanjing, China), pp. 713–718, December 2017.

[7] N. Hamerurlain and C. Sibertin-Blanc, "Specification of role-based interactions components in multi-agent systems," in *Software Engineering for Multi-Agent Systems*, 2004.

[8] G. Cabri, L. Leonardi, and F. Zambonelli, "Brain: A framework for flexible role-based interactions in multiagent systems," in *Lecture Notes in Computer Science*, 2003.

[9] A. Caetano, A. R. Silva, and J. Tribolet, "Using roles and business objects to model and understand business processes," in *ACM Symposium on Applied Computing*, (New Mexico), pp. 1308–1313, 2005.

[10] B. J. Biddle, *Role theory - expectation, identities and behaviours*. New York: Academic Press Inc., 1979.

[11] T. Kühn, M. Leuthäuser, S. Götz, C. Seidl, and U. Aßmann, "A metamodel family for role-based modeling and programming language," in *SLE 2014*, (Sweden), pp. 141–160, 2014.

[12] B. J. Biddle, "Recent developments in role theory," *Annual Revision Sociology*, vol. 12, pp. 67–92, 1986.

[13] N. Guarino and C. Welty, "A formal ontology of properties," in *EKAW 2000*, vol. 1937, pp. 97–112, R. Dieng and O. Corby, 2000.

[14] N. Guarino, "Concepts, attributes, and arbitrary relations: some linguistic and ontological criteria for structuring knowledge bases," *Data & Knowledge Engineering*, vol. 8, no. 3, pp. 249–261, 1992.

[15] J. Black and P. Koopman, "System safety as an emergent property in composite systems," in *IFIP International Conference on Dependable Systems & Networks*, vol. 19, pp. 369–378, 2009.

[16] M. Fowler, *UML Distilled. A brief guide to the standard object modeling language*. Boston, USA: Addison-Wesley, 2004.

[17] E. Hollnagel, *FRAM - The functional resonance analysis method*. Farnham, UK: Ashgate, 2012.

[18] J. Rasmussen, "Risk management in a dynamic society: a modeling problem," *Safety Science*, vol. 27, no. 2, pp. 183–213, 1997.

[19] N. G. Leveson, "A new accident model for engineering safer systems," *Safety Science*, vol. 42, pp. 237–270, April 2004.

[20] S. Baumgart, J. Fröberg, and S. Punnekkat, "Analyzing hazards in system-of-systems: described in a quarry site automation context," in *IEEE International System Conference (SysCOn)*, pp. 544–551, 2017.

[21] P. Barlatier and R. Dapoigny, "A type-theoretical approach for ontologies: the case of roles," *Applied Ontology*, vol. 7, no. 3, pp. 311–356, 2012.

[22] F. Steimann, "On the representation of roles in object-oriented and conceptual modeling," *Data & Knowledge Engineering*, vol. 35, no. 1, pp. 83–106, 2000.

[23] R. Liu and X. Zhang, "Understanding human behaviours with an object functional role perspective for robotics," *IEEE Transactions on Autonomous Mental Development*, vol. 8, no. 2, pp. 115–127, 2015.

[24] T. Halpin, "Orm/niam object-role modeling," in *Handbook on Architectures of Information Systems. International Handbooks on Information Systems*, pp. 81–101, P. Bernus, K. Mertins, G. Schmidt, 1998.